FINE STRUCTURE OF CLASS GROUPS $\mathrm{Cl}^{(p)}\,\mathbb{Q}(\zeta_n)$ AND THE KERVAIRE-MURTHY CONJECTURES

OLA HELENIUS AND ALEXANDER STOLIN

ABSTRACT. In 1977 Kervaire and Murthy presented three conjectures regarding $K_0\mathbb{Z}C_{p^n}$, where C_{p^n} is the cyclic group of order p^n and p is a semi-regular prime that is p does not divide h^+ (regular p does not divide the class number $h = h^+h^-$). The Mayer-Vietoris exact sequence provides the following short exact sequence

$$0 \to V_n \to \mathrm{Pic}\,\mathbb{Z}C_{p^n} \to \mathrm{Cl}\,\mathbb{Q}(\zeta_{n-1}) \times \mathrm{Pic}\,\mathbb{Z}C_{p^{n-1}} \to 0$$

Here ζ_{n-1} is a primitive p^n-th root of unity. The group V_n that injects into $\mathrm{Pic}\,\mathbb{Z}C_{p^n} \cong \tilde{K}_0\mathbb{Z}C_{p^n}$, is a canonical quotient of an in some sense simpler group $\mathcal{V}_n$. Both groups split in a "positive" and "negative" part. While V_n^- is well understood there is still no complete information on V_n^+. Kervaire and Murthy showed that $K_0\mathbb{Z}C_{p^n}$ and V_n are tightly connected to class groups of cyclotomic fields. They also conjectured that $V_n^+ \cong (\mathbb{Z}/p^n\mathbb{Z})^{r(p)}$, where $r(p)$ is the index of regularity of the prime p and that $\mathcal{V}_n^+ \cong V_n^+$, and moreover, $\mathrm{Char}\,\mathcal{V}_n^+ \cong \mathrm{Cl}^{(p)}\,\mathbb{Q}(\zeta_{n-1})$, the p-part of the class group.

Under an extra assumption on the prime p, Ullom proved in 1978 that $V_n^+ \cong (\mathbb{Z}/p^n\mathbb{Z})^{r(p)} \oplus (\mathbb{Z}/p^{n-1}\mathbb{Z})^{\lambda - r(p)}$, where λ is one of the Iwasawa invariants. Hence Kervaire and Murthys first conjecture holds only when $\lambda = r(p)$.

In the present paper we calculate $\mathcal{V}_n^+$ and prove that $\mathrm{Char}\,\mathcal{V}_n^+ \cong \mathrm{Cl}^{(p)}\,\mathbb{Q}(\zeta_{n-1})$ for all semi-regular primes which also gives us the structure of $\mathrm{Cl}^{(p)}\,\mathbb{Q}(\zeta_{n-1})$ as an abelian group. We also prove that under the same condition Ullom used, conjecture two always holds, that is $\mathcal{V}_n^+ \cong V_n^+$. Under the assumption $\lambda = r(p)$ we construct a special basis for a ring closely related to $\mathbb{Z}C_{p^n}$, consisting of units from a number field. This basis is used to prove that $\mathcal{V}_n^+ \cong V_n^+$ in this case and it also follows that the Iwasawa invariant ν equals $r(p)$. Moreover we conclude that $\lambda = r(p)$ is equivalent to that all three Kervaire and Murthy conjectures hold.

1. INTRODUCTION

Let p be an odd prime, C_{p^n} denote the cyclic group of order p^n and let ζ_n be a primitive p^{n+1}th root of unity. In this paper we work on the problem of finding $\mathrm{Pic}\,\mathbb{Z}C_{p^n}$. Our methods also lead to the calcultion of the p-part of the ideal

1991 *Mathematics Subject Classification.* 11R65, 11R21, 19A31.
Key words and phrases. Picard Groups, Integral Group Rings.

class group of $\mathbb{Z}[\zeta_n]$. Calculating Picard groups for a group ring like the one above is equivalent to calculating K_0 groups. Finding $K_0\mathbb{Z}G$ for various groups G was mentioned by R.G. Swan at his talk at the International Congress of Mathematicians in Nice 1970 as one of the important problems in algebraic K-theory. Of course, the reasons for this is are applications in topology. However, calculating $K_0(\mathbb{Z}G)$ seems to be pretty hard and even to this date there are no general results. Even when we restrict ourselves to $G = C_{p^n}$ no general explicit formulas are known. Several people have worked on this, though. Kervaire and Murthy presented in [K-M] an approach based on the pullback

$$\begin{array}{ccc} \mathbb{Z}C_{p^{n+1}} & \longrightarrow & \mathbb{Z}[\zeta_n] \\ \downarrow & & \downarrow \\ \mathbb{Z}C_{p^n} & \longrightarrow & \mathbb{F}_p[x]/(x^{p^n}-1) =: R_n \end{array} \tag{1.1}$$

The $(*, \mathrm{Pic})$-Mayer-Vietoris exact sequence associated to this pullback reads

$$(\mathbb{Z}C_{p^n})^* \times \mathbb{Z}[\zeta_n]^* \xrightarrow{j} R_n^* \to \operatorname{Pic}\mathbb{Z}C_{p^{n+1}} \to \operatorname{Pic}\mathbb{Z}C_{p^n} \times \operatorname{Pic}\mathbb{Z}[\zeta_n] \to \operatorname{Pic} R_n$$

Following Kervaire and Murthy, we observe that Picard groups of local rings are trivial, that the Picard group of a Dedekind ring equals the class group of the same ring and then define V_n as the co-kernel of the map j in the sequence above. Then we get

$$0 \to V_n \to \operatorname{Pic}\mathbb{Z}C_{p^{n+1}} \to \operatorname{Pic}\mathbb{Z}C_{p^n} \times \operatorname{Cl}\mathbb{Q}(\zeta_n) \to 0. \tag{1.2}$$

Kervaire and Murthy set out to calculate V_n and their approach is based on the fact that all rings involved can be acted upon by the Galois group $G_n := \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. If $s \in G_n$, let $s(\zeta_n) = \zeta_n^{\kappa(s)}$. If we represent the rings in the pullback as residue class rings of polynomials in the indeterminate X, the action is generated by $s(X) = X^{\kappa(s)}$ for all involved rings. G_n becomes a group of automorphisms of $\mathbb{Z}C_{p^{n+1}}$, $\mathbb{Z}C_{p^n}$ and R_n. The maps in the pullback above commutes with the action of G_n and the exact sequence becomes a sequence of G_n-modules. In particular, complex conjugation, which we denote by c, belongs to G_n and $c(X) = X^{-1}$. When M is a multiplicative G_n-module, like the group of units of one of the rings in the pullback, we let M^+ denote the subgroup of elements $v \in M$ such that $c(v) = v$ and M^- denote the subgroup of elements such that $c(v) = v^{-1}$. V_n is a finite abelian group of odd order and hence we have that $V_n = V_n^+ \times V_n^-$. The main result in Kervaire and Murthy's article is the following theorem

Theorem 1.1 (Kervaire and Murthy).

$$V_n^- \cong \prod_{\nu=1}^{n-1} (\mathbb{Z}/p^\nu\mathbb{Z})^{\frac{(p-1)^2 p^{n-\nu-1}}{2}}$$

and when p is semi-regular, there exists a canonical injection

$$\operatorname{Char} V_n^+ \to \operatorname{Cl}^{(p)} \mathbb{Q}(\zeta_{n-1}),$$

where $\operatorname{Cl}^{(p)} \mathbb{Q}(\zeta_{n-1})$ *is the p-primary component of the ideal class group of* $\mathbb{Q}(\zeta_{n-1})$.

The calculation of V_n^- is straightforward. Finding the information on V_n^+ turns out to be much harder. Kervaire and Murthy instead proves the result above with V_n^+ replaced by the $+$-part of

$$\mathcal{V}_n := \frac{R_n^*}{j(\mathbb{Z}[\zeta_n]^*)},$$

that is, constructs a canonical injection

$$\operatorname{Char} \mathcal{V}_n^+ \to \operatorname{Cl}^{(p)} \mathbb{Q}(\zeta_{n-1}) \tag{1.3}$$

Then, since V_n^+ is a canonical quotient of $\mathcal{V}_n^+$, 1.3 extends to an injection

$$\operatorname{Char} V_n^+ \to \operatorname{Cl}^{(p)} \mathbb{Q}(\zeta_{n-1})$$

via the canonical injection

$$\operatorname{Char} V_n^+ \to \operatorname{Char} \mathcal{V}_n^+.$$

The injection 1.3 is actually a composition of the Artin map in class field theory and a canonical injection from Iwasawa theory. The actual proof is mainly based on class field theory.

Let $r(p)$ be the index of regularity of p, that is the number of Bernoulli numbers $B_2, B_4, \ldots, B_{p-3}$ with numerators (in reduced form) divisible by p. Kervaire and Murthy formulate the following conjectures. For semi-regular primes:

$$V_n^+ = \mathcal{V}_n^+ \tag{1.4}$$

$$\operatorname{Char} \mathcal{V}_n^+ = \operatorname{Cl}^{(p)} \mathbb{Q}(\zeta_{n-1}) \tag{1.5}$$

$$\operatorname{Char} V_n^+ \cong \left(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\right)^{r(p)}, \tag{1.6}$$

When p is a regular prime it is known that $\operatorname{Cl}^{(p)} \mathbb{Q}(\zeta_{n-1})$ is trivial and hence $V_n = V_n^-$ is determined completely in [K-M].

In [U], Stephen Ullom uses Iwasawa theory and studies the action of $\operatorname{Aut} C_{p^n}$ on $\operatorname{Pic} \mathbb{Z}C_{p^n}$. He proves in that under a certain extra assumption on p, the first of Kervaire and Murthy's conjectures hold exactly when the Iwasawa invariant λ associated to p equals $r(p)$.

In this paper we use a different approach. Instead of directly studying $\mathbb{Z}C_{p^n}$ we study

$$A_n := \frac{\mathbb{Z}[x]}{\left(\frac{x^{p^n}-1}{x-1}\right)}$$

One can prove that $\operatorname{Pic}\mathbb{Z}C_{p^n} \cong \operatorname{Pic} A_n$. We then construct a pull back similar to Kervaire and Murthy's, but based on the ring A_n instead of $\mathbb{Z}C_{p^n}$. This gives us a different description of the group V_n. We then construct an injection $\alpha : \mathbb{Z}[\zeta_{n-1}]^* \to A_n^*$ and we show Kervaire and Murthy's $\mathcal{V}_n$ is isomorphic to the group

$$\frac{(A_n/pA_n)^*}{\alpha(\mathbb{Z}[\zeta_{n-1}]^*) \bmod p}.$$

In some sense this may be more natural since $\mathcal{V}_n^+$ which we want to calculate is conjectured to be isomorphic to $\mathrm{Cl}^{(p)}\,\mathbb{Q}(\zeta_{n-1})$, not $\mathrm{Cl}^{(p)}\,\mathbb{Q}(\zeta_n)$. We proceed by constructing a surjection $\mathcal{V}_n^+ \to \mathcal{V}_{n-1}^+$ and an injection $\mathcal{V}_{n-1}^+ \to \mathcal{V}_n^+$ and this allows us to show that

$$\mathcal{V}_n^+ \cong \big(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\big)^{r_0} \oplus \big(\frac{\mathbb{Z}}{p^{n-1}\mathbb{Z}}\big)^{r_1-r_0} \oplus \ldots \oplus \big(\frac{\mathbb{Z}}{p\mathbb{Z}}\big)^{r_{n-1}-r_{n-2}}$$

for all semi-regular primes. The sequence $\{r_k\}$ which we describe in section 2 is related to the order of certain groups of units in $\mathbb{Z}[\zeta_k]$.

In section 3 we then go on and prove a weak version of Kervaire and Murthys conjecture 1.5. For a group A, let $A(p) := \{a \in A \ : \ a^p = 1\}$. We prove that for semi-regular primes, $\mathrm{Cl}\,\mathbb{Q}(\zeta_{n-1})(p) \cong \mathcal{V}_n^+/(\mathcal{V}_n^+)^p$ by using Kervaire and Murthys injection $\operatorname{Char}\mathcal{V}_n^+ \to \mathrm{Cl}^{(p)}\,\mathbb{Q}(\zeta_{n-1})$ and constructing a new injection $\mathrm{Cl}\,\mathbb{Q}(\zeta_{n-1})(p) \to \operatorname{Char}\mathcal{V}_n^+$.

In section 4 we then use this weak version and results from section 2 to give a proof of Kervaire and Murthys conjecture 1.5. The proof relies on class field theory. Since we already have described the group $\mathcal{V}_n^+$ we of course also get a description of $\mathrm{Cl}^{(p)}\,\mathbb{Q}(\zeta_{n-1})$.

