On Kervaire–Murthy conjecture, Bernoulli and Iwasawa numbers, and zeroes of $p$-adic $L$-function

A. Stolin
Department of Mathematical Sciences
Chalmers University of Technology and
University of Gothenburg
Gothenburg, Sweden
E-mail: alexander.stolin@gu.se

Abstract

The aim of the present paper is to establish relations between Iwasawa and Bernoulli numbers based on some results by M. Kervaire and M. P. Murthy about the structure of the $K_0$ groups of the integer group rings of cyclic groups of prime power order $p^n$. In particular, we will prove that

- $\lambda_i \leq p - 1$ under assumption that the generalized Bernoulli number $B_{1,\omega^{-i}}$ is not divisible by $p^2$. Here $\omega$ is the Teichmüller character of $\mathbb{Z}/(p - 1)\mathbb{Z}$.
- $\lambda_i = 1$ if $B_{1,\omega^{-i}}$ is divisible by $p^2$.
- We will prove that $S_{n,i} \cong \mathbb{Z}/(p^{n+k_i})$, where $S_n$ is the Sylow $p$-subgroup of the class group of the field $\mathbb{Q}(\zeta_n)$. Here, $\zeta_n$ is a primitive $p^{n+1}$-root of unity, $\varepsilon_i$ are idempotents in the group ring $\mathbb{Z}_p[\text{Gal}(\mathbb{Q}(\zeta_0)/\mathbb{Q})]$, $S_{n,i} = \varepsilon_i(S_n)$, and $k_i$ is the $p$-adic valuation of $B_{1,\omega^{-i}}$.
- At the end we will prove that $k_i \leq 1$ and also $v_p(L_p(0,\omega^j)) \leq 1$ for even $j$ under certain conditions on zeroes of $L_p(0,\omega^j)$.
- Throughout the paper we assume that $p$ satisfies Vandiver’s conjecture.
1 Introduction

Let $C_n$ denote the cyclic group of order $p^n$, where $p$ is an odd prime. Let $\mathbb{Z}C_n$ be the integral group ring of $C_n$.

In this paper we study $\text{Pic} \mathbb{Z}C_n$ and some other groups related to it, in particular, the ideal class group $C(F_n)$ of the cyclotomic field $F_n = \mathbb{Q}(\zeta_n)$, where $\zeta_n$ is a primitive $p^n+1$-st root of unity.

Throughout this paper we assume that $p$ is semi-regular, that is $p$ does not divide the order of the ideal class group of the maximal real subfield $F_0^+ = \mathbb{Q}(\zeta_0 + \zeta_0^{-1})$ in $F_0$. Let $A$ be an abelian group. The following notation will be used in our paper:

- $F_n$ has been already defined, $F_n^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$;
- $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$;
- $N \cdot A$ (or sometimes $A^N$, if it is clear from a context) is the direct sum of $N$ copies of $A$;
- $dA$ or $A^d$ (depending on additive or multiplicative operation on $A$) stands for the subgroup of $A$ which consists of the elements of the form $da$ or $a^d$;
- $A^{(d)}$ stands for the subgroup of $A$ which consists of the elements of $A$ such that $da = 0$ or $a^d = 1$;
- $A_{(p)}$ denotes the Sylow $p$-component of $A$. For $A = C(F_n)$ we use a special notation $C(F_n)_{(p)} = S(F_n) = S_n$;
- if $R$ is a commutative ring, then $U(R)$ denotes the group of units of $R$.
- in the special case $R = \mathbb{Z}[\zeta_n]$, we use $E_n$ for $U(\mathbb{Z}[\zeta_n])$;
- further, we use notation $E_{n,k}$ for the subgroup of $E_n$ consisting of units which are congruent to 1 modulo $\mu_n = (1 - \zeta_n)^k$. 

MSC 2000 Primary 11R23, 11R29. Secondary 19A31.
Following [3] let us consider the fibre product diagram

\[
\begin{array}{c}
\mathbb{Z}C_{n+1} \xrightarrow{i_2} \mathbb{Z}[\zeta_n] \\
\downarrow i_1 \\
\mathbb{Z}C_n \xrightarrow{j_1} \mathbb{F}_p[x]/(x-1)p^n := R_n \\
\end{array}
\]

with obvious maps \(i_1, i_2, j_1, j_2\). The corresponding Mayer-Vietoris exact sequence can be written as follows:

\[
U(\mathbb{Z}C_n) \times E_n \xrightarrow{j} U(R_n) \rightarrow \text{Pic}(\mathbb{Z}C_{n+1}) \rightarrow \text{Pic}(\mathbb{Z}C_n) \times C(F_n) \rightarrow 0.
\]

One of the main problems in computing \(\text{Pic}(\mathbb{Z}C_{n+1})\) is thus to evaluate the cokernel \(W_n\) of the map \(j : U(\mathbb{Z}C_n) \times E_n \rightarrow U(R_n)\).

Instead of \(W_n\) we will evaluate a bigger group

\[V_n = \text{Coker}\{j_2 : E_n \rightarrow U(R_n)\}.\]

Clearly, \(W_n\) is a factor group of \(V_n\).

In the calculation of \(V_n\), a decisive role will be played by the action \(G_n = \text{Gal}(F_n/\mathbb{Q})\) on the various rings involved in the paper. Let \(\delta : G_n \rightarrow U(\mathbb{Z}/p^{n+1}\mathbb{Z})\) be the canonical isomorphism defined by \(s(\zeta_n) = \zeta_n^{\delta(s)}\), \(s \in G_n\). We will denote by \(x_n\) the generator in \(\mathbb{Z}[x]/(x^{p^n-1}) = \mathbb{Z}C_n\) and in \(\mathbb{F}_p[x]/(x-1)p^n = R_n\) that corresponds to \(x\). Since \(\delta(s)\) is an integer modulo \(p^{n+1}\), prime to \(p\), it is clear that both \(x_n^{\delta(s)}\) and \(x_n^{\delta(s)}\) are well-defined.

Moreover, the maps in the fibre product above commute with the action of \(G_n\). Let \(c \in G_n\) be the complex conjugation. It is clear that \(V_n = V_n^+ \times V_n^-\), where \(V_n^+\) consists of elements such that \(c(a) = a\) and \(V_n^-\) consists of elements such that \(c(a) = a^{-1}\) (we take into account that \(V_n\) is a \(p\)-group). Similarly, \(W_n = W_n^+ \times W_n^-\). For any abelian group \(A\), let us denote by \(A^*\) the group of characters of \(A\).

The main results proved by Kervaire and Murthy in [3] was

**Theorem 1.1.** If \(p\) is a semi-regular odd prime, then

\[(W_n^+)^* \subseteq (V_n^+)^* \subseteq S^-(F_{n-1}) = S(F_{n-1}) =: S_{n-1}.
\]

In other words, there is a surjection \(S_{n-1}^* \rightarrow V_n^+\).
They also conjectured that, in fact, \( W_n^+ \cong \mathcal{V}_n^+ \cong S_{n-1}^* \). The first main result of our paper is a weak version of the Kervaire and Murthy conjecture, namely

\[
(S_{n-1})^{(p)} \cong (\mathcal{V}_n^+/(\mathcal{V}_n^+)^p)^* = ((\mathcal{V}_n^+)^*)^{(p)}
\]

Another important result proved in this paper (which gives a new link between the class groups and the groups \( \mathcal{V}_n \)) is that there exists a canonical embedding

\[
S_{n-1}^{(p)} \to \mathcal{V}_n^-/(\mathcal{V}_n^-)^p
\]

Working on the Kervaire and Murthy conjecture, Ullom proved in [7] that under certain assumptions on the Iwasawa numbers \( \lambda_i \) explained later, the group \( W_n^+ \) can be described as follows:

\[
W_n^+ \cong r_0 \cdot (\mathbb{Z}/p^n\mathbb{Z}) \oplus (\lambda - r_0) \cdot (\mathbb{Z}/p^{n-1}\mathbb{Z}).
\]

Here

\[
r_0 = \dim_{\mathbb{F}_p}(S_0)_{(p)} = \dim_{\mathbb{F}_p}(S_0/S_0^p), \quad \lambda = \sum \lambda_i.
\]

Notice that \( r_0 \) also coincides with the number of Bernoulli numbers among \( B_2, B_4, \ldots, B_{p-3} \) which are divisible by \( p \). The Iwasawa invariant \( \lambda \) can be defined as follows. It is well-known due to Iwasawa and Washington (see [8]) that there exist two numbers \( \lambda \) and \( \nu \) called Iwasawa invariants such that \( S_n \) has \( p^{\lambda n + \nu} \) elements for sufficiently large \( n \).

Ullom’s proof is based on certain assumptions about the Iwasawa number \( \lambda \). More exactly,

\[
G_0 = \text{Gal}(F_0/\mathbb{Q}) \cong \mathbb{Z}/(p - 1)\mathbb{Z}
\]

acts on \( S_n \) and

\[
S_n = \bigoplus_{i=0}^{p-2} S_{n,i},
\]

where \( S_{n,i} = \varepsilon_i S_n \) and \( \varepsilon_i \) are idempotents in the group ring \( \mathbb{Z}_p[G_0] \). Since we work with semi-regular \( p \),

\[
\varepsilon_i S_0 \cong \mathbb{Z}_p/B_{1,\omega^{-i}}\mathbb{Z}_p \quad \text{for} \quad i = 3, 5, \ldots, p - 2.
\]

Here \( B_{1,\omega^{-i}} \) are generalized Bernoulli numbers and \( \omega \) is the Teichmüller character of \( \mathbb{Z}/(p - 1)\mathbb{Z} \) (see [8]).

Furthermore, for each \( i \) there exist \( \lambda_i \) and \( \nu_i \) such that \( S_{n,i} \) contains \( p^{\lambda_i n + \nu_i} \) elements. Ullom’s assumption was that \( \lambda_i < p - 1 \) and he conjectured that
it was true for any $p$. In this paper we will prove that $\lambda_i \leq p - 1$ under assumption that $B_{1,\omega^{-i}}$ is not divisible by $p^2$. Then we will prove that $\lambda_i = 1$ if $B_{1,\omega^{-i}}$ is divisible by $p^2$ that provides almost a complete proof of Ullom’s inequality under the assumption that Vandiver’s conjecture is true.

Remark 1.2. If $G_0$ acts on an abelian $p$-group $X$, then $X = \bigoplus_{i=0}^{p-2} X_i$ with $X_i = \varepsilon_i X$.

In our paper we will need the following presentation of $S_{n,i}$ (see [8] for details). Let $\omega$ be the Teichmüller character and $P_n(T) = (T + 1)^{p^n} - 1$. Let $f_i(T) \in \mathbb{Z}_p[[T]]$ be defined by the relation $f_i((1 + p)^s - 1) = L_p(s, \omega^{1-i})$, where $L_p$ is the $p$-adic L-function. In this terms the Iwasawa number $\lambda_i$ is the first coefficient of $f_i(T)$, which is not divisible by $p$.

By the $p$-adic Weierstrass Preparation Theorem $f_i(T) = U(T)p_i(T)$, where $U(T)$ is an invertible element of $\mathbb{Z}_p[[T]]$ such that $U(0) = 1$ and $p_i(T)$ is a unique polynomial of degree $\lambda_i$ with the leading coefficient co-prime to $p$ and all other coefficients divisible by $p$. Then

$$S_{n,i} = \mathbb{Z}_p[[T]]/(f_i, P_n) = \mathbb{Z}_p[T]/(p_i(T), P_n(T)).$$

2 Second presentation of $\mathcal{V}_n$ and norm maps

The following lemma was proved in [4].

Lemma 2.1. Let $A_n = \mathbb{Z}[x]/(x^p - 1)$. Then Pic $\mathbb{Z}C_n \cong$ Pic $A_n$

From now on we will study $A_n$ instead of $\mathbb{Z}C_n$. Clearly, we have the following fibre product:

$$
\begin{array}{c}
A_{n+1} \xrightarrow{i_2} \mathbb{Z}[\zeta_n] \\
\downarrow{i_1} \quad \quad \quad \downarrow{j_2} \\
A_n \xrightarrow{j_1} \mathbb{F}_p[x]/(x-1)^{p^n-1} := R'_n
\end{array}
$$

(1)

Lemma 2.2. Coker $\{j_2 : \mathbb{Z}[\zeta_n] \to U(\mathbb{F}_p[x]/(x - 1)^{p^n-1})\} \cong \mathcal{V}_n$.

Proof. We have to prove that

$$\text{Coker}(U(\mathbb{Z}[\zeta_n]) \to U(\mathbb{F}_p[x]/(x - 1)^{p^n})) =$$
Coker\((U(\mathbb{Z}[\zeta_n]) \rightarrow U(\mathbb{F}_p[x]/(x-1)^{p^n-1}))\).

Clearly, it is sufficient to prove that the element
\[ 1 + (x-1)^{p^n-1} \in U(\mathbb{F}_p[x]/(x-1)^p) \]

is the image of some unit of \(\mathbb{Z}[\zeta_n]\). It is easy to see that the image of the unit \((\zeta_{pn+1} - 1) / (\zeta_{n-1} - 1)\) under the map \(\mathbb{Z}[\zeta_n] \rightarrow \mathbb{F}_p[x]/(x-1)^p\), \(\zeta_n \rightarrow x\) is exactly \(1 + (x-1)^{p^n-1}\), and the proof is complete. \(\square\)

**Remark 2.3.** This lemma justifies an abuse of notation \(j_1, j_2, i_1, i_2, R_n\) in \([1]\).

The map \(N_n : \mathbb{Z}[\zeta_n] \rightarrow A_n\) such that \(N_n(ab) = N_n(a)N_n(b)\) and the diagram below is commutative has been introduced in \([5]\):

\[ \begin{array}{ccc}
A_{n+1} & \xrightarrow{i_2} & \mathbb{Z}[\zeta_n] \\
\downarrow{i_1} & & \downarrow{j_2} \\
A_n & \xrightarrow{j_1} & R_n
\end{array} \]

(2)

We would like to remind the reader this construction. The following fibre product diagram can be used for the construction without lost of generality:

\[ \begin{array}{ccc}
\mathbb{Z}_p[x]/(x^{p^{n+1}} - 1) & \xrightarrow{i_2} & \mathbb{Z}_p[\zeta_n] \\
\downarrow{i_1} & & \downarrow{j_2} \\
\mathbb{Z}_p[x]/(x^{p^n} - 1) & \xrightarrow{j_1} & R_n
\end{array} \]

We construct \(N_n\) using induction. If \(n = 1\), then \(\mathbb{Z}_p[x]/(x^{p^0} - 1) \cong \mathbb{Z}[\zeta_0]\) and \(N_1\) is the usual norm map.

Commutativity of (2) was proved in \([4]\). The formula
\[ \varphi_1(a_1) = (a_1, N_1(a_1)) \in \mathbb{Z}_p[x]/(x^{p^2} - 1) \]

defines an injective homomorphism \(\varphi_1 : U(\mathbb{Z}[\zeta_1]) \rightarrow U(\mathbb{Z}_p[x]/(x^{p^2} - 1))\). Now we can define \(N_2(a_2) = \varphi_1(N_{\mathbb{F}_2/F_1}(a_2))\).
Simultaneously, $N_2$ defines

$$
\varphi_2 : U(\mathbb{Z}_p[\zeta_2]) \to U(\mathbb{Z}_p[x]/(\frac{x^p - 1}{x - 1}))
$$

via $\varphi_2(a_2) = (a_2, N_2(a_2)) \in \mathbb{Z}_p[x]/(\frac{x^p - 1}{x - 1})$, and so on.

Proofs that all of the maps $\varphi_i, N_i$ are well-defined can be found in [5].

They use rings $A_{n,k} = \mathbb{Z}[x]/(\frac{x^{p^n + k} - 1}{x - 1})$.

**Proposition 2.4.** Formula $\varphi_{n-1}(a_{n-1}) = (a_{n-1}, N_{n-1}(a_{n-1}))$ defines an embedding $E_{n-1} \to U(\mathbb{Z}[x]/(\frac{x^{p^n} - 1}{x - 1}))$, and $\text{Coker}(j_1 : E_{n-1} \to U(R_n)) \cong \mathcal{V}_n$.

**Proof.** Since we deal with semi-regular primes, the fact we need follows from that of $\text{Norm}_{F_n/F_{n-1}}(E_n) = E_{n-1}$ and thus, $j_2(E_n) = j_1(E_{n-1})$ in $U(R_n)$. 

Let us denote by $U_{n,k}$ the subgroup of $U(\mathbb{Z}_p[\zeta_n]) := U_n$, which consists of units congruent to 1 modulo $(\zeta_n - 1)^k = \mu_n^k$.

**Theorem 2.5.** We have

$$
\mathcal{V}_n \cong U_n/(U_{n,p^n-1} \cdot E_n) \cong U_{n-1}/(U_{n-1,p^n-1} \cdot E_{n-1})
$$

**Remark 2.6.** We remind the reader that $\mathcal{V}_n \cong U_n/(U_{n,p^n} \cdot E_n)$ by definition.

**Proof.** The first isomorphism is clear. Let us prove that $\mathcal{V}_n \cong U_{n-1}/(U_{n-1,p^n-1} \cdot E_{n-1})$. The formula $\varphi_{n-1}(a) = (a, N_{n-1}(a))$ defines an embedding $\varphi_{n-1} : U_{n-1} \to U(\mathbb{Z}_p[x]/(\frac{x^{p^n} - 1}{x - 1}))$.

It is sufficient to prove that the composition map $\varphi_{n-1} \cdot j_1$ has the kernel $U_{n-1,p^n-1}$. To do this, first we note that $U(R_n)$ and $U_{n-1}/U_{n-1,p^n-1}$ have the same number of elements. Therefore, it is enough to prove that $U_{n-1,p^n-1}$ is contained in the kernel. This was proved in [5]. We would like to demonstrate the case $n = 2$. For this, we should prove that

$$(a, \text{Norm}_{F_1/F_0}(a)) \equiv (1, 1) \mod(p) \text{ in } \mathbb{Z}_p[x]/(\frac{x^2 - 1}{x - 1})$$

if $a \equiv 1 \mod \mu_1^{p^2-1}$. It is easy to see that $(a, \text{Norm}_{F_1/F_0}(a)) \equiv (1, 1) \mod p$ is equivalent to that of $\text{Norm}_{F_1/F_0}(\frac{a - 1}{p}) \equiv \frac{\text{Norm}_{F_1/F_0}(a)}{p} \equiv 0 \mod p$ in $\mathbb{Z}_p[\zeta_0]$. Since $a \equiv 1 \mod \mu_1^{p^2-1}$, both sides are congruent to 0 modulo $p$. The general case was proved in [5] using the rings $A_{n,k}$ and induction in $n, k$. 

**Remark 2.7.** In fact, it is not difficult to prove that $(a, \text{Norm}_{F_1/F_0}(a)) \equiv (1, 1) \mod(p)$ in $\mathbb{Z}_p[x]/(\frac{x^2 - 1}{x - 1})$ iff $a \equiv 1 \mod \mu_1^{p^2-1}$.
In the sequel we will need the following

**Corollary 2.8.** Suppose \( a \in U_2 \) is such that \( a \equiv 1 \mod \mu_2^{p^2-1} \). Then \( \text{Norm}_{F_2/F_1}(a) \equiv 1 \mod \mu_1^{p^2-1} \).

**Proof.** Consider the diagram 2 for \( n = 2 \). Then \( N_2(a) = (\text{Norm}_{F_2/F_1}(a), \text{Norm}_{F_2/F_0}(a)) \equiv (1,1) \mod (p) \) in \( \mathbb{Z}_p[x]/(x^{p^2-1} - 1) \). Consequently, \( \text{Norm}_{F_2/F_1}(a) \equiv 1 \mod \mu_1^{p^2-1} \). \( \square \)

### 3 Number of elements in \( \mathcal{V}_n^+ \)

Let us introduce integers \( r_n \) as the number of elements in \( E_{n,p^{n+1-1}}/E_{n,p^n+1} \). Similarly, let \( r_{n,i} \) be the number of elements in \( \varepsilon_i(E_{n,p^{n+1-1}}/E_{n,p^n+1}) \). In particular, it follows that \( r_n = \sum r_{n,i}, r_{0,i} = 1 \) if \( \lambda_{p-i} > 0 \), otherwise \( r_{0,i} = r_{k,i} = 0 \).

**Lemma 3.1.** If \( \varepsilon \in E_{n,p^{n+1}} \), then \( \varepsilon \) is real and therefore, \( E_{n,p^{n+1}} = E_{n,p^{n+1}}^+ \).

**Theorem 3.2.** Let \( \alpha \) be an ideal of \( \mathbb{Z}[\zeta_n] \) such that \( \alpha^p = (q) \). Let \( q \equiv 1 \mod \mu_n^{p^{n+1}-1} \). Then \( q \equiv 1 \mod \mu_n^{p^n} \).

Before we give a proof of the theorem, let us formulate its consequence, which we will need in sequel.