In section 5 we give some applications of our results. When the Iwasawa invariant λ equals $r(p)$, the index of regularity, we show that all three of Kervaire and Murthy's conjectures hold and that the Iwasawa invariant ν also equals $r(p)$. In fact, $\lambda = r(p)$ is equivalent to that all three conjectures hold.

We then move on and consider the same assumption Ullom used in [U]. We show that this leads to that $\lambda = r_1$ and prove that $V_n^+ = \mathcal{V}_n^+$ in this case too.

Finally we use our results to give some information about the structure of the group of units in $\mathbb{Z}[\zeta_n]$.

2. Preliminaries

We start this section by defining some rings that in some sense are close to $\mathbb{Z}C_{p^n}$. We discuss why we can and want to work with these rings instead of $\mathbb{Z}C_{p^n}$ and go on get an exact Mayer-Vietoris sequence from a certain pullback of these rings.

Let for $k \geq 0$ and $l \geq 1$

$$A_{k,l} := \frac{\mathbb{Z}[x]}{\left(\frac{x^{p^{k+l}}-1}{x^{p^k}-1}\right)}$$

and

$$D_{k,l} := A_{k,l} \bmod p.$$

We denote the class of x in $A_{k,l}$ by $x_{k,l}$ and in $D_{k,l}$ by $\bar{x}_{k,l}$. Sometimes we will, by abuse of notation, just denote classes by x. Note that $A_{n,1} \cong \mathbb{Z}[\zeta_n]$ and that

$$D_{k,l} \cong \frac{\mathbb{F}_p[x]}{(x-1)^{p^{k+l}-p^k}}.$$

By a generalization of Rim's theorem (see for example [ST1]) $\operatorname{Pic}\mathbb{Z}C_{p^n} \cong \operatorname{Pic} A_{0,n}$ for all $n \geq 1$ so for our purposes we can just as well work with $A_{0,n}$ instead of directly with $\mathbb{Z}C_{p^n}$. It is easy to see that there exists a pullback diagram

(2.1)
$$\begin{array}{ccc} A_{k,l+1} & \xrightarrow{i_{k,l+1}} & \mathbb{Z}[\zeta_{k+l}] \\ {\scriptstyle j_{k,l+1}}\downarrow & \swarrow{\scriptstyle N_{k,l}} & \downarrow{\scriptstyle f_{k,l}} \\ A_{k,l} & \xrightarrow{g_{k,l}} & D_{k,l} \end{array}$$

where $i_{k,l+1}(x_{k,l+1}) = \zeta_{k+l}$, $j_{k,l+1}(x_{k,l+1}) = x_{k,l}$, $f_{k,l}(\zeta_{k+l}) = \bar{x}_{k,l}$ and $g_{k,l}$ is just taking classes modulo p. The norm-maps $N_{k,l}$ will be constructed later in this paper. These maps are really the key to our methods.

The pullback 2.1 induces a Mayer-Vietoris exact sequence

$$\mathbb{Z}[\zeta_n]^* \oplus A_{0,n}^* \to D_{0,n}^* \to \operatorname{Pic} A_{0,n+1} \to \operatorname{Pic}\mathbb{Z}[\zeta_n] \oplus \operatorname{Pic} A_{0,n} \to \operatorname{Pic} D_{0,n},$$

Since $D_{0,n}$ is local, $\operatorname{Pic} D_{0,n} = 0$ and since $\mathbb{Z}[\zeta_n]$ is a Dedekind ring, $\operatorname{Pic}\mathbb{Z}[\zeta_n] \cong \operatorname{Cl}\mathbb{Q}(\zeta_n)$. By letting V_n be the cokernel

$$V_n := \frac{D_{0,n}^*}{\operatorname{Im}\{\mathbb{Z}[\zeta_n]^* \times A_{0,n}^* \to D_{0,n}^*\}}$$

we get an exact sequence

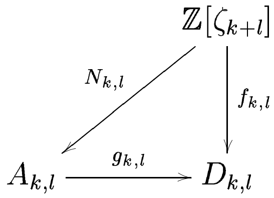
$$0 \to V_n \to \operatorname{Pic} A_{0,n+1} \to \operatorname{Cl} \mathbb{Q}(\zeta_n) \oplus \operatorname{Pic} A_{0,n} \to 0.$$

Note that definition of V_n is slightly different from the one from [K-M]. By abuse of notation, let c denote the automorphisms on $A^*_{k,l}$, $\mathbb{Z}[\zeta_n]^*$ and $D^*_{k,l}$ induced by $c(t) = t^{-1}$ for $t = x_{k,l}$, $t = \zeta_n$ and $t = \bar{x}_{k,l}$ respectively. We also denote the maps induced on $\mathcal{V}_n$ and V_n by c.

Before moving on we need to introduce the map $N_{k,l}$. An element $a \in A_{k,l+1}$ can be uniquely represented as a pair $(a_l, b_l) \in \mathbb{Z}[\zeta_{k+l}] \times A_{k,l}$. Using a similar argument on b_l, and then repeating this, we find that a can also be uniquely represented as an $(l+1)$-tuple $(a_l, \dots, a_m, \dots, a_0)$ where $a_m \in \mathbb{Z}[\zeta_{k+m}]$. In the rest of this paper we will identify an element of $A_{k,l+1}$ with both its representations as a pair or an $(l+1)$-tuple.

For $k \geq 0$ and $l \geq 1$ let $\tilde{N}_{k+l,l} : \mathbb{Z}[\zeta_{k+l}] \to \mathbb{Z}[\zeta_k]$ denote the usual norm.

Proposition 2.1. *For each $k \geq 0$ and $l \geq 1$ there exists a multiplicative map $N_{k,l}$ such that the diagram*



is commutative. Moreover, if $a \in \mathbb{Z}[\zeta_{k+l}]$, then

$$N_{k,l}(a) = (\tilde{N}_{k+l,1}(a), N_{k,l-1}(\tilde{N}_{k+l,1}(a))) = (\tilde{N}_{k+l,1}(a), \tilde{N}_{k+l,2}(a), \dots, \tilde{N}_{k+l,l}(a)).$$

The construction of $N_{k,l}$ can be found in [ST2]. Since it may not be well known we will for completeness repeat it here. Before this we notice an immediate consequence of the commutativity of the diagram in Proposition 2.1.

Corollary 2.2. $V_n = \frac{D^*_{0,n}}{\operatorname{Im}\{A^*_{0,n} \to D^*_{0,n}\}}$

Proof of Proposition 2.1. The maps $N_{k,l}$ will be constructed inductively. If $i = 1$ and k is arbitrary, we have $A_{k,1} \cong \mathbb{Z}[\zeta_k]$ and we define $N_{k,1}$ as the usual norm map $\tilde{N}_{k+1,1}$. Since $\tilde{N}_{k+1,1}(\zeta_{k+1}) = \zeta_k$ we only need to prove that our map is additive modulo p, which follows from the lemma below.

Lemma 2.3. *For $k \geq 0$ and $l \geq 1$ we have*

i) $A_{k+1,l}$ is a free $A_{k,l}$-module under $x_{k,l} \mapsto x^p_{k+1,l}$.
ii) The norm map $N : A_{k+1,l} \to A_{k,l}$, defined by taking the determinant of the multiplication operator, is additive modulo p.

This is Lemma 2.1 and Lemma 2.2 in [ST2] and proofs can be found there.

Now suppose $N_{k,j}$ is constructed for all k and all $j \leq l-1$. Let $\varphi = \varphi_{k+1,l} : \mathbb{Z}[\zeta_{k+l}] \to A_{k+1,l}$ be defined by $\varphi(a) = (a, N_{k+1,l-1}(a))$. It is clear that φ is multiplicative. From the lemma above we have a norm map $N : A_{k+1,l} \to A_{k,l}$. Define $N_{k,l} := N \circ \varphi$. It is clear that $N_{k,l}$ is multiplicative. Moreover, $N_{k,l}(\zeta_{k+l}) = N(\zeta_{k+l}, x_{k+1,l-1}) = N(x_{k+1,l}) = x_{k,l}$, where the latter equality follows by a direct computation. To prove that our map makes the diagram in the proposition above commute, we now only need to prove it is additive modulo p. This also follows by a direct calculation once you notice that

$$\varphi(a+b) - \varphi(a) - \varphi(b) = \frac{x_{k+1,l}^{p^{k+l+1}} - 1}{x_{k+1,l}^{p^{k+l}} - 1} \cdot r,$$

for some $r \in A_{k+1,l}$.

Regarding the other two equalities in Proposition 2.1, it is clear that the second one follows from the first. The first equality will follow from the lemma below.

Lemma 2.4. *The diagram*

$$\begin{array}{ccc} \mathbb{Z}[\zeta_{k+l}] & \xrightarrow{\tilde{N}_{k+l,1}} & \mathbb{Z}[\zeta_{k+l-1}] \\ {\scriptstyle N_{k,l}} \downarrow & & \downarrow {\scriptstyle N_{k-1,l}} \\ A_{k,l} & \xrightarrow{N} & A_{k-1,l} \end{array}$$

is commutative

Proof of Proposition 2.1. Recall that the maps denoted N (without subscript) are the usual norms defined by the determinant of the multiplication map. An element in $A_{k,l}$ can be represented as a pair $(a,b) \in \mathbb{Z}[\zeta_{k+l-1}] \times A_{k,l-1}$ and an element in $A_{k-1,l}$ can be represented as a pair $(c,d) \in \mathbb{Z}[\zeta_{k+l-2}] \times A_{k-1,l-1}$. If (a,b) represents an element in $A_{k,l}$ one can, directly from the definition, show that $N(a,b) = (\tilde{N}_{k+l-1,1}(a), N(b)) \in A_{k-1,l}$. We now use induction on l. If $l = 1$ the statement is well known. Suppose the diagram corresponding to the one above, but with l replaced by $l-1$, is commutative for all k. If $a \in \mathbb{Z}[\zeta_{k+l}]$ we have

$$N(N_{k,l}(a)) = N(N((a, N_{k+1,l-1}(a))) = (\tilde{N}_{k+l,2}(a), N(N(N_{k+1,l-1}(a))))$$

and

$$N_{k-1,l}(N(a)) = (\tilde{N}_{k+l,2}(a), N(N_{k,l-1}(\tilde{N}_{k+l,1}(a)))).$$

By the induction hypothesis applied to $(k+1, l-1)$ we get $N_{k,l-1} \circ \tilde{N}_{k+l,1} = N \circ N_{k+1,l-1}$ and this proves the lemma. ☐

With the proof of this Lemma the proof of Proposition 2.1 is complete. □

We will now use our the maps $N_{k,l}$ to get an inclusion of $\mathbb{Z}[\zeta_{k+l-1}]^*$ into $A^*_{k,l}$. Define $\varphi_{k,l} : \mathbb{Z}[\zeta_{k+l-1}]^* \to A^*_{k,l}$ be the injective group homomorphism defined by $\epsilon \mapsto (\epsilon, N_{k,l}(\epsilon))$. By Proposition 2.1, $\varphi_{k,l}$ is well defined. For future use we record this in a lemma.

Lemma 2.5. *Let $B_{k,l}$ be the subgroup of $A^*_{k,l}$ consisting of elements $(1, b)$, $b \in A^*_{k,l-1}$. Then $A^*_{k,l} \cong \mathbb{Z}[\zeta_{k+l-1}]^* \times B_{k,l}$*

In what follows, we identify $\mathbb{Z}[\zeta_{k+l-1}]^*$ with its image in $A^*_{k,l}$.

Before we move on we will state a technical lemma which is Theorem I.2.7 in [ST3].

Lemma 2.6. *Let $a \in \mathbb{Z}[\zeta_{k+l-1}]$. Then $g_{k,l}(a, N_{k,l-1}(a)) = 1 \in D_{k,l}$ if and only if $a \equiv 1$ mod $\lambda_{k+l-1}^{p^{k+l}-p^k}\}$. In particular,*

$$\ker(g_{k,l}|_{\mathbb{Z}[\zeta_{k+l-1}]^*}) = \{\epsilon \in \mathbb{Z}[\zeta_{k+l-1}]^* \, : \, \epsilon \equiv 1 \; mod \; \lambda_{k+l-1}^{p^{k+l}-p^k}\}$$

We will not repeat the proof here, but since the technique used is interesting we will indicate the main idea. If $a \in \mathbb{Z}[\zeta_{k+l-1}]^*$ and $g_{k,l}(a) = 1$ we get that $a \equiv 1 \bmod p$ in $\mathbb{Z}[\zeta_{k+l-1}]$, $N_{k,l-1}(a) \equiv 1 \bmod p$ in $A_{k,l-1}$ and that $f_{k,l-1}(\frac{a-1}{p}) = g_{k,l-1}(\frac{N_{k,l-1}(a)-1}{p})$. Since the norm map commutes with f and g this means that $N_{k,l-1}(\frac{a-1}{p}) \equiv \frac{N_{k,l-1}(a)-1}{p}$. The latter is a congruence in $A_{k,l-1}$ and by the same method as above we deduce a congruence in $\mathbb{Z}[\zeta_{k+l-2}]$ and a congruence in $A_{k,l-2}$. This can be repeated $l-1$ times until we get a congruence in $A_{k,1} \cong \mathbb{Z}[\zeta_k]$. The last congruence in general looks pretty complex, but can be analyzed and gives us the neccesary information.