**Corollary 3.3.** \( E_{n,p^{n+1-1}} = E_{n,p^n+1+1} \).

**Proof of Theorem 3.2.** Consider the extension \( F_n(\sqrt[p]{q})/F_n \). Only \( \mu_n \) ramifies in this extension. Let \( \varepsilon \in E_n \). Then for any valuation \( v \neq \mu, \varepsilon \) is a norm in the corresponding extension of local fields \( F_{n,v}(\sqrt[p]{q})/F_{n,v} \). Therefore, the local norm residue symbol with values in the group of \( p \)-th roots of unity \( (\varepsilon, q)_{\mu_n} = 1 \). By the product formula, \( (\varepsilon, q)_{\mu_n} = 1 \). Set \( \varepsilon = \zeta_n \). If \( q \equiv 1 \mod \mu_n^{p^{n+1}} \) but \( q \neq 1 \mod \mu_n^{p^n} \), then simple local computations (see for instance [1]) show that \( (\zeta_n, q)_{\mu_n} \neq 1 \). The theorem is proved. \( \square \)

**Theorem 3.4.** The number of elements in \( \mathcal{V}_n^+ \) is \( p^{r_0+...+r_{n-1}} \).

**Proof.** If \( n = 1 \), then it was proved in [3]. Let us denote the number of elements in group \( A \) by \( |A| \). Assume that \( |\mathcal{V}_n^+| = p^{r_0+...+r_{n-1}} \). Let us prove that \( |\mathcal{V}_{n+1}^+| = p^{r_0+...+r_{n-1}+r_n} \). Indeed, \( |(U_n/(U_n.p^{n} \cdot E))_{n+1}^+| = p^{r_0+...+r_{n-1}} \). Clearly,
\[
(U_n/(U_{n,p^n} \cdot E))^+ = U_n^+/(U_{n,p^n}^+ \cdot E^+) \quad \text{and} \quad U_{n,p^n}^+ = U_{n,p^{n+1}}^+ \quad \text{since} \quad p \quad \text{is odd.}
\]

Taking into account that \( Y_{n+1}^+ \simeq U_n^+/(U_{n,p^{n+1}}^+ \cdot E_n^+) \), it remains to prove that
\[
\left| \frac{U_{n,p^n}^+ \cdot E_n^+}{U_{n,p^{n+1}}^+ \cdot E_n^+} \right| = p^{r_n}.
\]

Let us use the isomorphism
\[
\frac{U_{n,k}^+ \cdot E_n^+}{E_n^+} \simeq U_{n,k}^+ \cdot E_n^+,
\]
which shows that we have to prove that
\[
\left| \frac{U_{n,p^n}^+}{U_{n,p^{n+1}}^+} \right| : \left| \frac{E_{n,p^n}^+}{E_{n,p^{n+1}}^+} \right| = p^{r_n}.
\]

It is easy to see that
\[
\left| \frac{U_{n,p^n}^+}{U_{n,p^{n+1}}^+} \right| = p^{\frac{n+1-n}{2}}.
\]

The second number can be computed as follows:
\[
\left| \frac{E_{n,p^n}^+}{E_{n,p^{n+1}}^+} \right| = \left| \frac{E_{n,p^n}^+}{(E_{n,p^n})^p} \right| : \left| \frac{E_{n,p^{n+1}}^+}{(E_{n,p^{n+1}})^p} \right| = p^{\frac{n+1-n}{2}} : p^{r_n}
\]

and the theorem is proved.

Closing this section we would like to mention the following

**Proposition 3.5.** \( r_0 \leq r_1 \leq \ldots \leq \lambda = \sum \lambda_i \).

**Proof.** Let \( \epsilon \in E_{n,p^n+1}/(E_{n,p^n})^p \). Then the extension \( F_n(\sqrt[p]{\epsilon})/F_n \) is unramified, which defines an embedding \( E_{n,p^n+1}/(E_{n,p^n})^p \) into \( S_n^* \). It is easy to see that the canonical embedding \( S_n^* \to S_{n+1}^* \) defines an embedding
\[
E_{n,p^n+1}/(E_{n,p^n})^p \to E_{n+1,p^n+2+1}/(E_{n,p^n+1})^p.
\]

Therefore, \( r_n \leq r_{n+1} \).

Furthermore, because of the projection \( S_n^* \to Y_{n+1}^+ \) (see \([3]\)) it is clear that \( p^{\lambda n+\nu} \geq p^{r_0+r_{n+1}+r_n} \), and the latter inequality implies that \( r_n \leq \lambda \). \( \square \)

**Corollary 3.6.** If \( p \) divides \( B_{1,\omega^{-i}} \), then the number of elements in \( \epsilon_i(Y_n^+) \) is \( p^{1+r_1+r_{n-1}+\ldots+r_{n-1}+1,i} \) and \( 1 \leq r_{1,i} \leq \ldots \leq r_{k,i} \leq \lambda_{p-i} \).
4 Weak Kervaire-Murthy Conjecture and New Link between $S$ and $V$ Groups

In this section let us denote by $(a, b)$ the local norm residue symbol with values in $p$-th roots of unity. Here $(a, b)$ are elements of the completion of $F_n$ with respect to $\mu_n$. Assume that $a \in U_{n,k} \setminus U_{n,k+1}$, $b \in U_{n,p^{n+1}-k} \setminus U_{n,p^{n+1-k+1}}$, and $k$ is prime to $p$.

Lemma 4.1 (see [1]). $(a, b) \neq 1$.

Theorem 4.2. Let $\alpha \in S_n^{(p)}$ and $\alpha^p = (q)$. Then the formula $f_\alpha(x) = (x, q)$, $x \in V_{n+1}^+$ defines a non-trivial character of $V_{n+1}^+$ (if $\alpha$ is not trivial).

Proof. Step 1. If $q \equiv 1 \pmod{\mu_n^{p^{n+1}-1}}$, then $\alpha = 1 \in S_n$.

Indeed, we already know that $q \equiv 1 \pmod{\mu_n^{p^{n+1}}}$ and hence the extension $F_n(\sqrt[q^n]{q})/F_n$ is non-ramified. Therefore, $q = \varepsilon \cdot a^p$ for some $\varepsilon \in E_n$, $a \in F_n$ and consequently $\alpha = 1$ in $S_n$.

Step 2. Without lost of generality we can assume that $q \in U_{n,k} \setminus U_{n,k+1}$ with $k < p^{n+1} - 1$ and $k$ being prime to $p$.

Indeed, if $k = p \cdot s$, then $q = 1 + a_0\mu_n^{ps} + t\mu_n^{ps+1}$, where $a_0$ is an integer prime to $p$. Easy computations show that $q(1 - a_0\mu_n^s)^p \in U_{n,k+1}$. Proceeding in this way, we can find $q_1 \in U_{n,k_1}$ such that $(q_1) = (\Gamma\alpha)^p$, $\Gamma \in U(F_n)$, and such that $k_1$ is prime to $p$.

Step 3. $1 + \mu_n^{p^{n+1}-k} \in V_{n+1}$.

Indeed, if $1 + \mu_n^{p^{n+1}-k} \equiv \varepsilon \pmod{\mu_n^{p^{n+1}-k}}$, $\varepsilon \in E_n$, then $(\varepsilon, q) = 1$. However, it is not true by Step 2 and Lemma of this section.

Step 4. Since $S_n = S_n^-$, the character constructed above is a non-trivial character of the group $V_{n+1}^-$. The proof is complete. \qed

Corollary 4.3. ("weak Kervaire–Murthy conjecture") $S_n^{(p)} \cong (V_{n+1}^+/(V_{n+1}^+)^p)^*$.

Corollary 4.4. $S_n^*/(S_n^*)^p \cong V_{n+1}^+/(V_{n+1}^+)^p$.

Proof. This follows from the existence of the surjection $S_n^* \twoheadrightarrow V_{n+1}^+$ constructed in [3]. \qed

Theorem 4.5. There exists a canonical embedding

$$i : S_n^{(p)} \rightarrow V_n^-/((V_n^-)^p)$$
Proof. Let $\alpha$ be an ideal such that $\alpha^p = (q)$. Define $i(\alpha) = q$. This map is well-defined because the number $q$ is defined up to a transformation $q \to \epsilon r^p q$, where $\epsilon \in E_n$. Clearly, the images of $q$ and $\epsilon r^p q$ coincide in $V_n / (V_n)^p$. If $\alpha \in \text{Ker}(i)$, then $q \equiv \epsilon r^p \text{ mod } (1 - \zeta_n)^{p^n - 1}$ and it follows from the Step 1 of the proof of the previous theorem that $\alpha = 1$. Hence, $i$ is an embedding.

Since $S = S^-$, it follows that $i$ maps $S_{n-1}$ into $(V_n / (V_n)^p)^- = V^- / (V^-)^p$. 

5 Ullom’s inequality

The aim of this section is to prove the following result (a weaker version of Ullom’s inequality):

**Theorem 5.1.** Let the generalized Bernoulli number $B_{1, \omega - i}$ is divisible by $p$ but not by $p^2$. Then the corresponding Iwasawa number $\lambda_i$ is less than $p$.

**Proof.** The proof will consist of several lemmas. For technical reasons it will be easier to deal with the original definition of $V_2$, namely

\[ V_k = \text{Coker}\{j_2 : E_k \rightarrow U(R_k)\}, \quad k = 1, 2; \]

see Introduction.

Let us also make an important note: $R_2 = \mathbb{Z}[\zeta_2] / (\zeta_2 - 1)^{p^2}$ and $R_1 = \mathbb{Z}[\zeta_1] / (\zeta_1 - 1)^p$

**Lemma 5.2.** The map $\pi : R_2 \rightarrow R_1$ defined as $\pi(x) = x^p$ is an surjective homomorphism of rings, which induces an epimorphism of the corresponding groups of units $\pi : U(R_2) \rightarrow U(R_1)$ and $\pi : V_2 \rightarrow V_1$.

**Proof.** $\pi(a + b) = (a + b)^p = \pi(a) + \pi(b)$ and $\pi(m) = m^p = m$, $m \in \mathbb{Z}$ because $(p) = (\zeta_2 - 1)^{p^3 - p^2} = (\zeta_1 - 1)^{p^2 - p} = 0 \in R_2$. Furthermore, $\pi(\zeta_2 - 1) = (\zeta_2 - 1)^p = \zeta_1 - 1$ and $\pi(1 + (\zeta_2 - 1)^k) = (1 + (\zeta_2 - 1)^k)^p = 1 + (\zeta_1 - 1)^k$ what proves that $\pi$ is surjective homomorphism of the rings and the corresponding groups of units.