If for example $l = 2$, we get after just one step $a \equiv 1 \bmod p$ in $\mathbb{Z}[\zeta_{k+1}]$, $N(a) \equiv 1 \bmod p$ and $N(\frac{a-1}{p}) \equiv \frac{N(a)-1}{p} \bmod p$ in $A_{k,1} \cong \mathbb{Z}[\zeta_k]$, where N is the usual norm. By viewing N as a product of automorphisms, recalling that N is additive modulo p and that the usual trace of any element of $\mathbb{Z}[\zeta_{k+1}]$ is divisible by p, we get that $N(a) \equiv 1 \bmod p^2$ and hence that $N(\frac{a-1}{p}) \equiv 0 \bmod p$. By analyzing how the norm acts one can show that this means that $a \equiv 1 \bmod \lambda_{k+1}^{p^{k+2}-p^k}$

In the rest of this paper we paper will only need the the rings $A_{k,l}$ and $D_{k,l}$ in the case $k = 0$. Therefore we will simplify the notation a little by setting $A_l := A_{0,l}$, $D_l := D_{0,l}$, $g_l := g_{0,l}$, $f_l := f_{0,l}$, $i_l := i_{0,l}$, $j_l := j_{0,l}$ and $N_l := N_{0,l}$.

Now define $\mathcal{V}_n$ as

$$\mathcal{V}_n := \frac{\tilde{D}_n^*}{\mathrm{Im}\{\tilde{\mathbb{Z}}[\zeta_{n-1}]^* \to \tilde{D}_n^*\}},$$

where $\tilde{\mathbb{Z}}[\zeta_{n-1}]^*$ are the group of all units ϵ such that $\epsilon \equiv 1 \bmod \lambda_{n-1}$, where λ_n denotes the ideal $(\zeta_n - 1)$, and $\tilde{D}_n^*$ are the units that are congruent to 1 modulo the class of $(\bar{x}-1)$ in D_n^*. This definition is equivalent to the definition in [K-M] by the following Proposition.

Proposition 2.7. *The two definitions of $\mathcal{V}_n$ coincide.*

Proof of Proposition 2.1. The kernel of the surjection $(\mathbb{F}_p[x]/(x-1)^{p^n})^* \to (\mathbb{F}_p[x]/(x-1)^{p^n-1})^* = D_n^*$ consists of units congruent to 1 mod $(x-1)^{p^n-1}$. Let $\eta := \zeta_n^{\frac{p^{n+1}+1}{2}}$. Then $\eta^2 = \zeta_n$ and $c(\eta) = \eta^{-1}$. Let $\epsilon := \frac{\eta^{p^n+1}-\eta^{-(p^n+1)}}{\eta-\eta^{-1}}$. One can by a direct calculation show that $\epsilon = 1 + (\zeta_n - 1)^{p^n-1} + t(\zeta_n-1)^{p^n}$ for some $t \in \mathbb{Z}[\zeta_n]$. If $a = 1 + a_{p^n-1}(x_n-1)^{p^n-1} \in (\mathbb{F}_p[x]/(x-1)^{p^n})^*$, $a_{p^n-1} \in \mathbb{F}_p^*$, Then it is just a matter of calculations to show that $a = f_n(\epsilon)^{a_{p^n-1}}$. This shows that $(\mathbb{F}_p[x]/(x-1)^{p^n})^*/f_n'(\mathbb{Z}[\zeta_n]^*) \cong (\mathbb{F}_p[x]/(x-1)^{p^n-1})^*/f_n(\mathbb{Z}[\zeta_n]^*)$. Since

$$\begin{array}{ccc} & & \mathbb{Z}[\zeta_n]^* \\ & \swarrow^{N} & \downarrow f \\ \mathbb{Z}[\zeta_{n-1}]^* & \xrightarrow{\;g\;} & \tilde{D}_n^{*+} \end{array}$$

is commutative and N (which is the restriction of the usual norm-map) surjective when p is semi-regular (Lemma 2.10) the proposition follows. □

Let $\mathcal{V}_n^+ := \{v \in \mathcal{V}_n \;:\; c(v) = v\}$. What we want to do is to find the structure of $\mathcal{V}_n^+$. For $n \geq 0$ and $k \geq 0$, define

$$U_{n,k} := \{real\ \epsilon \in \mathbb{Z}[\zeta_n]^* : \epsilon \equiv 1 \bmod \lambda_n^k\}.$$

One of our main results is the following proposition.

Proposition 2.8. *If p is semi-regular, $|\mathcal{V}_n^+| = |\mathcal{V}_{n-1}^+| \cdot |U_{n-1,p^n-1}/(U_{n-1,p^{n-1}+1})^p|$.*

Here U^p denotes the group of p-th powers of elements of the group U. Note that we in this paper sometimes use the notation R^n for n copies of the ring (or group) R. The context will make it clear which one of these two things we mean.

For $k = 0, 1, \ldots$, define r_k by

$$|U_{k,p^{k+1}-1}/(U_{k,p^k+1})^p| = p^{r_k}.$$

By Lemma 2 in [ST1] we get that $U_{k,p^{k+1}-1} = U_{k,p^{k+1}}$ and since the the λ_n-adic valuation of $\epsilon - 1$, where ϵ is a real unit, is even, $U_{k,p^{k+1}} = U_{k,p^{k+1}+1}$. We hence have

Lemma 2.9. $U_{k,p^{k+1}-1} = U_{k,p^{k+1}+1}$.

One can prove that $r_0 = r(p)$, the index of irregularity, since if the λ_0-adic valuation of $\epsilon \in \mathbb{Z}[\zeta_0]^{*+}$ is less than $p-1$, then local considerations show that the extension $\mathbb{Q}(\zeta_0) \subseteq \mathbb{Q}(\zeta_0, \sqrt[p]{\epsilon})$ is ramified. The result then follows from the fact that

$$\frac{U_{0,p-1}}{(U_{0,2})^p} \cong \frac{S_0}{pS_0}$$

where S_0 is the p-class group of $\mathbb{Q}(\zeta_0)$.

Before the proof of Proposition 2.8 we will state and a lemma, which is well-known.

Lemma 2.10. *If p is semi-regular $N_{n-1} : \mathbb{Z}[\zeta_{n-1}] \to A_{n-1}$ maps $U_{n-1,1}$ surjectively onto $U_{n-2,1}$.*

Proof of Proposition 2.8. In a similar way as the ideal $\lambda_n := (\zeta_n - 1)$ equal the ideal $(\zeta_n - \zeta_n^{-1})$ in $\mathbb{Z}[\zeta_n]$ one can show that that $(\bar{x} - 1) = (\bar{x} - \bar{x}^{-1})$ in D_n. It is easy to show that $\tilde{D}_n^{*+}$ can be represented by elements $1 + a_2(\bar{x} - \bar{x}^{-1})^2 + a_4(\bar{x} - \bar{x}^{-1})^4 + \ldots + a_{p^n-3}(x - x^{-1})^{p^n-3}$, $a_i \in \mathbb{F}_p$. Hence $|\tilde{D}_n^{*+}| = p^{(p^n-3)/2}$. We want to evaluate

$$|\tilde{D}_n^{*+}|/|g_n(U_{n-1,1})|.$$

By Lemma 2.6 we have

$$g_n(U_{n-1,1}) \cong \frac{U_{n-1,1}}{U_{n-1,p^n-1}}.$$

Since $g_n(U_{n-1,1}) \subseteq g_n(\mathbb{Z}[\zeta_{n-1}]^{*+}) \subseteq \tilde{D}_n^{*+}$ the group $U_{n-1,1}/U_{n-1,p^n-1}$ is finite. Similarly $\mathbb{Z}[\zeta_{n-1}]^{*+}/U_{n-1,p^n-1}$ is finite. This shows that $\mathbb{Z}[\zeta_{n-1}]^{*+}/U_{n-1,1}$ is finite since

$$|\frac{\mathbb{Z}[\zeta_{n-1}]^{*+}}{U_{n-1,1}}||\frac{U_{n-1,1}}{U_{n-1,p^n-1}}| = |\frac{\mathbb{Z}[\zeta_{n-1}]^{*+}}{U_{n-1,p^n-1}}|.$$

We can write

$$(2.2)\qquad \begin{aligned} |\frac{U_{n-1,1}}{U_{n-1,p^n-1}}| &= |\frac{U_{n-1,1}}{U_{n-1,p^{n-1}-1}}||\frac{U_{n-1,p^{n-1}-1}}{U_{n-1,p^{n-1}+1}}||\frac{U_{n-1,p^{n-1}+1}}{U_{n-1,p^n-1}}| = \\ &= |\frac{U_{n-1,1}}{U_{n-1,p^{n-1}-1}}||\frac{U_{n-1,p^{n-1}-1}}{U_{n-1,p^{n-1}+1}}||\frac{U_{n-1,p^{n-1}+1}/(U_{n-1,p^{n-1}+1})^p}{U_{n-1,p^n-1}/(U_{n-1,p^{n-1}+1})^p}| = \\ &= |\frac{U_{n-1,1}}{U_{n-1,p^{n-1}-1}}||\frac{U_{n-1,p^{n-1}-1}}{U_{n-1,p^{n-1}+1}}||\frac{U_{n-1,p^{n-1}+1}}{(U_{n-1,p^{n-1}+1})^p}||\frac{U_{n-1,p^n-1}}{(U_{n-1,p^{n-1}+1})^p}|^{-1} \end{aligned}$$

By Dirichlet's theorem on units we have $(\mathbb{Z}[\zeta_{n-1}]^*)^+ \cong \mathbb{Z}^{\frac{p^n-p^{n-1}}{2}-1}$ Since all quotient groups involved are finite we get that $U_{n-1,1}$, U_{n-1,p^n-1}, $U_{n-1,p^{n-1}-1}$ and $U_{n-1,p^{n-1}+1}$ are all isomorphic to $\mathbb{Z}^{\frac{p^n-p^{n-1}}{2}-1}$. The rest of the proof is devoted to the analysis of the four right hand factors of 2.2.

Obviously,

$$\frac{U_{n-1,p^{n-1}+1}}{(U_{n-1,p^{n-1}+1})^p} \cong \frac{\mathbb{Z}^{\frac{p^n-p^{n-1}}{2}-1}}{(p\mathbb{Z})^{\frac{p^n-p^{n-1}}{2}-1}} \cong C_p^{\frac{p^n-p^{n-1}}{2}-1}.$$

This shows that

$$|\frac{U_{n-1,p^{n-1}+1}}{(U_{n-1,p^{n-1}+1})^p}| = p^{\frac{p^n-p^{n-1}}{2}-1}.$$

We now turn to the second factor of the right hand side of 2.2. We will show that this number is p by finding a unit $\epsilon \notin U_{p^{n-1}+1}$ such that

$$< \epsilon >= \frac{U_{n-1,p^{n-1}-1}}{U_{n-1,p^{n-1}+1}}.$$

Since the p-th power of any unit in $U_{n-1,p^{n-1}-1}$ belongs to $U_{n-1,p^{n-1}+1}$ this is enough. Let $\zeta = \zeta_{n-1}$ and $\eta := \zeta^{\frac{p^n+1}{2}}$. Then $\eta^2 = \zeta$ and $c(\eta) = \eta^{-1}$. Let $\epsilon := \frac{\eta^{p^{n-1}+1}-\eta^{-(p^{n-1}+1)}}{\eta-\eta^{-1}}$. Then $c(\epsilon) = \epsilon$ and one can by direct calculations show that ϵ is the unit we are looking for.

We now want to calculate

$$|\frac{U_{n-1,1}}{U_{n-1,p^{n-1}-1}}|.$$

Consider the commutative diagram

$$\begin{array}{ccc} & & \mathbb{Z}[\zeta_{n-1}]^* \\ & \swarrow^{N_{n-1}} & \downarrow f_{n-1} \\ A^*_{n-1} & \xrightarrow{g_{n-1}} & D^*_{n-1} \end{array}$$

It is clear that $f_{n-1}(U_{n-1,1}) \subseteq \tilde{D}^{*+}_{n-1}$ and that $g_{n-2}(U_{n-2,1}) \subseteq \tilde{D}^{*+}_{n-1}$. By Lemma 2.10 we have a commutative diagram

$$\begin{array}{ccc} & & U_{n-1,1} \\ & \swarrow^{N} & \downarrow f \\ U_{n-2,1} & \xrightarrow{g} & \tilde{D}^{*+}_{n-1} \end{array}$$

where N is surjective. Clearly, $f(U_{n-1,1}) = g(U_{n-2,1})$.

It is easy to see that $\ker(f) = U_{n-1,p^{n-1}-1}$ so by above

$$\frac{U_{n-1,1}}{U_{n-1,p^{n-1}-1}} \cong f(U_{n-1,1}) = g(U_{n-2,1}).$$

Now recall that by definition $\mathcal{V}^+_{n-1} = \tilde{D}^{*+}_{n-1}/g(U_{n-2,1})$. Hence

$$\left|\frac{U_{n-1,1}}{U_{n-1,p^{n-1}-1}}\right| = |g(U_{n-2,1})| = |\tilde{D}^{*+}_{n-1}||\mathcal{V}^+_{n-1}|^{-1} = p^{\frac{p^{n-1}-3}{2}}|\mathcal{V}^+_{n-1}|^{-1}.$$

This finally gives

$$\begin{aligned} |\mathcal{V}^+_n| &= |\tilde{D}^{*+}_n||g(U_{n-1,1})|^{-1} = \\ &= p^{\frac{p^n-3}{2}} \cdot p^{-\frac{p^{n-1}-3}{2}} \cdot |\mathcal{V}^+_{n-1}| \cdot p^{-1} \cdot p^{-\frac{p^n-p^{n-1}}{2}+1} \cdot \left|\frac{U_{n-1,p^n-1}}{(U_{n-1,p^{n-1}+1})^p}\right| = \\ &= |\mathcal{V}^+_{n-1}| \cdot \left|\frac{U_{n-1,p^n-1}}{(U_{n-1,p^{n-1}+1})^p}\right| \end{aligned}$$

which is what we wanted to show.

□

Proposition 2.11. *The sequence $\{r_k\}$ is non-decreasing, bounded by the Iwasawa invariant λ and $|\mathcal{V}^+_n| = p^{r_0+r_1+\ldots+r_{n-1}}$.*

Proof of Proposition 2.8. Recall that $(\lambda_k) = (\lambda^p_{k+1})$ as ideals in $\mathbb{Z}[\zeta_{k+1}]$. By Lemma 2.9, the inclusion of $\mathbb{Z}[\zeta_k]$ in $\mathbb{Z}[\zeta_{k+1}]$ induces an inclusion of $U_{k,p^{k+1}-1} =$

$U_{k,p^{k+1}+1}$ into $U_{k+1,p^{k+2}+p} \subseteq U_{k+1,p^{k+2}-1}$. Since a p-th power in $\mathbb{Z}[\zeta_k]$ obviously is a p-th power in $\mathbb{Z}[\zeta_{k+1}]$ we get an homomorphism of

$$\frac{U_{k,p^{k+1}-1}}{(U_{k,p^k+1})^p} \to \frac{U_{k+1,p^{k+2}-1}}{(U_{k+1,p^{k+1}+1})^p}. \tag{2.3}$$

If $\epsilon \in U_{k,p^{k+1}-1}$ is a not p-th power in $\mathbb{Z}[\zeta_k]$ then one can show that $\mathbb{Q}(\zeta_k) \subseteq \mathbb{Q}(\zeta_k, \epsilon)$ is an unramified extension of degree p. If ϵ would be a p-th power in $\mathbb{Z}[\zeta_{k+1}]$ we would get $\mathbb{Q}(\zeta_{k+1}) = \mathbb{Q}(\zeta_k, \epsilon)$ which is impossible since $\mathbb{Q}(\zeta_k) \subseteq Q(\zeta_{k+1})$ is ramified. Hence the homomorphism 2.3 is injective. This shows that the sequence $\{r_k\}$ is non-decreasing.

Since it is known by for example [K-M] that $|\mathcal{V}_1^+| = p^{r_0}$, by induction and Proposition 2.8 we now immediately get: $|\mathcal{V}_n^+| = p^{r_0+r_1+\ldots+r_{n-1}}$.

Assume now that $r_N > \lambda$ for some N. Then it follows that $|\mathcal{V}_n^+|$ grows faster than $p^{\lambda n}$ and this contradicts to that of $|\mathcal{V}_n^+| < |\operatorname{Cl}^{(p)} \mathbb{Q}(\zeta_n)| = p^{\lambda n+\nu}$. This observation completes the proof. □

We now go on and prove the following proposition:

Proposition 2.12. *There exists a surjection* $\pi_n : \mathcal{V}_n^+ \to \mathcal{V}_{n-1}^+$.

Proof of Proposition 2.8. The canonical surjection $j_n : A_n \to A_{n-1}$ can be considered mod (p) and hence yields a surjection $\bar{j}_n : D_n \to D_{n-1}$. Suppose that $\bar{u} \in D_{n-1}^{*+}$, $\bar{v} \in D_n^{*+}$, $\bar{j}_n(\bar{v}) = \bar{u}$ and that $\bar{v} = g_n(v)$, where $v = (\epsilon, N_{n-1}(\epsilon))$, $\epsilon \in \mathbb{Z}[\zeta_{n-1}]$. Then $j_n(v) = N_{n-1}(\epsilon)$, and $\bar{u} = \bar{j}_n(\bar{v}) = \bar{j}_n g_n N_{n-1}(\epsilon)$. But $N_{n-1}(\epsilon) = (\tilde{N}_{n-1,1}(\epsilon), N_{n-2}\tilde{N}_{n-1,1}(\epsilon))$ by Proposition 2.1. In other words, if $\bar{v}$ represents 1 in $\mathcal{V}_n$, then $\bar{j}_n(\bar{v})$ represents 1 in $\mathcal{V}_{n-1}$ so the map $\bar{j}_n$ induces a well defined surjection $\mathcal{V}_n^+ \to \mathcal{V}_{n-1}^+$. □

It is now not hard to find the kernal of π_n.

Proposition 2.13. *For any semi-regular prime p,* $\ker \pi_n \cong (\mathbb{Z}/p\mathbb{Z})^{r_{n-1}}$.

Proof. Proposition 2.8 and the definition of r_n clearly implies that $|\ker \pi_n| = p^{r_{n-1}}$. We need to prove that any element in $\ker \pi_n$ has order at most p. Suppose that in the surjection $D_n^{*+} \to D_{n-1}^{*+}$, the element $u \in D_{n-1}^{*+}$ is the image of $v \in D_n^{*+}$ and suppose $u = g_{n-1}((\epsilon, N_{n-2}(\epsilon)))$ for some $\epsilon \in U_{n-2,1} \subset \mathbb{Z}[\zeta_{n-2}]$. For some $a \in A_n$, $v = g_n(a)$ and $(\epsilon, N_{n-2}(\epsilon)) = j_n(a)$. Since p is semi-regular we know from Lemma 2.10 that the norm map N_{n-1} resticted to $U_{n-1,1}$ is surjective onto $U_{n-2,1}$ and acts as the usual norm $\tilde{N}_{n-1,1}$. Hence there exists $\epsilon' \in U_{n-1,1}$ such that $N_{n-1}(\epsilon') = (\epsilon, N_{n-2}(\epsilon))$. This means that $(\epsilon', N_{n-1}(\epsilon')) \in A_n^{*+}$ maps to $(\epsilon, N_{n-2}(\epsilon))$ under j_n. Since $f_{n-1}(\epsilon') = g_{n-1}N_{n-1}(\epsilon') = u$ and all the maps come from a pullback we get that $a = (\epsilon', N_{n-1}(\epsilon'))$, that is, v is the image of a unit in $U_{n-1,1}$. Now define $\tilde{D}^{*+}_{n,(k)} := \{a \in \tilde{D}^{*+}_n : a \equiv 1 \bmod (x-1)^k\}$. Then

$$\ker \pi_n = \frac{\ker\{\tilde{D}^{*+}_n \to \tilde{D}^{*+}_{n-1}\}}{\ker\{\tilde{D}^{*+}_n \to \tilde{D}^{*+}_{n-1}\} \cap g_n(\mathbb{Z}[\zeta_{n-1}]^{*+})} = \frac{\tilde{D}^{*+}_{n,(p^{n-1}-1)}}{g_n(U_{n-1,p^{n-1}-1})}.$$

Now note that if $b \in \tilde{D}^{*+}_{n,(p^{n-1})}$, then $b^p = 1$ so such a unit clearly has order p. We will show that any unit $a \in \tilde{D}^{*+}_{n,(p^{n-1}-1)}$ can be written as $a = bg_n(\epsilon)^k$ for some $b \in \tilde{D}^{*+}_{n,(p^{n-1})}$, natural number k and $\epsilon \in U_{n-1,p^{n-1}-1}$. Then $a^p = b^p g_n(\epsilon)^{kp}$ is clearly trivial in $\ker \pi_n \subseteq \mathcal{V}^+_n$. Let $\eta := \zeta_{n-1}^{\frac{p^n+1}{2}}$. Then $\eta^2 = \zeta_{n-1}$ and $c(\eta) = \eta^{-1}$. Let $\epsilon := \frac{\eta^{p^{n-1}+1} - \eta^{-(p^{n-1}+1)}}{\eta - \eta^{-1}}$. One can by a direct calculation show that $\epsilon \in U_{n-1,p^{n-1}-1} \setminus U_{n-1,p^{n-1}+1}$. In fact, $\epsilon = 1 + e_{p^{n-1}-1}(\zeta_{n-1} - \zeta_{n-1}^{-1})^{p^{n-1}-1} + t(\zeta_{n-1} - \zeta_{n-1}^{-1})^{p^{n-1}+1}$ for some non-zero $e_{p^{n-1}-1} \in \mathbb{Z}[\zeta_{n-2}]$, not divisible by λ_{n-1}, and some $t \in \mathbb{Z}$. Suppose $a = 1 + a_{p^{n-1}-1}(x_{n-1} - x_{n-1}^{-1})^{p^{n-1}-1} + \ldots \in \tilde{D}^{*+}_{n,(p^{n-1}-1)}$, $a_{p^{n-1}-1} \in \mathbb{F}_p^*$. Since $e_{p^{n-1}-1}$ is not divisible by λ_{n-1}, $g_n(\epsilon) \in \mathbb{F}_p^*$ Hence we can choose k such that $kg_n(e_{p^{n-1}-1}) \equiv a_{p^{n-1}-1} \bmod p$. Then it is just a matter of calculations to show that $a = bg_n(\epsilon)^k$, where $b \in \tilde{D}^{*+}_{n,(p^{n-1})}$, which concludes the proof □

One of our main theorems is the following:

Theorem 2.14. *For every semi-regular prime p*

$$\mathcal{V}^+_n \cong \Big(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\Big)^{r_0} \oplus \Big(\frac{\mathbb{Z}}{p^{n-1}\mathbb{Z}}\Big)^{r_1 - r_0} \oplus \ldots \oplus \Big(\frac{\mathbb{Z}}{p\mathbb{Z}}\Big)^{r_{n-1}-r_{n-2}}.$$

To prove this we need to introduce some techniques from [K-M].

Let $P_{0,n}$ be the group of principal fractional ideals in $\mathbb{Q}(\zeta_n)$ prime to λ_n. Let H_n be the subgroup of fractional ideals congruent to 1 modulo $\lambda_n^{p^n}$. In [K-M], p. 431, it is proved that there exists a canonical isomorphism

$$J : \frac{P_{0,n}}{H_n} \to \frac{(\mathbb{F}_p[x]/(x-1)^{p^n})^*}{f'_n(\mathbb{Z}[\zeta_n]^*)} =: \mathcal{V}'_n.$$

Now consider the injection $\iota : \mathbb{Q}(\zeta_{n-1}) \to \mathbb{Q}(\zeta_n)$, $\zeta_{n-1} \mapsto \zeta_n^p$. It is clear we get an induced map $P_{0,n-1} \to P_{0,n}$. Since ι map λ_{n-1} to λ_n^p it is easy to see that we get an induced homomorphism

$$\alpha'_n : \frac{P_{0,n-1}}{H_{n-1}} \to \frac{P_{0,n}}{H_n}.$$

Considered as a map $\alpha'_n : \mathcal{V}'_{n-1} \to \mathcal{V}'_n$ this map acts as $(\mathbb{F}_p[x]/(x-1)^{p^{n-1}})^* \ni x_{n-1} \mapsto x_n^p \in (\mathbb{F}_p[x]/(x-1)^{p^n})^*$. Since $\mathcal{V}'_n \cong \mathcal{V}_n$ (see Proposition 2.7) we can consider this as a homomorphism $\alpha_n : \mathcal{V}_{n-1} \to \mathcal{V}_n$. Clearly we then get that

α is induced by $x_{n-1} \to x_n^p$ Note however, that $x_{n-1} \mapsto x_n^p$ does not induce a homomorphism $D_{n-1}^* \to D_n^*$.