To prove that $\pi : U(R_2) \rightarrow U(R_1)$ induces a surjection $\pi : V_2 \rightarrow V_1$ we need to prove that $\pi(E_2) \subseteq E_1$. Since $p$ satisfies Vandiver’s conjecture, we can use the subgroup of cyclotomic units $C(k) \subset E_k$ insted of $E_k$. This means
that we have to show that $\pi(C(2)) \subseteq C(1)$. However, this is clear because of our previous computations:

$$
\pi\left(\frac{\zeta_2^m - 1}{\zeta_2 - 1}\right) = \pi(1 + \zeta_2 + \ldots + \zeta_2^{m-1}) = 1 + \zeta_1 + \ldots + \zeta_1^{m-1} = \frac{\zeta_1^m - 1}{\zeta_1 - 1}.
$$

The latter computation completes the proof. \hfill \Box

**Corollary 5.3.** If $x \in V_2$ is such that $x^p = 1$, then $x \in \ker(\pi)$.

**Lemma 5.4.** If $\lambda_i \geq p$, then $S_{1,i}$ has $p$ generators as an abelian group (we assume that $p$ is semi-regular).

**Proof.** We have already mentioned in Introduction that it follows from results of [8] that

$$S_{1,i} \cong \frac{\mathbb{Z}_p[T]}{((T + 1)^p - 1, p_i(T))},$$

where $p_i(T)$ is a polynomial of degree $\lambda_i$ and such that all the coefficients except of the leading one are divisible by $p$. Clearly,

$$S_{1,i}/(S_{1,i})^p \cong \frac{\mathbb{Z}_p[T]}{(p, T^p, T^\lambda_i)} = \frac{\mathbb{Z}_p[T]}{(p, T^p)},$$

what proves the lemma. \hfill \Box

**Lemma 5.5.** If $\lambda_i \geq p$ and $b_i := B_{1,\omega^{-i}}$ is divisible by $p$ but not by $p^2$, then $S_{1,i} \cong V_{2, p^{-i}} \cong (\mathbb{F}_p)^p$ as abelian groups. Here $V_{2, p^{-i}} = \mathbb{F}_{p^{-i}}V_2$.

**Proof.** Consider the following fibre product:

$$
\begin{array}{c}
\mathbb{Z}_p[T]/((T + 1)^p - 1) \xrightarrow{i_1} \mathbb{Z}_p[\zeta_0] = \mathbb{Z}_p[T]/((T + 1)^p - 1) \\
\mathbb{Z}_p[T]/(T) \xrightarrow{j_1} \mathbb{F}_p
\end{array}
$$

Here, $i_1(T) = 0$, $j_1(\zeta_0) = 1$ and horizontal maps are defined by $T \to T$, $1 \to 1$.

Let us write elements of $\mathbb{Z}_p[T]/((T + 1)^p - 1)$ as pairs $(x \in \mathbb{Z}_p, y \in \mathbb{Z}_p[\zeta_0])$ with clear compatibility conditions. In order to prove that $S_{1,i} \cong (\mathbb{F}_p)^p$, it is sufficient to show that $(p_i(0), p_i(\zeta_0 - 1))$ divides $(p, p)$ in $\mathbb{Z}_p[T]/((T + 1)^p - 1)$.
Indeed, \( p_i(0) = b_i \) and \( p_i(\zeta_0 - 1) = b_i + \sum a_k(\zeta_0 - 1)^k + (\zeta_0 - 1)^{\lambda_i} \). Since \( p \) divides \( a_k \), \( (p) = (b_i) = (\zeta_0 - 1)^{p-1} \), and \( \lambda_i \geq p \), we see that \( p_i(\zeta_0 - 1) = b_i(1 + (\zeta_0 - 1)X) \) and therefore, \( (p_i(0), p_i(\zeta_0 - 1)) = (b_i, b_i) \times (1, 1 + (\zeta_0 - 1)X) \). It follows that \( (p_i(0), p_i(\zeta_0 - 1)) \) divides \( (p, p) \) and due to the weak Kervaire–Murthy conjecture the lemma is completely proved.

Now, we can finish proof of the theorem.

Due to 5.2 we have a surjection \( \pi : \varepsilon_{p-i} \mathcal{V}_2 \to \varepsilon_{p-i} \mathcal{V}_1 \). On the other hand, due to 5.3 and 5.5 \( \pi(\varepsilon_{p-i} \mathcal{V}_2) = 1 \). This contradiction completes the proof of the theorem.

\[ \square \]

6 Further relations between Bernoulli and Iwasawa numbers

The aim of this section is to prove that if the generalized Bernoulli number \( b_i = B_{1,\omega-i} \) is divisible by \( p^2 \), then the Iwasawa number \( \lambda_i = 1 \)

6.1 Fine structure of \( \mathcal{V}_{2,p-i}^+ \) if \( p^2 \) divides \( b_i \)

**Theorem 6.1.** Let \( b_i = p^{k_i}t, k_i \geq 2 \), where \( t \) is co-prime to \( p \). Then \( (\mathcal{V}_{2,p-i})^+ \cong (\mathbb{Z}/(p^2)) \oplus \mathbb{F}_p^k \), where \( k = \text{min}(\lambda_i - 1, p - 1) \).

**Proof.** \( \mathcal{V}_{2,p-i}^+ \) is a factor of \( \varepsilon_{p-i}(\mathcal{V}_2) = \varepsilon_{p-i}(U_1/U_{1,p^2-1}) = \varepsilon_{p-i}(U_1/U_{1,p^2+1}) \) because \( p - i \) is an even number between 2 and \( p - 3 \). It is easy to prove that \( \varepsilon_{p-i}(V_2) = (\mathbb{Z}/(p^2)) \oplus \mathbb{F}_p^{p-1} \).

It follows from the weak Kervaire–Murthy conjecture and 5.3 that \( \mathcal{V}_{2,p-i}^+ \cong (\mathbb{Z}/(p^2)) \oplus \mathbb{F}_p^k \) or \( \mathcal{V}_{2,p-i}^+ \cong \mathbb{F}_p^{k+1} \). So, we have to exclude the second possibility.

Let us denote the local norm residue symbol with values in \( p \)-roots of unity from the section 4 by \( (a, b)_{n,0} \). In particular, we are interested in \( (a, b)_{1,0} \) and \( (c, d)_{0,0} \). Let us also consider the local norm residue symbol with values in \( p^2 \)-roots of unity, which we denote by \( (a, b)_{n,1} \). Note that it is defined if \( n > 0 \).

Let us make the following easy remarks. To simplify notations, from now on we denote \( \mathcal{V}_{n,p-i}^+ \) by \( \mathcal{V}_{n,p-i} \)

**•** \( (a^p, b)_{1,1} = (a, b)_{1,0} \);
• if \( b \in \mathbb{Z}_p[\zeta_0] \), then \( (a, b)_{1,0} = (\text{Norm}_{F_1/F_0}(a), b)_{0,0} \);

• \((1 + (\zeta_0 - 1)^i, 1 + (\zeta_0 - 1)^j)_{0,0} = 1, \text{ if } i + j > p;\)

• \((1 + (\zeta_0 - 1)^i, 1 + (\zeta_0 - 1)^{p-i})_{0,0} \neq 1.\)

Let \( v_2 \) be the image of \( 1 + (\zeta_1 - 1)^{p-i} \) in \( V_{2,p-i} \). Let \( v_1 \) be the image of \( 1 + (\zeta_0 - 1)^{p-i} \) in \( V_{1,p-i} \cong \mathbb{Z}/(p) \). Clearly, \( \text{Norm}_{F_1/F_0}(v_2) \) generates the same element in \( V_{1,p-i} \cong \mathbb{Z}/(p) \) as \( v_1 \). We will write \( \text{Norm}_{F_1/F_0}(v_2) = v_1 \).

**Lemma 6.2.** Let us assume that \( p^2 \) divides \( b_i \). Then there exists an ideal \( \alpha \subset \mathbb{Z}[\zeta_0] \), whose class belongs to \( S_{0,i} \) such that \( \alpha^{p^2} = (q) \), \( q \in \mathbb{Z}[\zeta_0] \) and \( \alpha^p \) is not a principal ideal.

**Proof.** The statement follows from the fact that \( S_{0,i} \cong \mathbb{Z}_p/(b_i) \).

**Lemma 6.3.** Let \( v_2, q \) be as above. Then \( (v_2, q)_{1,1} \) is a primitive \( p^2 \)-root of unity.

**Proof.** Since \( \alpha \) generates an element of \( S_{0,i} \), it follows from results of Section 4 that \( q \) can be chosen such that \( q \equiv 1 \mod(\zeta_0 - 1)^i \). Let us compute \( (v_2, q)_{1,1}^p \).

\[
(v_2, q)_{1,1}^p = (v_2, q)_{1,1} = (v_2, q)_{1,0} = (\text{Norm}_{F_1/F_0}(v_2), q)_{0,0} = (v_1, q)_{0,0} \neq 1
\]

Since \( (v_2, q)_{1,1}^p \) is a non-trivial \( p \)-root of unity, clearly \( (v_2, q)_{1,1} \) is a \( p^2 \)-root of unity.

**Lemma 6.4.** Let \( q \) be as above. Then the formula \( \langle v, \alpha \rangle = (v, q)_{1,1} \) defines a character of \( V_{2,p-i} \).

**Proof.** We have to prove that \( (v, q)_{1,1} = 1 \) if \( v \) is a unit of \( \mathbb{Z}[\zeta_1] \) or \( v \equiv 1 \mod(1 - \zeta_1)^{p^2+1} \), the latter because

\[
\varepsilon_{1-p}(V_2) = \varepsilon_{p-i}(U_1/U_{1,p^2-1}) = \varepsilon_{p-i}(U_1/U_{1,p^2+1}).
\]

If \( v \) is a unit, then the extension \( F_1(u^{1/p^2})/F_1 \) can ramify at \( (1 - \zeta_1) \) only. Furthermore, for any prime \( \theta \neq (1 - \zeta_1) \) we have \( q = r^{p^2} \times \text{local unit} \) for some \( r \in (F_0)_\theta \). It follows that \( (v, q)_{\theta} = 1 \), here \( (v, q)_{\theta} \) is the corresponding local symbol with values in \( p^2 \)-roots of unity. The product formula implies that \( (v, q)_{1,1} = 1 \).