Lemma 2.15. *The map α_n is injective on $\mathcal{V}_{n-1}^+$.*

Proof. In this proof, denote $\mathbb{Q}(\zeta_n)$ by F_n. Let L_n be the p-part of the Hilbert class field of F_n and let K_n/F_n be the p-part of the ray class field extension associated with the ray group H_n. In other words we have the following Artin map

$$\Phi_{F_n} : \; I_0(F_n) \to \mathrm{Gal}(K_n/F_n),$$

which induces an isomorphism $(I_0(F_n)/H_n)_p \to \mathrm{Gal}(K_n/F_n)$. Here $I_0(F_n)$ is the group of ideals of F_n which are prime to λ_n, and $(I_0(F_n)/H_n)_p$ is the p-component of $I_0(F_n)/H_n$.

The following facts were proved in [K-M]:

$$1) \;\; \mathrm{Gal}^+(K_n/F_n) \cong \mathrm{Gal}^+(K_n/L_n) \cong \mathcal{V}_n^+$$

$$2) \;\; K_{n-1} \cap F_n = F_{n-1} \text{ (lemma 4.4)}.$$

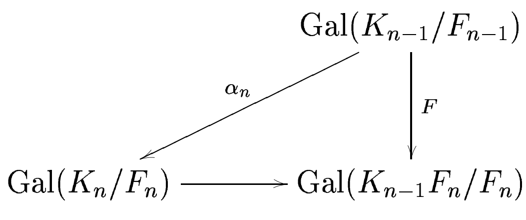
Obviously the field extension F_n/F_{n-1} induces a natural homomorphism

$$\mathrm{Gal}(K_{n-1}/F_{n-1}) \cong (I_0(F_{n-1})/H_{n-1})_p \to (I_0(F_n)/H_n)_p \cong \mathrm{Gal}(K_n/F_n)$$

which we denote with some abuse of notations by α_n. Therefore it is sufficient to prove that the latter α_n is injective. First we note that the natural map $F : \; \mathrm{Gal}(K_{n-1}/F_{n-1}) \to \mathrm{Gal}(K_{n-1}F_n/F_n)$ is an isomorphism. Let us prove that $K_{n-1}F_n \subset K_n$. Consider the Artin map $\Phi'_{F_n} : \; I_0(F_n) \to \mathrm{Gal}(K_{n-1}F_n/F_n)$ (of course F is induced by the canonical embedding $I_0(F_{n-1}) \to I_0(F_n)$). We have to show that the kernel of Φ'_{F_n} contains H_n.

To see this note that $F^{-1}(\Phi'_{F_n}(s)) = \Phi_{F_{n-1}}(N_{F_n/F_{n-1}}(s))$ for any $s \in I_0(F_n)$. If $s \in H_n$ then without loss of generality $s = 1 + \lambda_n^{p^n} t$, $t \in \mathbb{Z}[\zeta_n]$, and thus, $N_{F_n/F_{n-1}}(s)) = 1 + pt_1$ for some $t_1 \in \mathbb{Z}[\zeta_{n-1}]$. Now it is clear that $\Phi'_{F_n}(s) = id_{K_n}$ since $\Phi_{F_{n-1}}(1 + pt_1) = id_{K_{n-1}}$.

It follows that the identical map $id : \; I_0(F_n) \to I_0(F_n)$ induces the canonical Galois surjection $\mathrm{Gal}(K_n/F_n) \to \mathrm{Gal}(K_{n-1}F_n/F_n)$ and we have the following commutative diagram:



If $\alpha_n(a) = id$ then $F(a) = id$ and $a = id$ because F is an isomorphism which proves the lemma. $\square$

Proof of Theorem 2.14. Induction with respect to n. If $n = 1$ the result is known from for example [K-M]. Suppose the result holds with the index equal to $n-1$. Proposition 2.12 tells us that we have a surjection $\pi_n : \mathcal{V}_n^+ \to \mathcal{V}_{n-1}^+$ and Proposition 2.13 that $\ker \pi_n$ isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{r_{n-1}}$. Suppose $1 + (x_{n-1} - 1)^k$ is non-trivial in $\mathcal{V}_{n-1}^+$. Since

$$\begin{array}{ccc} \mathbb{Z}[\zeta_{n-1}]^{*+} & \longrightarrow & D_n^{*+} \\ \Big\downarrow{\scriptstyle \tilde{N}_{n,1}} & & \Big\downarrow \\ \mathbb{Z}[\zeta_{n-2}]^{*+} & \longrightarrow & D_{n-1}^{*+} \end{array} \tag{2.4}$$

is commutative, $1 + (x_n - 1)^k$ is non-trivial in $\mathcal{V}_n^+$. Moreover, since α_n is injective,

$$\alpha(1 + (x_{n-1} - 1)^k) = 1 + (x_n^p - 1)^k = (1 + (x_n - 1)^k)^p$$

is non-trivial in $\mathcal{V}_n^+$. Now let $1 + (x_{n-1} - 1)^{s_i}$ generate $\mathcal{V}_{n-1}^+$ and suppose $\pi_n(a_i) = 1 + (x_{n-1} - 1)^{s_i}$. Since $\pi_n(1 + (x_n - 1)^{s_i}) = 1 + (x_{n-1} - 1)^{s_i}$ we get $a_i = b_i(1 + (x_n - 1)^{s_i})$ for some $b_i \in \ker \pi_n$, which implies that b_i^p is trivial. Suppose $1 + (x_{n-1} - 1)^{s_i}$ has exponent p^k for some $1 \leq k \leq n-1$. To prove the theorem we need to prove that a_i has exponent p^{k+1}. Since $\ker \pi_n \cong (\mathbb{Z}/p\mathbb{Z})^{r_{n-1}}$, a_i has exponent less than or equal to p^{k+1}. But $(1 + (x_{n-1} - 1)^{s_i})^{p^k} = 1 + (x_{n-1} - 1)^{p^k s_i}$ is non-trivial in $\mathcal{V}_{n-1}^+$ so

$$a_i^{p^{k+1}} = b_i^{p^{k+1}}(1 + (x_n - 1)^{s_i})^{p^{k+1}} = (1 + (x_n - 1)^{s_i})^{p^{k+1}}$$

is non-trivial in $\mathcal{V}_n^+$ by above, which is what we needed to show $\square$

3. A Weak Version of the Kervaire-Murthy Conjecture

In this section we will prove that $\mathrm{Cl}\,\mathbb{Q}(\zeta_{n-1})(p) \cong \mathcal{V}_n^+/(\mathcal{V}_n^+)^p$. Here $A(p) := \{x \in A : x^p = 1\}$. It follows from Theorem 2.14 that $\mathcal{V}_n^+/(\mathcal{V}_n^+)^p$ has r_{n-1} generators, and it was proved in [K-M] that $\mathrm{Char}\,\mathcal{V}_n^+$ can be embedded into $\mathrm{Cl}^{(p)}\,\mathbb{Q}(\zeta_{n-1})$.

So, in order to prove the result we need, it suffices to prove the following

Theorem 3.1. *There exists an embedding* $\mathrm{Cl}\,\mathbb{Q}(\zeta_{n-1})(p) \to \mathrm{Char}\,\mathcal{V}_n^+$.

Proof. First note that all our maps, g_n, j_n, N_n etc and rings A_n and can be extended p-adically. Let $A_{n,(p)}$ be defined by

$$A_{n,(p)} := \frac{\mathbb{Z}_p[x]}{\left(\frac{x^{p^n}-1}{x-1}\right)},$$

where $\mathbb{Z}_p$ denotes the ring of p-adic integers. We have a commutative diagram

(3.1)
$$\begin{array}{ccc} A_{n,(p)} & \xrightarrow{i_n} & \mathbb{Z}_p[\zeta_{n-1}] \\ \downarrow j_n & \swarrow N_{n-1} & \downarrow f_{n-1} \\ A_{n-1,(p)} & \xrightarrow{g_{n-1}} & D_{n-1} \end{array}$$

Let $U_{n,k,(p)} := \{real\, \epsilon \in \mathbb{Z}_p[\zeta_n]^* \,:\, \epsilon \equiv 1 \bmod \lambda_n^k\}$ Considering pairs $(a, N_{n-1}(a))$, where $a \in \mathbb{Z}_p[\zeta_{n-1}]$, we can embed $\mathbb{Z}_p[\zeta_{n-1}]^*$ into $A^*_{n,(p)}$. In [S2] it was proved that D_n^* is isomorphic to $\mathbb{Z}_p[\zeta_{n-1}]^*/U_{n-1,p^n-1,(p)}$ (see also Lemma 2.6). We hence have the following proposition

Proposition 3.2.

$$\mathcal{V}_n \cong \frac{\mathbb{Z}_p[\zeta_{n-1}]^*}{U_{n-1,p^n-1,(p)} \cdot g_n(\mathbb{Z}[\zeta_{n-1}]^*)}.$$

Now for any valuation ω of $F_{n-1} = \mathbb{Q}(\zeta_{n-1})$ and any $a, b \in \mathbb{Q}(\zeta_{n-1})^*$ we have the norm residue symbol $(a,b)_\omega$ with values in the group of p-th (not p^n) roots of unity. Let $\omega = \lambda_{n-1} = (\zeta_{n-1} - \zeta_{n-1}^{-1})$ and let $\eta_k = 1 - \lambda_{n-1}^k$. Then

$$(\eta_i, \eta_j)_{\lambda_{n-1}} = (\eta_i, \eta_{i+j})_{\lambda_{n-1}} (\eta_{i+j}, \eta_j)_{\lambda_{n-1}} (\eta_{i+j}, \lambda_{n-1})^{-j}_{\lambda_{n-1}}$$

It follows that $(a,b)_{\lambda_{n-1}} = 1$ if $a \in U_{n-1,k}$, $b \in U_{n-1,s}$ and $k + s > p^n$. Further, $(\eta_{p^n}, \lambda_{n-1})_{\lambda_{n-1}} = \zeta_0$ and therefore $(\eta_i, \eta_j)_{\lambda_{n-1}} \neq 1$ if $i + j = p^n$, j is co-prime to p.

Let α be an ideal in $\mathbb{Z}[\zeta_{n-1}]$ co-prime to λ_{n-1} and such that $\alpha^p = (q)$, where $q = 1 + \lambda_{n-1}^2 t \in \mathbb{Z}[\zeta_{n-1}]$ (we can choose such q since $\zeta_{n-1} = 1 + \lambda_{n-1}\zeta_{n-1}(1+\zeta_{n-1})^{-1}$ and $\zeta_{n-1}(1+\zeta_{n-1})^{-1} \in \mathbb{Z}[\zeta_{n-1}]^*$). Define the following action of $\mathrm{Cl}\,\mathbb{Q}(\zeta_{n-1})(p)$ on $U^+_{n-1,2,(p)}$:

$$\tau_\alpha(v) = (v, q)_{\lambda_{n-1}}$$

Let us prove that this action is well-defined. First of all it is independent of the choice of the representative α in $\mathrm{Cl}\,\mathbb{Q}(\zeta_{n-1})(p)$ because if we use $r\alpha$ instead of α then $(v, r^p q)_{\lambda_{n-1}} = (v, q)_{\lambda_{n-1}}$.

The action is independent of the choice of q by the following reason: another generator of α^p, which is 1 modulo λ_{n-1}^2, differs from "the old" q by some unit $\gamma = 1 + \lambda_{n-1}^2 t_1$, and it can be easily verified that γ is either real or $\gamma = \zeta_{n-1}^{pk}\gamma_1$

with a real unit γ_1. Hence we must consider $\tau_{\gamma q}(v)$ for real γ. In other words we have to prove that $(v,\gamma)_{\lambda_{n-1}} = 1$. But if the latter is untrue, then $(v,\gamma)_{\lambda_{n-1}} = \zeta_0$, which is not consistent with the action of the "complex conjugation" (v and γ are real, while ζ_0 is not real).

Clearly $(U_{n-1,p^n-1,(p)}, q)_{\lambda_{n-1}} = 1$. It remains to prove that $(\gamma, q)_{\lambda_{n-1}} = 1$ for any unit γ and we will obtain an action of $\mathrm{Cl}\,\mathbb{Q}(\zeta_{n-1})(p)$ on $\mathcal{V}_n^+$. For this consider a field extension $F_{n-1}(q^{1/p})/F_{n-1}$. Since $(q) = \alpha^p$, it can remify in the λ_{n-1} only. Then clearly $(\gamma, q)_\omega = 1$ for any $\omega \neq \lambda_{n-1}$ and it follows from the product formula that $(\gamma, q)_{\lambda_{n-1}} = 1$.

Therefore $\mathrm{Cl}\,\mathbb{Q}(\zeta_{n-1})(p)$ acts on $\mathcal{V}_n^+$ and obviously $\tau_{\alpha\beta} = \tau_\alpha\tau_\beta$.

The last stage is to prove that any $\alpha \in \mathrm{Cl}\,\mathbb{Q}(\zeta_{n-1})(p)$ acts non-trivially on $\mathcal{V}_n^+$. Let $(q) = \alpha^p$ and let $q = 1 + \lambda_{n-1}^k t$ with some $k > 1$ and t, co-prime to λ_{n-1}.

Let us prove that $k < p^n - 1$. Assume that $k > p^n - 1$. Then the field extension $F_{n-1}(q^{1/p})/F_{n-1}$ is unramified. It is well-known that if p is semi-regular, then $F_{n-1}(q^{1/p}) = F_{n-1}(\gamma^{1/p})$ for some unit γ. Kummer's theory says that $q = \gamma r^p$ and then obviously $\alpha = (r)$, i.e. α is a principal ideal. So, it remains to prove that the case $k = p^n - 1$ is impossible. For this consider ζ_{n-1} and take into account that $\zeta_{n-1} = 1 + \lambda_{n-1}\zeta_{n-1}(1 + \zeta_{n-1})^{-1}$. Then clearly it follows from the properties of the local norm residue symbol $(\, , \,)_{\lambda_{n-1}}$ that $(\zeta_{n-1}, q)_{\lambda_{n-1}} \neq 1$. On the other hand $(\zeta_{n-1}, q)_\omega = 1$ for any $\omega \neq \lambda_{n-1}$ because ζ_{n-1} is a unit and the extension $F_{n-1}(q^{1/p})/F_{n-1}$ is unramified in ω. Therefore $(\zeta_{n-1}, q)_{\lambda_{n-1}} = 1$ by the product formula and the case $k = p^n - 1$ is impossible and $k < p^n - 1$.

Now let us consider the cyclic subgroup of $\mathrm{Cl}\,\mathbb{Q}(\zeta_{n-1})(p)$ generated by α and all the q_i which generate all α^{ps} for non-trivial α^s (i.e. s is co-prime to p). Let us choose that $q \in U_{n-1,k,(p)}$, which has the maximal value of k.

Then $gcd(k,p) = 1$ (otherwise consider $q(1 - \lambda_{n-1}^{k/p})^p)$. Next we prove that k is odd. If untrue, consider the following element from our set of $\{q_i\}$, namely $q/\sigma(q)$, where σ is the complex conjugation. Easy computations show that if k is even for q, then $q/\sigma(q) \in U_{n-1,s,(p)}$ with $s > k$. On the other hand $q/\sigma(q)$ is in our chosen set of $\{q_i\}$ because it generates some ideal from the class of α^2 since $\mathrm{Cl}\,\mathbb{Q}(\zeta_{n-1})(p) = \mathrm{Cl}\,\mathbb{Q}(\zeta_{n-1})(p)^-$. Therefore we have proved that k is odd. Then $(\eta_{p^n-k}, q) \neq 1$ and this means that η_{p^n-k} is a non-trivial element of $\mathcal{V}_n^+$ for which $\tau_\alpha(\eta_{p^n-k}) \neq 1$.

The theorem is proved.

□

One of the Kervaire-Murthy conjectures was that $\operatorname{Char} \mathcal{V}_n^+ \cong \mathrm{Cl}^{(p)} \mathbb{Q}(\zeta_{n-1})$. Now we partially solve this conjecture.

Corollary 3.3. $\mathrm{Cl}\, \mathbb{Q}(\zeta_{n-1})(p) \cong \mathcal{V}_n^+/(\mathcal{V}_n^+)^p \cong (\mathbb{Z}/p\mathbb{Z})^{r_{n-1}}$ *(see Section 2 for the definition of* r_{n-1}*).*

Proof. It remains to prove the second isomorphism only, which follows from Theorem 2.14. □

Now it is clear that the Assumption 2 from [H-S], which we used there to describe $\mathcal{V}_n^+$, is valid for any semi-regular prime.

Corollary 3.4. *Any unramified extension of* $\mathbb{Q}(\zeta_{n-1}) = F_{n-1}$ *of degree* p *is of the form* $F_{n-1}(\epsilon^{1/p})/F_{n-1}$*, where* ϵ *is a unit satisfying* $\epsilon \equiv 1 \bmod \lambda_{n-1}^{p^n+1}$*.*

Now let us consider the Iwasawa module $T_p(\mathbb{Q})$ as a $\mathbb{Z}_p$-module. It is known from the Iwasawa theory that $T_p(\mathbb{Q}) \cong \mathbb{Z}_p^\lambda$ for semi-regular p, where λ is the Iwasawa invariant for p (see [W, Corollary 13.29]) and consequently $\mathrm{Cl}^{(p)}(F_N)$ has λ generators as an abelian group for big N Therefore we obtain the following

Corollary 3.5. *There exists an integer* N *such that* $r_k = \lambda$ *for* $k > N$*. Moreover, any unramified extension of* $\mathbb{Q}(\zeta_k) = F_k$ *of degree* p *is of the form* $F_k(\epsilon^{1/p})/F_k$*, where* $\epsilon \in \mathbb{Z}[\zeta_N]^*$ *is a unit satisfying* $\epsilon \equiv 1 \bmod \lambda_N^{p^{N+1}+1}$*.*

Finally we obtain Kummer's Lemma for semi-regular primes

Corollary 3.6. *Let a unit* $\epsilon \in \mathbb{Z}[\zeta_{n-1}]^*$ *satisfy* $\epsilon \equiv r^p \bmod \lambda_{n-1}^{p^n-1}$*. Then* $\epsilon = \gamma^p \gamma_1$ *with units* γ, γ_1 *and* $\gamma_1 \equiv 1 \bmod \lambda_{n-1}^{p^n+1}$*.*

Proof. If $\epsilon \equiv r^p \bmod \lambda_{n-1}^{p^n-1}$ then $r^{-p}\epsilon \equiv 1 \bmod \lambda_{n-1}^{p^n-1}$ and it follows from the proof of the theorem that in fact $r^{-p}\epsilon \equiv 1 \bmod \lambda_{n-1}^{p^n}$. Then the extension $F_{n-1}(\epsilon^{1/p})/F_{n-1}$ is unramified and therefore by Corollary 3.4 $\epsilon = \gamma^p\gamma_1$, where $\gamma_1 \equiv 1 \bmod \lambda_{n-1}^{p^n+1}$. Clearly, then γ is a unit. □

4. The Kervaire-Murthy Conjecture

This section is devoted to the proof the following theorem.

Theorem 4.1. *Let* p *be a semi-regular prime. Then* $\operatorname{Char} \mathcal{V}_n^+ \cong \mathrm{Cl}^{(p)} \mathbb{Q}(\zeta_{n-1})$*.*

We start by defening the ray group H'_n of F_n by

$$H'_n = \{(a) \subseteq F_n : a \equiv 1 \bmod \lambda_n^{p^n-1}\}.$$

Let $I_0(F_n)$ be the group of all ideals of F_n prime to λ_n and let $P_{0,n}$ be the group of all principal fractional ideal of F_n prime to λ_n. Let K'_n/F_n be the p-part of the ray extension associated to H'_n. Then the Artin map gives us an isomorphism

$$\mathrm{Gal}(K'_n/F_n) \cong (I_n/H'_n)_p.$$

Lemma 4.2. *Let p be a semi-regular prime. Then $\mathcal{V}_n \cong P_{0,n-1}/H'_{n-1}$ and $(P_{0,n-1}/H'_{n-1})^+ = (I_0(F_{n-1})/H'_{n-1})^+_p$.*

Before the proof, again recall that we define $\mathcal{V}_n$ by

$$\mathcal{V}_n := \frac{D_n^*}{\gamma_n(\mathbb{Z}[\zeta_{n-1}]^*)},$$

where $\mathbb{Z}[\zeta_{n-1}]^*$ is embedded in A_n using the map $a \mapsto (a, N_n(a))$. Our definition is equivalent to the one in [K-M] by Proposition 2.7.

Proof. First recall that by Lemma 2.6 $(a, N_n(a)) \equiv 1 \bmod p$ in A_n if and only if $a \equiv 1 \bmod \lambda_{n-1}^{p^n-1}$ in $\mathbb{Z}[\zeta_{n-1}]$, that is, if and only if $(a) \in H'_{n-1}$. By just counting elements it follows that for any $b \in A_n$, $b \equiv 1 \bmod (x-1)$ there exists $a \in \mathbb{Z}[\zeta_{n-1}]$ such that $b \equiv (a, N_n(a)) \bmod p$. This shows that $g_n : \mathbb{Z}[\zeta_{n-1}] \to \mathcal{V}_n$ induces a well defined, bijective homomorphism

$$G : P_{0,n}/H'_n \to \mathcal{V}_n.$$

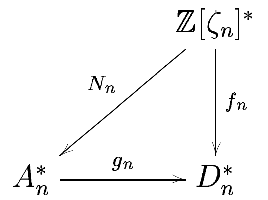
For the second equality note that if α represents an ideal in $(I_0(F_{n-1})/H'_{n-1})^+_p$ then $\alpha^{\tau} \dot{=} \alpha(a)$ for some $(a) \in H'_{n-1}$. Since $\alpha^{P^N} \in H'_{n-1}$ for some N we also get that α^{P^N} is principal. Hence α represents an element of $(\mathrm{Cl}^{(p)}(F_{n-1}))^+$ which is trivial by the semi-regularity condition which means α is principal. □

Corollary 4.3. $\mathcal{V}_n^+ \cong \mathrm{Gal}^+(K'_n/F_n)$.

We will also use the following lemma.

Lemma 4.4. $K'_{n-1}F_n \subseteq K_n \subset K'_n$.

Proof. The second inclusion is trivial. For the first, consider the commutative diagram



Recall that $\mathbb{Z}[\zeta_{n-1}]^*$ is mapped into A_n and that N_n acts as the usual norm $\tilde{N}_{n,1}$. It follows that if $b \in H_n$, that is $b \equiv 1 \bmod \lambda_n^{p^n}$, then $\tilde{N}_{n,1}(b) \equiv 1 \bmod \lambda_{n-1}^{p^n-1}$, that is $\tilde{N}_{n,1}(b) \in H'_{n-1}$. To show the inclusion we have to show that $\Phi_{F_n}(b)$ acts trivially on $K'_{n-1}F_n$ if $b \in H_n$. But since the restriction of the Artin map Φ_{F_n} to K'_{n-1} is $\Phi_{F_{n-1}} \circ \tilde{N}_{n,1}$ this follows from above. □

Now we want to extend some results of [K-M]. Let $F = \bigcup F_n$ and let K be the maximal abelian p-extension of F such that only the prime λ (the unique extension of λ_n to F) ramifies in K. Clearly K_n and K'_n are subfields of K.

Let $E = \bigcup \mathbb{Z}[\zeta_n]^*$ and $M_n = F(E^{1/p^n})$. It was shown in [K-M] that $M_n \subset K$. Set $M = \bigcup M_n$. The group $\mathrm{Gal}(K/M)$ was described by Iwasawa, namely $\mathrm{Char}\,\mathrm{Gal}(K/M) \cong S$, where S is the direct limit of $S_n := \mathrm{Cl}^{(p)}\,\mathbb{Q}(\zeta_n)$ with respect to the canonical embeddings $\mathrm{Cl}^{(p)}\,\mathbb{Q}(\zeta_n) \to \mathrm{Cl}^{(p)}\,\mathbb{Q}(\zeta_{n+1})$.

Now, since p is odd, $\mathrm{Gal}(K/F) = \mathrm{Gal}^+(K/F) \oplus \mathrm{Gal}^-(K/F)$ and it was explained in [K-M] that for the semi-regular primes

$$\mathrm{Gal}(K/M) = \mathrm{Gal}^+(K/M) = \mathrm{Gal}^+(K/F) = \mathrm{Char}(S)$$

It follows that $\mathrm{Gal}(M/F) = \mathrm{Gal}^-(K/F)$ and if we define K^+ to be the subfield of K fixed by $\mathrm{Gal}^-(K/F)$ then we see that $K = K^+M$ and $K^+ \cap M = F$. Moreover,

$$\mathrm{Gal}(K^+/F) = \mathrm{Gal}(K/M) = \mathrm{Gal}^+(K/M) = \mathrm{Gal}^+(K/F) = \mathrm{Char}(S) := G^+$$

We also need the subfields KS_n of K^+ defined as follows: S_n is a subgroup of S and the latter group is dual to G^+. Let $S_n^\perp \subset G^+$ be the subgroup annihilating S_n and let $KS_n \subset K^+$ be fixed by $S_n^\perp$. Then obviously we have $\mathrm{Gal}(KS_n/F) = \mathrm{Char}(S_n)$, and since S is the direct limit of S_n it follows that $K^+ = \bigcup KS_n$.