It remains to prove that \( (v, q)_{1,1} = 1 \) if \( v \equiv 1 \mod(1 - \zeta_1)^{p^2+1} \). Indeed, \( v = t^p \) for some \( t \in \mathbb{Z}_p[\zeta_1] \) such that \( t \equiv 1 \mod(1 - \zeta_1)^{p^2+1} \) and \( (v, q)_{1,1} = (t, q)_{1,0} = (\text{Norm}_{F_1/F_0}(t), q)_{0,0} = 1 \) because \( \text{Norm}_{F_1/F_0}(t) \equiv 1 \mod(p) \) and \( q \) can be chosen to satisfy \( q \equiv 1 \mod(1 - \zeta_0)^2 \). \( \square \)
Now we can finish the proof of the theorem. We have proved that \((v, q)_{1,1}\) is a character of \(\mathcal{V}_{2,p-i}\) and since \((v_2, q)_{1,1}\) is a primitive \(p^2\)-root of unity, we can exclude the possibility \(\mathcal{V}_{2,p-i} \cong \mathbb{F}_p^k\).

\[\square\]

### 6.2 The Main Theorem I

**Theorem 6.5.** Assume \(p^2\) divides \(b_i\), \(q\) is the same as in the previous subsection, and \(\sigma\) is a generator of \(\text{Gal}(F_1/F_0)\) such that \(\sigma(\zeta_1) = \zeta_1^{p+1}\). Then \(\sigma(v_2)/v_2 = v_2^p\), where \(v_2\) is a generator of \(\mathcal{V}_{2,p-i}\) such that \((v_2, q)_{1,1} = \zeta_1\).

**Proof.** Let us consider \((\sigma(v_2), q)_{1,1}\), where \(q\) is the same as in the previous subsection. We have \((\sigma(v_2), q)_{1,1} = \sigma((v_2, q)_{1,1}) = \zeta_1^{p+1} = (v_2, q)_{1,1}^{p+1}\). Hence, \((\sigma(v_2)/v_2, q)_{1,1} = (v_2^2, q)_{1,1} = \zeta_0\).

Let us consider the annihilator of \(\sigma(v_2)/v_2\) in the character group \((\mathcal{V}_{2,p-i})^*\). We denote it by \(\text{Ann}(\sigma(v_2)/v_2)\).

**Lemma 6.6.** \(\text{Ann}(\sigma(v_2)/v_2) \cong \mathbb{F}_p^{k+1}\), where \(k = \min(\lambda_i - 1, p - 1)\).

**Proof.** The proof consists of three statements below.

- \(\sigma(v_2)/v_2\) has order \(p\). Indeed, \((\sigma(v_2)/v_2, q)_{1,1} = \zeta_0\). Since \((\mathcal{V}_{2,p-i})^* \cong (\mathbb{Z}/(p^2)) \oplus \mathbb{F}_p^k\) and \(q\) generates a character of order \(p^2\), it follows that the value of any character on \(\sigma(v_2)/v_2\) is either a primitive \(p\)-root of unity or 1. Consequently, \(\sigma(v_2)/v_2\) has order \(p\) (it cannot be 1 because \((\sigma(v_2)/v_2, q)_{1,1} = \zeta_0\)).

- Therefore, \((\mathcal{V}_{2,p-i})^*/\text{Ann}(\sigma(v_2)/v_2) \cong \mathbb{F}_p^k\).

- Since \(q\) generates a character of order \(p^2\), \((\sigma(v_2)/v_2, q)_{1,1} = \zeta_0\), and \((\mathcal{V}_{2,p-i})^* \cong (\mathbb{Z}/(p^2)) \oplus \mathbb{F}_p^k\), we can deduce that \(\text{Ann}(\sigma(v_2)/v_2) \cong \mathbb{F}_p^{k+1}\).

\[\square\]

Now, we can complete the proof of the theorem. By the Kervaire–Murthy theorem, \(\text{Ann}(\sigma(v_2)/v_2)\) is a subgroup of \(S_{1,i}\). By the lemma above and the weak Kervaire–Murthy conjecture, we have \(\text{Ann}(\sigma(v_2)/v_2) \cong S_{1,i}^{(p)}\), the subgroup of elements of order \(p\). Thus, for any ideal \(\alpha_m = (q_m) \subset \mathbb{Z}[\zeta_1]\) we have \((\sigma(v_2)/v_2, q_m)_{1,0} = 1\) and \((\sigma(v_2)/v_2, q_m)_{1,0} = (v_2, q_m)_{1,0} = (v_2, q_m)^{p+1}\). It follows that \((\sigma(v_2)/v_2, q_m)_{1,0} = (v_2^p, q_m)_{1,0}\). Therefore, for any character \(\chi \in \mathcal{V}_{2,p-i}^*\), we have \(\chi(\sigma(v_2)/v_2) = \chi(v_2^p)\) and consequently \(\sigma(v_2)/v_2 = v_2^p\).

\[\square\]
6.3 Main Theorem II

Lemma 6.7. \( \varepsilon_{p^{-i}}(V_2) \) and \( V_{2,p^{-i}} \) are \( \mathbb{Z}_p[[T]] \)-modules with one generator. Here the action is defined as follows: \( T \cdot v = \sigma(v)/v \) and \( a \cdot v = v^a, \ a \in \mathbb{Z}_p. \)

Proof. \( \varepsilon_{p^{-i}}(V_2) = \varepsilon_{p^{-i}}(U_1/U_{1,p^{2-1}}). \) Since \( \varepsilon_{p^{-i}}(U_1) \) is an \( \mathbb{Z}_p[[T]] \)-modules with one generator, it is also true for its factors \( \varepsilon_{p^{-i}}(V_2) \) and \( V_{2,p^{-i}} \) because \( U_{1,p^{2-1}} \) and the image of \( U(\mathbb{Z}[\zeta]) \) in \( V_2 \) are \( \mathbb{Z}_p[[T]] \)-submodules.

\[ \square \]

Lemma 6.8. \( \varepsilon_{p^{-i}}(V_2) \cong \mathbb{Z}_p[[T]]/(T^p, pT, p^2). \)

Proof. It is easy to verify that \( pT \) and \( p^2 \) annihilate \( V_2 \). Further, \( \varepsilon_{p^{-i}}(U_1) \) is annihilated by \( (T + 1)^p - 1 \). Since \( pT \) annihilates \( \varepsilon_{p^{-i}}(V_2) \), we deduce that \( T^p \) annihilates it too. Finally, it is easy to see that both \( \varepsilon_{p^{-i}}(V_2) \) and \( \mathbb{Z}_p[[T]]/(T^p, pT, p^2) \) contain \( p^{i+1} \) elements. The last observation completes the proof.

\[ \square \]

Theorem 6.9. If the generalized Bernoulli number \( b_i = B_{1,\omega^{-1}} \) is divisible by \( p^2 \), then the Iwasawa number \( \lambda_i = 1 \)

Proof. It follows from \ref{6.3} that \( T - p \) annihilates \( V_{2,p^{-i}} \). Therefore, as a \( \mathbb{Z}_p[[T]] \)-module \( V_{2,p^{-i}} \) factors through \( \mathbb{Z}_p[[T]]/(T^p, pT, p^2, T - p) \cong \mathbb{Z}_p/(p^2) \). Since we already know that \( V_{2,p^{-i}} \cong \mathbb{Z}/(p^2) \oplus \mathbb{F}^k \), where \( k = min(\lambda_i - 1, p - 1) \), we conclude that \( V_{2,p^{-i}} \cong \mathbb{Z}/(p^2) \) and \( \lambda_i = 1 \).

\[ \square \]

Corollary 6.10. \( V_{n,p^{-i}} \cong \mathbb{Z}/(p^n) \) if \( p^2 \) divides \( b_i \).

Proof. It is an easy consequence of Corollary 3.6.

\[ \square \]

Corollary 6.11. \( S_{n,i} \cong \mathbb{Z}/(p^{n+k_i}) \) if \( p^2 \) divides \( b_i \). Here \( k_i \) is the \( p \)-adic valuation of \( b_i \).

Proof. The statement follows from the fact that \( \text{Norm}_{F_{n+1}/F_n}(i_{F_{n+1}/F_n})(\alpha) = \alpha^p \) for any ideal \( \alpha \subset \mathbb{Z}[[\zeta_n]] \) and that of \( \text{Norm}_{F_{n+1}/F_n} : S_{n+1} \rightarrow S_n \) is surjective while \( i_{F_{n+1}/F_n} : S_n \rightarrow S_{n+1} \) is injective.

\[ \square \]

7 Fine structure of \( V_{n,p^{-i}} \) and \( S_{n,i} \) if \( p^2 \) does not divide \( b_i \)

Throughout this section we assume that the \( p \)-adic valuation \( v_p(b_i) = 1 \). We already know that if \( p^2 \) does not divide \( b_i \), then \( \lambda_i \) satisfies Ullom’s inequality \( \lambda_i \leq p - 1 \) and \( S_{0,i} \cong \mathbb{F}_p. \)
7.1 Fine structure of $\mathcal{V}_{n,p-i}$

**Lemma 7.1.** Let $\alpha \in S_{0,i}$. Then $\alpha = \beta^p$, where $\beta \in S_{1,i}$.

*Proof.* We consider $S_{1,i}$ as a $\mathbb{Z}_p[[T]]$-module. It follows from results of [8] that

$$ S_{1,i} \cong \frac{\mathbb{Z}_p[[T]]}{((T + 1)^p - 1, f_i(T))} = \frac{\mathbb{Z}_p[T]}{((T + 1)^p - 1, p_i(T))^i}, $$

where $f_i(T), p_i(T)$ were defined in Introduction.

Clearly, $S_{1,i}/(S_{1,i})^p \cong \frac{\mathbb{Z}_p[T]}{(p_i(T)^{\lambda_1})} = \mathbb{F}_p[T]/(T^\lambda_1)$, because of Ullom’s inequality. Let us prove that the image of $S_{0,i}$ under the canonical embedding $i_{F_1/F_0} : S_{0,i} \to S_{1,i}$ is contained in $S_{1,i}^p$. Indeed, this image is generated by $N(T) = 1 + (T + 1) + \cdots + (T + 1)^{p-1} = ((T + 1)^p - 1)/T$. Again, because of Ullom’s inequality, the image of $N(T)$ in $S_{1,i}/(S_{1,i})^p \cong \mathbb{Z}_p[T]/(p_i(T)^{\lambda_1})$ is zero. The lemma is proved. $\square$

The crucial step in computation of $\mathcal{V}_{n,p-i}$ is to consider the case $n = 2$. From the weak Kervaire–Murthy conjecture and Ullom’s inequality, we know that as an abelian group $\mathcal{V}_{2,p-i}$ has $\lambda_i$ generators. Thus, we have two possibilities: $\mathcal{V}_{2,p-i} \cong \mathbb{Z}/(p^2) \oplus \mathbb{F}_p^{\lambda_i-1}$ or $\mathcal{V}_{2,p-i} \cong \mathbb{F}_p^{\lambda_i}$.

**Theorem 7.2.** $\mathcal{V}_{2,p-i} \cong \mathbb{Z}/(p^2) \oplus \mathbb{F}_p^{\lambda_i-1}$.

*Proof.* It is sufficient to find an element in $\mathcal{V}_{2,p-i}^*$ of order $p^2$.

With some abuse of notations, let $\alpha^p = (q)$, $q \in \mathbb{Z}[\zeta_0]$. Since $\beta^p = \alpha$ in $S_{1,i}$, it follows that $\beta^{p^2} = (qt^p)$, where $q \in \mathbb{Z}[\zeta_1]$. We claim that the required character is defined by $(v, qt^p)_{1,1}$. To prove this, we follow the proof of Theorem 6.1.

**Lemma 7.3.** $(v, qt^p)_{1,1} = \zeta_1$ for some $v$.

*Proof.* We have $(v, qt^p)_{1,1} = (v, qt^p)_{1,1} = (v, q)_{1,1} = (v, q)_{1,0} = (\text{Norm}_{F_1/F_0}(v), q)_{0,0}$. Clearly, we can choose $v$ such that $(\text{Norm}_{F_1/F_0}(v), q)_{0,0} = \zeta_0$ and therefore, $(v, qt^p)_{1,1} = \zeta_1$. $\square$

**Lemma 7.4.** Let $r \in \mathbb{Z}_p[\zeta_1]$ be such that $r \equiv 1 \mod (1 - \zeta_1)p^{2+1}$. Then $(r, qt^p)_{1,1} = 1$. Further, $(\epsilon, qt^p)_{1,1} = 1$ if $\epsilon \in \mathbb{Z}[\zeta_1]$.

*Proof.* Since $r = r_1^p$, where $r_1 \in \mathbb{Z}_p[\zeta_1]$, we can proceed exactly as in the proof of Lemma 6.4. Since $(qt^p) = \beta^{p^2}$, again we can simply repeat the arguments of the proof of Lemma 6.4. $\square$
Two lemmas above imply that the element \( qt^p \) induces a character of \( V_{2,p-i} \) of order \( p^2 \). The theorem is proved. \( \square \)

**Corollary 7.5.** If \( b_i \) is not divisible by \( p^2 \), then \( V_{n,p-i} \cong \mathbb{Z}/(p^n) \oplus (\mathbb{Z}/(p^{n-1}))^{\lambda_i-1} \).

**Proof.** Corollary 3.6 implies that \( r_{m,p-i} = \lambda_i \) for any \( m \geq 1 \) and moreover, the number of elements in \( V_{n,p-i} \) is \( p^{1+\lambda_i} \). On the other hand, \( V_{n,p-i} \) is a factor of a bigger group \( \varepsilon_{p,i}(V_n) = \varepsilon_{p,i}(U_{n-1}/U_{n-1,p^n-1}) \). It is easy to verify that \( \varepsilon_{p,i}(V_n) \cong \mathbb{Z}/(p^n) \oplus T \), where the abelian group \( T \) has exponent \( p^n-1 \) (an exact formula can be derived from [3] but we do not need it). Comparing the number of elements and the number of generators of \( V_{n,p-i} \) which is \( \lambda_i \), we can deduce that \( V_{n,p-i} \cong \mathbb{Z}/(p^n) \oplus (\mathbb{Z}/(p^{n-1}))^{\lambda_i-1} \). \( \square \)

### 7.2 Fine structure of \( S_{n,i} \)

Let \( A \) be a finite abelian group such that \( A \cong \oplus_j \mathbb{Z}/(p^j) \). Let us denote the abelian group \( \oplus_j \mathbb{Z}/(p^j+m) \) by \( \Sigma_m A \).

**Lemma 7.6.** \( S_{n+1,i} \cong \Sigma_n S_{1,i} \).

**Proof.** The fact follows from the following observations:

- all the groups \( S_{k,i}, \ k \geq 1 \), have \( \lambda_i \) generators;
- \( \text{Norm}_{F_{k+1}/F_k}(i_{F_{k+1}/F_k}(\alpha)) = \alpha^p, \ \alpha \in S_{k,i} \).

**Remark:** it is well-known that \( i_{F_{k+1}/F_k} : S_{k,i} \to S_{k+1,i} \) is an embedding and \( \text{Norm}_{F_{k+1}/F_k} : S_{k+1,i} \to S_{k,i} \) is a surjection. \( \square \)

It remains to compute \( S_{1,i} \).

**Theorem 7.7.** Assume that \( 1 \leq \lambda_i < p - 1 \). Then \( S_{1,i} \cong \mathbb{Z}/(p^2) \oplus \mathbb{F}_p^{\lambda_i-1} \).

**Proof.** \( S_{1,i} \cong \mathbb{Z}_p[T]/((T + 1)^p - 1, f_i(T)) \), see [3]. Since \( p^2 \) does not divide \( b_i \), the polynomial \( f_i(T) \) is irreducible. Let \( a \) be its root. Then \( \mathbb{Z}_p[T]/(f_i(T)) \cong \mathbb{Z}_p[a], \ a, a^2, \ldots, a^{\lambda_i-1} \) generate \( \mathbb{Z}_p[a] \) as an abelian group, \( (p) = (a^{\lambda_i}) \) in \( \mathbb{Z}_p[a] \), and \( S_{1,i} \cong \mathbb{Z}_p[a]/((a + 1)^p - 1) \). Further, \( ((a + 1)^p - 1) = (a^{\lambda_i+1}) \) because \( \lambda_i < p - 1 \). It follows that the element \( 1 \in \mathbb{Z}_p[a] \) has exponent \( p^2 \) and all other generators of \( \mathbb{Z}_p[a], \ a, a^2, \ldots, a^{\lambda_i-1} \) have exponent \( p \). The theorem is proved. \( \square \)
The case \( \lambda_i = p - 1 \) is more delicate. To treat this case we need the Cartesian square from Lemma 5.5. Let us denote the ring \( \mathbb{Z}_p[T]/((T+1)^p-1) \) by \( B \). We have to study \( B/(f_i(T)) \). We remind the reader that any element \( b \in B \) can be written as a pair \((c, d)\), \( c \in \mathbb{Z}_p, d \in \mathbb{Z}_p[\zeta_0] \). In this notation \( f_i(T) = (b_i, f_i(\zeta_0 - 1)) \).

A simple analysis of this case shows the following result:

**Theorem 7.8.** The element \( 1 \in \mathbb{Z}_p[T]/((T+1)^p-1) \) has exponent \( p^e \) with \( \kappa = \left[ \frac{k}{p-1} \right] + 1 \). Here \( k = v_p(f_i(\zeta_0 - 1)) \), where \( v_p \) is the extension of the \( p \)-adic valuation on \( \mathbb{Z}_p \) to \( \mathbb{Z}_p[\zeta_0] \).

**Remark 7.9.** \( v_p(f_i(\zeta_0 - 1)) = v_p(L_p(s_0, \omega^{1-i})) \), where \( L_p \) is a \( p \)-adic L-function, \( \omega \) is the Teichmüller character of \( \mathbb{Z}/(p - 1)\mathbb{Z} \), and \( s_0 \) satisfies the following equation: \( (p + 1)^{s_0} = \zeta_0 \).

### 7.3 Fine structure of the group ”Local units modulo closure of the cyclotomic units”

Our aim is to describe the group \( (U_{n,1}/C(n))^+ \), where \( U_{n,1} \) is the group of units of \( \mathbb{Z}_p[\zeta_n] \) congruent 1 modulo \( (\zeta_n - 1) \) and \( C(n) \) is the closer of the subgroup of the cyclotomic units. Let \( G_{n,k} = \text{Gal}(F_n/F_k) \). If \( A \) is a \( G \)-module, then \( A^G \) is a submodule of \( G \)-invariant elements of \( A \). We begin with the following result:

**Theorem 7.10.** The canonical map \( (U_{k,1}/C(k))^+ \to (U_{n,1}/C(n))^+ \) is an embedding and \( \{(U_{n,1}/C(n))^{G_{n,k}}\}^+ \cong (U_{k,1}/C(k))^+ \).

**Proof.** Let us consider the following short exact sequence:

\[
0 \to C(n) \to U_{n,1} \to U_{n,1}/C(n) \to 0.
\]

Thus, we get the corresponding exact sequence of cohomologies:

\[
0 \to C(n)^{G_{n,k}} \to U_{n,1}^{G_{n,k}} \to (U_{n,1}/C(n))^{G_{n,k}} \to H^1(G_{n,k}, C(n)).
\]

Thus, to prove the theorem we have to show that \( H^1(G_{n,k}, C(n)^+) = 1 \).

Let us show first that the Herbrand index \( h(G_{n,k}, C(n)^+) = 1 \). Indeed, \( C(n)^+ \) is a finite index subgroup of the group of global units \( E_n \). Its closure contains an open subgroup of \( U_{n,1}^+ \) due to Leopoldt’s conjecture about the closure of the group of global units, which is true in our case. Thus, \( C(n)^+ \)
contains an open subgroup $X$ of $U_{n,1}^+$ as well. Consequently, $h(G_{n,k}, C(n)^+) = h(X) \cdot h(C(n)^+/X) = 1$ because $h(C(n)^+/X) = 1$ since the group $C(n)^+/X$ is finite and $h(X) = 1$ because $X$ can be chosen as a projective $G_{n,k}$-module, see [1], chapter 6.

Therefore, it suffices to prove that $H^2(G_{n,k}, C(n)) = 1$. However, it is clear because $H^2(G_{n,k}, C(n)) = C(k)/\text{Norm}_{F_n/F_k}(C(n)) = 1$ because the norm is surjective on the group of cyclotomic units.

Let us give another proof of the same theorem based on a lemma needed in the sequel. Let us remind the reader that series $f_i(T)$ and polynomials $p_i(T), P_n(T)$ were defined in Introduction. Let us define $g_i(T) = f_i(\frac{1+p_i}{1+p_i^2} - 1)$ and the polynomial $q_i(T)$ exactly in the same way as $p_i(T)$ was defined from $f_i(T)$. It is clear that $\deg(p_i) = \deg(q_i) = \lambda_i$. Furthermore, with our choice of the polynomials $p_i, q_i$ we have $p_i(0) = f_i(0) = L_p(0, \omega^{1-i}) = b_i$ and $q_i(0) = g_i(0) = f_i(p) = L_p(1, \omega^{1-i}) := c_i$.

However, generally speaking $p_i(p) \neq f_i(p)$ while we only have $v_p(f_i(p)) = v_p(p_i(p)) = v_p(c_i)$. As in Introduction, we denote $(T + 1)^n - 1$ by $P_n(T)$ and $P_n(T)/P_k(T)$ by $P_{n,k}(T)$.

**Lemma 7.11.** We have:

- $\varepsilon_{p^{-1}}U_{n,1} \cong \mathbb{Z}_p[[T]]/(P_n(T)) = \mathbb{Z}_p[T]/(P_n(T))$;
- $\varepsilon_{p^{-1}}C(n) \cong (g_i(T))/(g_i(T)P_n(T))$;
- $\varepsilon_{p^{-1}}(U_{n,1}/C(n)) \cong \mathbb{Z}_p[[T]]/(P_n(T), g_i(T)) = \mathbb{Z}_p[T]/(P_n(T), g_i(T))$.