Similarly, starting from the extensions $F_n \subset K_n$ and $F_n \subset K'_n$ we can define extensions of F_n, namely K_n^+ and ${K'_n}^+$ such that $\mathrm{Gal}(K_n^+/F_n) = \mathcal{V}_n^+$ and $\mathrm{Gal}({K'_n}^+/F_n) = \mathcal{V}_{n+1}^+$. Since $K_n \cap F = F_n$ (see [K-M]) we have $\mathrm{Gal}(K_nF/F) \cong \mathrm{Gal}(K_n/F_n)$ and consequently

$$\mathrm{Gal}(K_n^+M/M) \cong \mathrm{Gal}(K_n^+F/F) \cong \mathrm{Gal}(K_n^+/F_n) = \mathcal{V}_n^+$$

Lemma 4.5. $K_n^+F \subset KS_{n-1}$

Proof. It was proved in [K-M] that the canonical surjection

$$\mathrm{Gal}(K^+/F) = \mathrm{Gal}^+(K/F) = \mathrm{Char}(S) \to \mathcal{V}_n^+$$

factors through $\mathrm{Char}(S_{n-1})$ and hence KS_{n-1} contains K_n^+F. □

Theorem 4.6. $K^+ = \bigcup K_n^+F$

Proof. It suffices to prove that KS_n is contained in K_N^+F for some big N. Results of Section 3 imply that for big N both groups $\mathrm{Char}(S_N)$ and $\mathcal{V}_N^+$ have λ generators, where λ is the Iwasawa invariant. We also know that $\mathrm{Char}(S_N)$ has $p^{\lambda N+\nu}$ elements and $\mathcal{V}_N^+$ has $p^{\lambda N+\nu_1}$ elements, where ν, ν_1 do not depend on N. Moreover, it follows from the structure of $\mathcal{V}_N^+$ that any cyclic component of $\mathcal{V}_N^+$ has $p^{N+\nu_i}$ elements where ν_i also do not depend on N. Therefore every cyclic component of $\mathrm{Char}(S_N)$ has more than $p^{N+\nu_i}$ elements.

Now we want to compare the kernels of two canonical surjections, $\mathrm{Char}(S_N) \to \mathcal{V}_{N+1}^+$ and $\mathrm{Char}(S_N) \to \mathrm{Char}(S_n)$. The first kernel has $p^{\nu-\nu_1-p}$ elements. Each cyclic component of the second kernel has $p^{N+\nu_i-n_i}$ elements where $S_n \cong \bigoplus \mathbb{Z}/p^{n_i}\mathbb{Z}$. Therefore for big N the first kernel is contained in the second and we deduce that $KS_n \subset K_{N+1}^+F$. □

Let us construct a homomorphism $r: S_n \to \mathrm{Char}\,\mathcal{V}_{n+1}^+$. Choose an element $b \in S_n$ and its representative β, an ideal in $\mathbb{Z}[\zeta_n]$ co-prime to p. Then $\beta^{p^k} = (q)$, where $q = 1 + \lambda_n^2 t \in \mathbb{Z}[\zeta_n]$ (see the proof of Proposition 3.2). Then we know from [K-M] that $F(q^{1/p^k}) \subset K$ and more exactly $F(q^{1/p^k}) \subset K_N^+M$ for some N. Without loss of generality we can assume that $N \geq n+1$. For any $v \in \mathcal{V}_N^+ = \mathrm{Gal}(K_N^+M/M)$ define $\tau_b(v) = v(q^{1/p^k}) \cdot q^{-1/p^k}$ (Kummer's pairing). Since by Lemma 2.15 $\mathcal{V}_{n+1}^+$ is a subgroup of $\mathcal{V}_N^+$, we can finally define $r(b) \in \mathrm{Char}\,\mathcal{V}_{n+1}^+$ as the corresponding restriction of τ_b.

Theorem 4.7. *r is injective.*

Proof. Before we start proving the theorem we need the following

Lemma 4.8. *Let α be an ideal of $\mathbb{Z}[\zeta_n]$ such that $\alpha^p = (q)$ with $q \equiv 1 \bmod \lambda_n^2$. Then $F_n(q^{1/p}) \subset K_n'$.*

Proof. We have to prove that $\Phi_{F_n}(a) = id$ on $F_n(q^{1/p})$ for any $a \equiv 1 \bmod \lambda_n^{p^{n+1}-1}$. By the Reciprocity Law (see for instance [C-F], ch. VII) it is true if a is a local norm from the λ_n-adic completion of $F_n(q^{1/p})$. The latter is equivalent to that of $(a,q)_{\lambda_n} = 1$ and this was established in the proof of Theorem 3.1, where the corresponding local symbol was defined. □

We continue the proof of the theorem. It is sufficient to prove that r is injective on the subgroup of elements of order p. So, let $b^p = (q)$ where we can assume that $q \equiv 1 \bmod \lambda_n^2$. Then $q \in K_n' \subset K_{n+1}$. We have to find

$$v \in \mathcal{V}_{n+1}^+ = \mathrm{Gal}^+(K_{n+1}/F_{n+1}) = (P_{0,n+1}/H_{n+1})^+$$

such that $v(q^{1/p}) \times q^{-1/p} \neq 1$. So, without loss of generality we can assume that $v \in \mathbb{Z}[\zeta_{n+1}]$ and $v \equiv 1 \mod \lambda_{n+1}$. Further, v acts on K_{n+1} as $\Phi_{F_{n+1}}(v)$. On the other hand $q^{1/p} \in K'_n$ and therefore $\Phi_{F_{n+1}}(v)(q^{1/p}) = \Phi_{F_n}(N_{F_{n+1}/F_n}(v))(q^{1/p})$. By Proposition 2.7 and Lemma 4.2, N_{F_{n+1}/F_n} induces an isomorphism between $P_{0,n+1}/H_{n+1}$ and $P_{0,n}/H'_n$. Thus we have to find $w \in \mathbb{Z}[\zeta_n]$ such that $\Phi_{F_n}(w)(q^{1/p}) \neq q^{1/p}$. Again, by the Reciprocity Law we have that $\Phi_{F_n}(w)\psi_{\lambda_n}(w) = id$, where ψ_{λ_n} is the local Artin map. We get that

$$\Phi_{F_n}(w)(q^{1/p}) \times q^{-1/p} = \psi_{\lambda_n}(w^{-1})(q^{1/p}) \cdot q^{-1/p} = (q, w)_{\lambda_n}$$

(the symbol $(\,,\,)_{\lambda_n}$ was defined in the proof of Theorem 3.1) Then the required w exists by Theorem 3.1. □

Corollary 4.9. *Theorem 4.1 holds, i.e.* $\mathrm{Cl}^{(p)}(F_n) \cong \mathrm{Char}\, \mathcal{V}^+_{n+1}$

Corollary 4.10. *For any semi-regular prime p*

$$1) \quad \mathrm{Cl}^{(p)}\, \mathbb{Q}(\zeta_0) \cong \mathrm{Pic}^{(p)}\, \mathbb{Z}C_p \cong (\mathbb{Z}/p\mathbb{Z})^{r(p)}$$

$$2) \quad \mathrm{Pic}^{(p)}\, \mathbb{Z}C_{p^2} \cong (\mathbb{Z}/p\mathbb{Z})^{\frac{p-3}{2}+r_1-r(p)} \oplus (\mathbb{Z}/p^2\mathbb{Z})^{2r(p)}$$

5. Applications

The case $\lambda = r(p)$

We now proceed by making an assumption under which we will prove all of the Kervaire-Murthy conjectures.

Assumption 1. $\lambda = r(p)$

Then it follows that $\mathrm{Cl}^{(p)}\, \mathbb{Q}(\zeta_n) \cong (\mathbb{Z}/p^{n+1}\mathbb{Z})^{r(p)}$ for all n The assumption $\lambda = r(p)$ follows from certain congruence assumptions on Bernoulli numbers (see page 202 in [W]) known to hold for all primes less than 4.000.000. Of course all these primes are semi-regular.

The following result follows directly from Theorem 2.14.

Theorem 5.1. *If p is a semi-regular prime and r the index of irregularity and Assumption 1 holds, then* $\mathcal{V}^+_n \cong (\mathbb{Z}/p^n\mathbb{Z})^r$.

We now proceed to show how we can directly show that $\mathcal{V}^+_n = V^+_n$ when $\mathcal{V}^+_n \cong (\mathbb{Z}/p^n\mathbb{Z})^r$. The proof of this relies of constructing a certain basis for D^+_{n-1} consisting of norms of elements from $\mathbb{Z}[\zeta_{n-1}]^*$ considered $\mod p$.

Let $\Phi : U_{n-1,p^n-p^{n-1}} \to D_{n-1}^+$ be defined by

$$\Phi(\epsilon) = N_{n-1}(\frac{\epsilon - 1}{p}) - \frac{N_{n-1}(\epsilon) - 1}{p} \mod p.$$

Since N_{n-1} is additive $\mod p$ one can show with some simple calculations that Φ is a group homomorphism. See Lemmas 5.6 and 5.12 for details.

Explicitly, what we want to prove is the following.

Theorem 5.2. *If $\mathcal{V}_n^+ \cong (\mathbb{Z}/p^n\mathbb{Z})^r$, then Φ is a surjective group homomorphism.*

As we can see by the following corollary, the theorem is what we need.

Corollary 5.3. *If $\mathcal{V}_n^+ \cong (\mathbb{Z}/p^n\mathbb{Z})^r$, then $V_n^+ = \mathcal{V}_n^+$*

Proof of the Corollary. We want to show that for any $(1, \gamma) \in A_n^*$ there exists $(\epsilon, N_{n-1}(\epsilon)) \in A_n^*$ such that $(1, \gamma) \equiv (\epsilon, N_{n-1}(\epsilon)) \mod p$, or more explicitly that for all $\gamma \in A_{n-1}^{*+}$, $\gamma \equiv 1 \bmod p$ there exists $\epsilon \in \mathbb{Z}[\zeta_{n-1}]^*$ such that $(\epsilon, N(\epsilon)) \equiv (1, \gamma)$ mod p in A_n. This is really equivalent to the following three statements in $\mathbb{Z}[\zeta_{n-1}]$, A_{n-1} and D_{n-1} respectively

$$\begin{aligned} \epsilon &\equiv 1 \mod p \\ N_{n-1}(\epsilon) &\equiv \gamma \mod p \\ N_{n-1}(\frac{\epsilon - 1}{p}) &\equiv \frac{N_{n-1}(\epsilon) - \gamma}{p} \mod p \end{aligned}$$

Note that $(1, \gamma) \in A_n$ implies $g_{n-1}(\gamma) = f_{n-1}(1)$ in D_{n-1}, or in other words, that $\gamma \equiv 1 \mod p$. Hence we only need to show that for any $\gamma \in A_{n-1}^{*+}$ there exists $\epsilon \in U_{n-1,p^n-p^{n-1}}$ such that

$$N_{n-1}(\frac{\epsilon - 1}{p}) - \frac{N_{n-1}(\epsilon) - 1}{p} \equiv \frac{1 - \gamma}{p} \mod p.$$

But the left hand side is exactly $\Phi(\epsilon)$ so the corollary really does follow from Theorem 5.2 $\square$

We now proceed to start proving Theorem 5.2. Recall that $r = r(p)$ are the number of indexes $i_1, i_2 \dots i_r$ among $1, 2 \dots (p-3)/2$ such that the nominator of the Bernoulli number B_{i_k} (in reduced form) is divisible by p.

Let $\bar{E}_n : D_n \to D_n^*$ be the truncated exponantial map defined by

$$\bar{E}_n(y) = 1 + y + \frac{y^2}{2!} + \ldots + \frac{y^{p-1}}{(p-1)!}$$

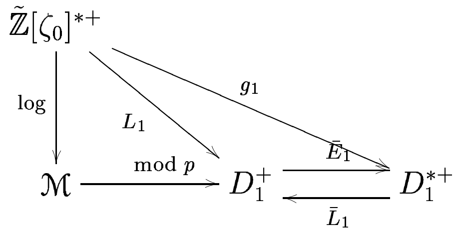
and let $\bar{L_n} : D_n^* \to D_n$ be the truncated logarithm map

$$\bar{L_n}(1+y) = y - \frac{y^2}{2} + \ldots - \frac{y^{p-1}}{(p-1)}.$$

We also consider the usual λ-adic log-map defined by a power series as usual.