**Proof.** The first two items were proved in [8], chapters 13, 15.

Let us prove the third statement. It was proved in [8], chapter 15, that $P_n$ and $g_i$ have no common roots. This implies that $(P_n) \cap (g_i) = (P_n \cdot g_i)$. Thus,

$$
\varepsilon_{p^{-1}}(U_{n,1}/C(n)) \cong \frac{\mathbb{Z}_p[[T]]/(P_n(T))}{(g_i(T))/(g_i(T)P_n(T))} = \frac{\mathbb{Z}_p[[T]]/(P_n(T))}{(g_i(T))/(g_i(T) \cap P_n(T))} = 
\mathbb{Z}_p[[T]]/(P_n(T), g_i(T)).$

$\square$
This lemma enables us to give another proof of Theorem 7.3.

Let \( R = \mathbb{Z}_p[[T]]/(g_i(T)) \) and let \( M_n = R/(P_n) \) be an \( R \)-module. Clearly, the lemma above shows that \( M_n = \mathbb{Z}_p[[T]]/(P_n(T), g_i(T)) \cong \varepsilon_{p^{-i}}(U_{n,1}/C(n)) \).

Let us notice that \( P_n \) is not a zero divisor in \( R \) because \( P_n \) and \( g_i \) have distinct roots. Then multiplication by \( P_{n,k} \) determines a well-defined \( R \)-module map \( m : M_k \to M_n \) because \( m(P_k) = P_n \). It is clear that \( m \) is an embedding. Indeed, if \( m(x) = 0 \), then \( P_{n,k} \cdot x = P_n \cdot y = P_{n,k} P_k \cdot y \) for some \( y \in R \). Since \( P_{n,k} \) is not a zero divisor in \( R \), we conclude that \( x = P_k \cdot y = 0 \in M_k \).

Furthermore, let us prove that \( \{y \in M_n : P_k \cdot y = 0\} \cong M_k \). Indeed, \( P_k \cdot y = P_n \cdot z = P_k \cdot m(z) \) for some \( z \in R \) and consequently \( y = m(z) \). Since \( m \) is an embedding, the required statement follows.

The two statements above are equivalent to Theorem 7.3 formulated in terms of \( \mathbb{Z}_p[[T]] \)-modules.

At this point we remind the reader that we assume that \( p \) divides \( b_i \). Clearly, then \( p \) divides \( c_i \) and vise versa.

**Theorem 7.12.**

1. If \( p^2 \) divides \( b_i \), then \( \lambda_i = 1 \) and \( p^2 \) does not divide \( c_i \);
2. If \( p^2 \) does not divide \( b_i \) and \( 2 \leq \lambda_i \leq p - 1 \), then \( p^2 \) does not divide \( c_i \);
3. If \( p^2 \) divides \( c_i \), then \( p^2 \) does not divide \( b_i \) and \( \lambda_i = 1 \).

**Proof.**

1. We already know that \( \lambda_i = 1 \). Then \( c_i = g_i(0) = f_i(p) = b_i + pa_1 + p^2 Z_1 \), where \( p \) does not divide \( a_1 \). Then the statement is clear.

2. \( c_i = b_i + p^2 Z_2 \).

3. We already know that if \( 2 \leq \lambda_i \leq p - 1 \), then \( p^2 \) does not divide \( b_i \) and consequently it does not divide \( c_i \) as well. Hence, \( \lambda_i = 1 \). Then \( p^2 \) does not divide \( b_i \) because \( c_i = b_i + pa_1 + p^2 Z_1 \).

\[ \square \]

**Corollary 7.13.** Assume that \( p^2 \) divides \( c_i \). Then \( \varepsilon_{p^{-i}}(U_{n,1}/C(n)) \cong \mathbb{Z}/(p^{n+\lambda_i}) \) with \( l_i = v_p(c_i) \)

**Proof.** Let us perform a simple computation:

\[ \varepsilon_{p^{-i}}(U_{0,1}/C(0)) \cong \mathbb{Z}_p[[T]]/(T, g_i(T)) = \mathbb{Z}_p/(g_i(0)) = \mathbb{Z}/(p^{l_i}) = M_0. \]

We already know that \( \lambda_i = 1 \) and hence, \( M_1 \cong \mathbb{Z}/(p^k) \) for some \( k \). We have the embedding \( m : M_0 \to M_1 \) determined by the formula \( m(1_{M_0}) = ((T+1)^p/T) \).

21
1_{M_1}. Also, we have a canonical projection \( \text{res} : M_1 \to M_0, \text{res}(1_{M_1}) = 1_{M_0} \). Further, \( \text{res}(m(1_{M_0})) = \text{res}((T + 1)^p - 1/T) \cdot 1_{M_1} = p \cdot 1_{M_0} \). This computation shows that \( k = 1 + l_i \). Similar computations with \( m : M_1 \to M_2 \) and \( \text{res} : M_2 \to M_1 \) yield \( \text{res}(m(1_{M_1})) = p \cdot 1_{M_0} \) and so on.

\[ \Box \]

**Corollary 7.14.** Assume that \( p^2 \) does not divide \( c_i \) and \( 1 \leq \lambda_i < p - 1 \) Then

- \( \varepsilon_{p-i}(U_{1,1}/C(1)) \cong \mathbb{Z}/(p^2) \oplus \mathbb{F}_{p}^{\lambda_i-1} \).
- \( \varepsilon_{p-i}(U_{n,1}/C(n)) \cong \mathbb{Z}/(p^{n+1}) \oplus (\mathbb{Z}/p^n)^{\lambda_i-1} \).

**Proof.** Proofs are literally the same as the proofs of the analogous statements about the structure of the class groups in Subsection 7.2. \( \Box \)

**Remark 7.15.** Results of Subsections 7.2 and 7.3 show that the class groups \( S_{n,i} \) and the groups \( \varepsilon_{p-i}(U_{n,1}/C(n)) \) in majority of cases are dual to each other. Therefore, it is natural to conjecture that these groups are always dual to each other. However, it follows from Theorem 7.12 that if \( p^2 \) divides \( c_i \), it does not divide \( b_i \) and hence, our conjecture does not hold in this case.

Therefore, if we anyway believe in that conjecture, we have to exclude the case \( p^2 \) divides \( c_i = L_p(1, \omega^{1-i}) \). Let us do this in the next section.

### 8 \( L_p(1, \omega^{1-i}), L_p(0, \omega^{1-i}) \) are not divisible by \( p^2 \)?

#### 8.1 \( \mathcal{V} \)-duality

In this subsection we will prove the following result.

**Theorem 8.1.** Let us assume that \( \lambda_i = 1 \) and \( p^2 \) does not divide \( b_i \). Then the group \( \text{Gal}(F_1/F_0) \) acts non-trivially on \( \mathcal{V}_2^+ \).

**Remark 8.2.** In the definition of \( \mathcal{V}_2 \) (given by Kervaire and Murthy in [3]) has a natural structure a \( \text{Gal}(F_2/F_0) \)-module. However, they proved that \( \text{Gal}(F_2/F_1) \) acts on \( \mathcal{V}_2 \) trivially. Consequently, \( \mathcal{V}_2 \) is a \( \text{Gal}(F_1/F_0) \)-module.

**Proof.** Our proof is based on the main result of [3] (mentioned earlier in the paper, Theorem 1.1, however we need it in its complete form because it traces the action of \( \text{Gal}(F_2/F_0) \) or equivalently \( \text{Gal}(F_1/F_0) \)).
• Let $g$ be a generator of $G = \text{Gal}(F_1/F_0) \cong \mathbb{Z}/p\mathbb{Z}$ and let us define the following natural action of $G$ on $\mathcal{V}_2^*(g\chi)(v) = g(\chi(g^{-1}v))$, where $\chi \in \mathcal{V}_2^*, v \in \mathcal{V}_2$.

• Then $(\mathcal{V}_2^*)^*$ is isomorphic to a $G$-submodule of $S_1^{(p)}$.

• Assuming the Kervaire and Murthy conjecture that $S_1^{(p)} \cong (\mathcal{V}_2^*)^* \cong \mathbb{Z}/p^2\mathbb{Z}$, we get the formula $< gs, v > = g(< s, g^{-1}v >)$ or equivalently $g(< g^{-1}s, v >) = < s, gv >$. Here $s \in S_1^{(p)}$.

Now, let us proceed to the proof of our theorem. Clearly, without losing generality we may assume that $S_1^{(p)} = S_{1,i}$.

Then, since $\lambda_i = 1$ and $p^2$ does not divide $b_i$, our previous computations show that $S_1^{(p)} \cong \mathcal{V}_2^+ \cong \mathbb{Z}/p^2\mathbb{Z}$, i.e. the Kervaire and Murthy conjecture is true in our situation.

Let us choose $g \in G$ such that $g(\zeta_1) = \zeta_1^{1+p}$. It is well-known due to Iwasawa that the subgroup $\{ s \in S_1^{(p)} : g(s) = s \} \cong S_0^{(p)} \cong \mathbb{Z}/p\mathbb{Z}$. Therefore, $G$ acts on $S_1^{(p)}$ non-trivially and we can choose a generator $s \in S_1^{(p)}$ such that $g^{-1}(s) = s^{1+p}$. Further, we can choose a generator $v \in \mathcal{V}_2^+$ such that $< s, v > = \zeta_1$.

Suppose $G$ acts on $\mathcal{V}_2^+$ trivially. Then

$$\zeta_1 = < s, v > = < s, g(v) > = g(< g^{-1}(s), v >) = g(\zeta_1^{1+p}) = \zeta_1^{1+2p}.$$ 

Clearly, it is impossible and hence, $G$ acts on $\mathcal{V}_2^+$ non-trivially. 

\[ \square \]

### 8.2 E-duality

Let us assume that $\lambda_i = 1$ and $p^2$ does divide $c_i$.

Results of this subsection are based on Chapter 8 of [8]. Let $E$ be the group of real units of $\mathbb{Z}[\zeta_0]$ and in this subsection we denote $U_{0,1}^+$ by $U$. Since $p$ satisfies Vandiver’s conjecture, $U/(C(0))^+ = U/\bar{E}$, where $\bar{E}$ is the closure of $E$ in $U$.

Let us denote $E/E_{p^2}$ by $E_{p^2}$. It was proved in [8] that $\varepsilon_{p-i}E_{p^2} \cong \mathbb{Z}/(p^2)$ and $\varepsilon_{p-i}U/\varepsilon_{p-i}E \cong \mathbb{Z}/(p^{\nu(c_i)}) = \mathbb{Z}/(c_i)$, according to Corollary 7.13.

Let $\eta \in E$ generate $\varepsilon_{p-i}E_{p^2}$. Let us consider $\varepsilon_{p-i}(\eta) \in \varepsilon_{p-i}\bar{E}$. Since $\varepsilon_{p-i}(E/E_{p^2}) = \varepsilon_{p-i}U/\varepsilon_{p-i}E_{p^2}$ and $E_{p^2} \subset \bar{E}^{p^2}$, we see that $\eta^{-1}\varepsilon_{p-i}(\eta) \in \bar{E}^{p^2}$.

Thus $\eta = \varepsilon_{p-i}(\eta)\gamma_{p^2}$ and we obtained the following
Lemma 8.3. \( \eta \in E \) is a local \( p^2 \)-power.

Proof. \( \varepsilon_{p-i}(\eta) \) is a local \( p^2 \)-power because \( \varepsilon_{p-i}(\eta) \in \varepsilon_{p-i}\overline{E} = (\varepsilon_{p-i}U)^{\nu_i(c_i)} \) and \( \nu_i(c_i) \geq 2 \). Thus, \( \eta \in E \) is a local \( p^2 \)-power.

\[
8.3 \quad L_p(1, \omega^{1-i}) \text{ is not divisible by } p^2 ?
\]

Now we can prove the first main result of this section

Theorem 8.4. \( L_p(1, \omega^{1-i}) \) is not divisible by \( p^2 \).

Proof. Assuming that \( L_p(1, \omega^{1-i}) \) is divisible by \( p^2 \), in several steps we will come to contradiction.

- Clearly, \( \eta \) is not a \( p \)-power in the field \( F_0 \) because it generates \( \varepsilon_{p-i}(E/E_p^2) \).
- \( \eta \) is not a \( p \)-power in the field \( F_1 \) because otherwise \( F_1 = F_0(\eta^{1/p}) \) and \( F_1 \) becomes a non-ramified extension of \( F_0 \).
- Hence, the extension \( F_1(\eta^{1/p^2})/F_1 \) is non-ramified and consequently \( \eta \) induces a character of \( S_1^{(p)} \).
- Let \( E_1 \) be the subgroup of the group of units of \( \mathbb{Z}[[\zeta_1]] \) which are local \( p^2 \)-powers. Then \( E_1 \) generates a subgroup of the group of characters of \( S_1^{(p)} \). The corresponding pairing between \( S_1^{(p)} \) and \( E_1 \) satisfies \( < gs, \varepsilon > = g(< s, g^{-1}\varepsilon >) \).
- Let \( X \subseteq (S_1^{(p)})^* \cong \mathbb{Z}/(p^2) \) be the subgroup generated by \( \eta \). Comparing formulas \( < gs, \varepsilon > = g(< s, g^{-1}\varepsilon >) \) and \( < gs, v > = g(< s, g^{-1}v >) \) we can conclude that \( X \cong V_2^+ \) as \( G \)-modules.
- However, the latter is impossible because \( G \) acts trivially on \( X (\eta \in F_0) \) and non-trivially on \( V_2^+ \).

The theorem is proved.

\[
8.4 \quad L_p(0, \omega^{1-i}) \text{ is not divisible by } p^2 ?
\]

Now we can prove the second main result of this section

Theorem 8.5. \( L_p(0, \omega^{1-i}) \) is not divisible by \( p^2 \).
Proof. Assuming that $L_p(0, \omega^{1-i})$ is divisible by $p^2$, in several steps we will come to contradiction.

We remind the reader that we already know that $\lambda_i = 1$ and $c_i$ is divisible by $p$ but not by $p^2$. Let us assume first that $v_p(L_p(0, \omega^{1-i})) = v_p(b_i) = 2$. The reader will see that the general case will be possible to treat exactly in the same way.

- Since $S_{0,i} \cong \mathbb{Z}/(p^2)$ and $S_{1,i} \cong \mathbb{Z}/(p^3)$ under our assumptions, we deduce that $S^G_{1,i} \cong \mathbb{Z}/(p^2) = S^p_{1,i}$.
- Our previous computations show that $\varepsilon_{p-i} \mathcal{V}_1^+ \cong \mathbb{F}_p \cong \varepsilon_{p-i}(U_{0,1}/C(0))$ and $\varepsilon_{p-i} \mathcal{V}_2^+ \cong \mathbb{Z}/(p^2) \cong \varepsilon_{p-i}(U_{1,1}/C(1))$.
- Since there exists a canonical projection of $G$-modules $U_{1,1} \to \mathcal{V}_2^+$, we deduce that $\varepsilon_{p-i} \mathcal{V}_2^+ \cong \varepsilon_{p-i}(U_{1,1}/C(1))$ as $G$-modules.
- $(U_{1,1}/C(1)))^G \cong U_{1,1}/C(0))$ by Theorem 7.10, we see that $G$ acts on $\varepsilon_{p-i} \mathcal{V}_2^+$ non-trivially.
- By the main Kervaire–Murthy theorem (3), $(\varepsilon_{p-i} \mathcal{V}_2^+)^* \cong (S^G_{1,i})^*$ as $G$-modules.
- Let us fix $g \in G$ such that $g(\zeta_1) = \zeta_1^{1+p}$. Let us choose $v \in \varepsilon \mathcal{V}_2^+$ so that $g^{-1}(v) = v^{1+p}$ and $s \in S^G_{1,i}$ satisfying $< s, v > = \zeta_1$.
- Now, as before let us perform a simple computation:

$$< s, v > = \zeta_1 = < gs, v > = g < s, g^{-1}(v) > = g(\zeta_1^{1+p}) = \zeta_1^{1+2p}.$$ 

The latter equality is impossible and the theorem is proved. \[\square\]

### 8.5 Correction to the previous results of this section

The results of this section must be corrected. What went wrong? Let us take a look at the proof of Theorem 8.1. We chose a generator of $g \in G$ such that $g(\zeta_1) = \zeta_1^{1+p}$ and a generator $s \in S_{1,i}$ such that $g^{-1}(s) = s^{1+p}$.

Unfortunately, these two choices might be incompatible. We can only claim that $g(s) = s^{1+kp}$ with an integer $k$ defined modulo $p$. Similarly, $g(v) = v^{1+lp}$, where $v \in \mathcal{V}_2^+$ satisfies $< s, v >= \zeta_1$.

Further, since $< g(s), g(v) >= g(\zeta_1)$, we see that $k+l = 1$. Assuming that $L_p(1, \omega^{1-i})$ is divisible by $p^2$, we can deduce that $l = 0 \ mod(p)$ and hence $g(s) = s^{1+p}$. 

25
Let us consider $S_{1,i}$ as an $\mathbb{Z}_p[[T]]/(f_i(T), (1 + T)^p - 1)$-module. It follows that $T - p$ acts trivially on $S_{1,i} \cong \mathbb{Z}/(p^2)$. Since $\lambda_i = 1$, we infer that $f_i(T)$ has a root of the form $T = p + ap^2$ for some $a \in \mathbb{Z}_p$.

Furthermore, $T = (1 + p)^s - 1$ and hence $s_0 = \log_{1+p}(1 + p + ap^2) = 1 + bp$ is a zero of $L_p(s, \omega^{1-i})$. We have proved

**Theorem 8.6.** Let $\lambda_i = 1$. If $L_p(s, \omega^{1-i})$ has no zeroes of the form

$$s_0 = \log_{1+p}(1 + p + ap^2) = 1 + bp, \ b \in \mathbb{Z}_p,$$

then $L_p(1, \omega^{1-i})$ is not divisible by $p^2$.

The case $k = 0, l = 1$ can be conditionally excluded using a similar result.

**Theorem 8.7.** Let $\lambda_i = 1$. If $L_p(s, \omega^{1-i})$ has no zeroes of the form

$$s_0 = \log_{1+p}(1 + ap^2) = bp, \ b \in \mathbb{Z}_p,$$

then $L_p(0, \omega^{1-i})$ is not divisible by $p^2$.

**Remark 8.8.** The previous conditional theorem proves the Kervaire and Murthy conjecture (conditionally) with only one possible exception: $\lambda_i = p - 1$.

## 9 Conclusion remarks

The Kervaire and Murthy conjecture has another interesting form. Let us denote by $\mathbb{A}(F_n)$ the ring of adeles of the field $F_n$. Let $w$ be a valuation of $F_n$, different from $\mu_n = (1 - \zeta_n)$. Let $\mathbb{Q}_w$ be the completion of $\mathbb{Z}[\zeta_n]$ at $w$. Let us consider the following subgroup $K_{p^{n+1}-1}$ of $GL(1, \mathbb{A}(F_n))$, namely

$$K_{p^{n+1}-1} = GL(1, \mathbb{Q}) \times U_{n,p^{n+1}-1} \times \prod GL(1, \mathbb{Q}_w).$$

Then the Kervaire and Murthy conjecture can be formulated as

**Conjecture 9.1.** $(S_n^\text{−})^* \cong \{GL(1, F_n) \setminus GL(1, \mathbb{A}(F_n))/K_{p^{n+1}-1}\}^+(p)$

## 10 Afterword

This is my last paper before my retirement from the Department of Mathematical Sciences, Chalmers University of Technology/ University of Göteborg, Sweden after almost 25 years of professional service. I appreciated and enjoyed very much its friendly and calm atmosphere, which encouraged and helped me to work on the problems of my interest ”i lugn och ro.”
References

[1] Algebraic number theory. Edited by I.W.S. Cassels and A. Fröhlich, Academic Press, London, 1967.

[2] O. Helenius, A. Stolin. Fine structure of class groups and the Kervaire-Murthy conjectures. Preprint Chalmers University of Technology 2002:58, 2002:64.

[3] Kervaire, M., Murthy, M.P. On the projective class group of cyclic groups of prime power order. Comment. Math. Helv. 52 (1977), no. 3, 415-452.

[4] A. Stolin. An explicit formula for the Picard group of the cyclic group of order $p^2$. Proc. Amer. Math. Soc. 121 (1994), no. 2, 375-383.

[5] A. Stolin. On the Picard group of the integer group ring of the cyclic $p$-group and of rings close to it. Commutative ring theory, 443-455. Lecture Notes in Pure and Appl. Math., 185, Dekker, New York, 1997.

[6] A. Stolin. On the Picard group of the integer group ring of the cyclic $p$-group and certain Galois groups. I. J. Number Theory, 72 (1998), no. 1, 48-66.

[7] S. Ullom. Class group of cyclotomic fields and group rings. I. London Math. Soc. (2) 17 (1978), no. 2, 231-239.

[8] L. Washington. Introduction to cyclotomic fields. Second edition. Graduate Texts in Math., 83. Springer-Verlag, New York, 1997.