We denote the cyclytomic units of $\mathbb{Z}[\zeta_0]^{*+}$ by C_0^+. Let $\mathcal{M}$ be the group of real λ_0-adic integers with zero trace. Any $a \in \mathcal{M}$ can be uniquely presented as $a = \sum_{i=1}^{m-1} b_i \lambda_0^{2i}$, $m = (p-1)/2$. Consider the homomorphism $\Psi : \mathbb{Z}[\zeta_0]^* \to \mathcal{M}$ defined by $\epsilon \mapsto \log(\epsilon^{p-1})$. Following [B-S], page 370-375, we see that there are exactly r elements λ_0^{2i}, namely $\lambda_0^{2i_k}$, such that $\lambda_0^{2i} \notin \Psi(C_0^+)$. This implies that for exactly the r indexes $i_1, i_2 \ldots i_r$ we have $(\bar{x}_1 - \bar{x}_1^{-1})^{2i_k} \neq g_1(log(\epsilon^{p-1}))$ for any $\epsilon \in C_0^+$.

Suppose $(x - x^{-1})^{2i_s} = g_1(\log \epsilon)$ for some $\epsilon \in \mathbb{Z}[\zeta_0]^{*+}$. It is well known that the index of C_0^+ in $\mathbb{Z}[\zeta_0]^{*+}$ equals the classnumber h_+ of $\mathbb{Q}(\zeta_0)^+$. Since p is semi-regular there exists s with $(s,p) = 1$ such that $\epsilon^s \in C_0^+$ and by co-primality of $s(p-1)$ and p we can find u, v such that $1 = s(p-1)u + pv$. Then $\epsilon = \epsilon^{s(p-1)u+pv} = (\epsilon^s)^{p-1}\epsilon^{pv}$ so $\log((\epsilon^{su})^{(p-1)u}) = \log \epsilon - pv \log \epsilon \equiv \log \epsilon \equiv (x - x^{-1})^{2i_s}$, which is a contradiction. Hence $(x - x^{-1})^{2i_s} \notin g_1(\log \mathbb{Z}[\zeta_0]^{*+})$. Since formally, $\exp(\log(1+y)) = 1 + y$ it is not hard to see that $E_1(L_1(1+y)) \equiv 1 + y \mod p$ and that we have a commutative diagram



Recall that $D_{n,(s)}^{*+} := \{y \in D_n^{*+} : y \equiv 1 \mod (x - x^{-1})^s\}$ and that we know that $\mathcal{V}_1^+ := D_1^{*+}/g_1(\mathbb{Z}[\zeta_0]^{*+})$ has $r := r(p)$ generators. If we now apply the map E_1 and do some simple calculations we now get the following proposition.

Proposition 5.4. *The r elements $\bar{E_1}((x_1 - x_1^{-1})^{2i_k})$ generate $D_1^{*+}/g_1(\mathbb{Z}[\zeta_0]^{*+})$ and belong to $D_{1,(2)}^{*+}$ but do not belong to $D_{1,(p-2)}^{*+}$.*

We now want to lift this result to D_n^{*+}. From now on (exepting Lemma 4.11) we will denote the generator $x \in D_n$ by x_n.

Proposition 5.5. *If Assumption 1 holds, then the r elements $\bar{E_n}((x_n - x_n^{-1})^{2i_k})$ generate the group $\mathcal{V}_n^+ := D_n^{*+}/g_n(\mathbb{Z}[\zeta_{n-1}]^{*+})$. The elements $\bar{E_n}((x_n - x_n^{-1})^{2i_k})^{p^{n-1}}$ are non-trivial in $\mathcal{V}_n^+$, belong to $D_{n,(p^{n-1})}^{*+}$ but do not belong to $D_{n,(p^n-2p^{n-1})}^{*+}$*

Proof. Induction on n. If $n=1$ this is exactly Proposition 5.4. Suppose the statement holds for the index equal to $n-1$. The diagram

$$\begin{array}{ccc} \mathbb{Z}[\zeta_{n-1}]^{*+} & \longrightarrow & D_n^{*+} \\ \big\downarrow{\scriptstyle \tilde{N}_{n,1}} & & \big\downarrow \\ \mathbb{Z}[\zeta_{n-2}]^{*+} & \longrightarrow & D_{n-1}^{*+} \end{array} \tag{5.1}$$

is commutative. Hence, if $z_n \in D_n^*$ is mapped to $z_{n-1} \in D_{n-1}^*$ and $z_{n-1} \notin \operatorname{Im}\mathbb{Z}[\zeta_{n-2}]^*$, then $z_n \notin \operatorname{Im}\mathbb{Z}[\zeta_{n-1}]^*$. Moreover, $z_n^p \notin \operatorname{Im}\mathbb{Z}[\zeta_{n-1}]^*$ in this case. This follows from the fact that $\mathcal{V}_m^+ \cong (\mathbb{Z}/p^m\mathbb{Z})^r$ for all m. Hence, if an element $z \in \mathcal{V}_n^+$ has order p, then the surjection $\mathcal{V}_n^+ \to \mathcal{V}_{n-1}^+$ maps z to the neutral element in $\mathcal{V}_{n-1}^+$. Now, the elements $\bar{E}_n((x_n - x_n^{-1})^{2i_k})^{p^{n-1}}$ are not in the image of $\mathbb{Z}[\zeta_{n-1}]^*$ by Theorem 4.3 and since $\bar{E}_n((x_n - x_n^{-1})^{2i_k})^{p^{n-2}}$ clearly map onto $\bar{E}_{n-1}((x_{n-1} - x_{n-1}^{-1})^{2i_k})^{p^{n-2}} \notin g_{n-1}(\mathbb{Z}[\zeta_{n-2}]^{*+})$ by induction. Finally, since $1 \leq 2i_k \leq p-1$ we get $p^{n-1} \leq 2p^{n-1}i_k \leq p^n - 2p^{n-1}$ and this means that all the elements

$$\begin{aligned} \bar{E}_n((x_n - x_n^{-1})^{2i_k})^{p^{n-1}} &= (1 + (x_n - x_n^{-1})^{2i_k} + \ldots)^{p^{n-1}} = \\ &= 1 + (x_n - x_n^{-1})^{2p^{n-1}i_k} + \ldots \end{aligned}$$

fulfil our requirements. □

Recall that $c : D_n \to D_n$ is the map induced by $\bar{x} \mapsto \bar{x}^{-1}$ and that $D_n^+ := \{a \in D_n : c(a) = a\}$ Define $\varphi : U^+_{n-1,p^n-p^{n-1}} \to D^+_{n-1}$ by $\varphi(\gamma) = N_{n-1}(\frac{\gamma-1}{p}) \mod p$.

Lemma 5.6. *φ is a homomorphism from the multiplicative group $U^+_{n-1,p^n-p^{n-1}}$ to the additive group D^+_{n-1} and the kernel is $U^+_{n-1,p^n-1} = U^+_{n-1,p^n+1}$.*

Proof. Let ϵ and γ belong to $\in U^+_{n-1,p^n-p^{n-1}}$. Then, since N_{n-1} is additive mod p and $N_{n-1}(\epsilon) \equiv 1 \mod p$,

$$\begin{aligned} N_{n-1}(\frac{\epsilon\gamma - 1}{p}) &\equiv N_{n-1}(\frac{\epsilon(\gamma-1) + (\epsilon - 1)}{p}) \equiv \\ &\equiv N_{n-1}(\epsilon)N_{n-1}(\frac{\gamma-1}{p}) + N_{n-1}(\frac{\epsilon-1}{p}) \equiv \\ &\equiv N_{n-1}(\frac{\gamma-1}{p}) + N_{n-1}(\frac{\epsilon-1}{p}) \mod p \end{aligned}$$

so φ is a homomorphism. Suppose $N_{n-1}((\gamma-1)/p) \equiv 0 \mod p$. Then, by Proposition 2.1, $f_{n-1}((\gamma-1)/p) = 0$ which means $\gamma \in U^+_{n-1,p^n-1} = U^+_{n-1,p^n+1}$ (the latter equality is due to Lemma 3.2). □

In this notation, what we want to prove is the following

Proposition 5.7. *If Assumption 1 holds, then the map*

$$\tilde{\varphi} : (U_{n-1,p^n-p^{n-1}})/(U_{n-1,p^n+1}) \to D^+_{n-1}$$

induced by φ is an isomorphism.

Since $\tilde{\varphi}$ is obviously injective it is enough to prove the following proposition

Proposition 5.8. *Suppose Assumption 1 holds. Then*

$$|D^+_{n-1}| = \left|\frac{U_{n-1,p^n-p^{n-1}}}{U_{n-1,p^n+1}}\right|.$$

Proof. Recall that $|D^+_{n-1}| = p^{\frac{p^{n-1}-1}{2}}$ so we need to prove that

$$|(U_{n-1,p^n-p^{n-1}})/(U_{n-1,p^n-1})| = p^{\frac{p^{n-1}-1}{2}}.$$

An element of $\mathcal{V}^+_n$ of the form $b = 1+(x_n - x_n^{-1})^{2s_1}$, where $p^{n-1} < 2s \leq 2s_1 < p^n - 1$, correspond to a non-trivial element of

$$\frac{D^{*+}_{n,(2s)}}{g_n(\mathbb{Z}[\zeta_{n-1}]^{*+}) \cap D^{*+}_{n,(2s)}}$$

which is a canonical subgroup of $\mathcal{V}^+_n$. If t_{2s} is the number of independent such elements b, then

$$\frac{D^{*+}_{n,(2s)}}{g_n(\mathbb{Z}[\zeta_{n-1}]^{*+}) \cap D^{*+}_{n,(2s)}} \cong (\mathbb{Z}/p\mathbb{Z})^{t_{2s}}$$

By Proposition 5.5, $t_{2s} = 0$ if $2s > p^n - 2p^{n-1}$. On the other hand

$$g_n(\mathbb{Z}[\zeta_{n-1}]^{*+}) \cap D^{*+}_{n,(2s)} \cong U_{n-1,2s}/U_{n-1,p^n-1}$$

since $U_{n-1,p^n-1} = \ker(g_n)$, and hence $U_{n-1,2s}/U_{n-1,p^n-1} \cong D^{*+}_{n,(2s)}$ if $2s > p^n - 2p^{n-1}$. The number of elements in $D^{*+}_{n,(2s)}$ is $p^{\frac{p^n-1-2s}{2}}$. Setting $2s = p^n - p^{n-1}$ completes the proof. □

We now have to do carefull estimations of some congruences of our norm-maps.

Lemma 5.9. *Let $2 \leq n$ and $1 \leq k < n$. If $\epsilon \in \mathbb{Z}[\zeta_{n-1}]$ and If $\epsilon \equiv 1 \mod p^{s+1}\lambda_{n-1}^{p^{n-1}-p^k}$, then $(N_{n-1}(\epsilon) - 1)/p$ can be represented by a polynomial $f(x) = p^s f_1(x)$ in A_{n-1}, where $f_1(x) \equiv 0 \mod (x-1)^{p^{n-1}-p^{k-1}}$ in D_{n-1}.*

Before the proof, recall that the usual norm $\tilde{N}_{n,1}$, $1 \le n, 1 \le k < n$, can be viewed as a product of automorphisms of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}(\zeta_{n-1})$. If $t_n \in \mathbb{Z}[\zeta_n]$ and $t_{n-1} \in \mathbb{Z}[\zeta_{n-1}]$ we immediately get $\tilde{N}_{n,1}(1+t_{n-1}t_n) = 1 + \mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{n-1})}(t_n)t_{n-1}t'$ for some $t' \in \mathbb{Z}[\zeta_{n-1}]$. Recall that the trace is always divisible by p. In the proof below we will for convenience denote any generic element whose value is not interesting for us by the letter t.

Proof. Induction on n. If $n = 2$ (which implies $k = 1$), $N_{n-1} = \tilde{N}_{1,1} : \mathbb{Z}[\zeta_1] \to A_1 \cong \mathbb{Z}[\zeta_0]$. Let $\epsilon := 1 + tp^{s+1}$ Then $\epsilon = 1 + tp^s\lambda_1^{p^2-p} = 1 + tp^s\lambda_0^{p-1}$. By the note above,

$$\frac{\tilde{N}_{1,1}(\epsilon) - 1}{p} = tp^s\lambda_0^{p-1}$$

which is represented by some $f(x) = p^s(x-1)^{p-1}f_1(x)$ in A_1 Suppose the statement of the Lemma holds with the index equal to $n-2$. Let $\epsilon := 1 + tp^{s+1}\lambda_{n-1}^{p^{n-1}-p^k}$. Note that $\epsilon = 1+tp^{s+1}\lambda_{n-2}^{p^{n-2}-p^{k-1}}$ and by the note before this proof, $\tilde{N}_{n-1,1}(\epsilon) = 1 + tp^{s+2}\lambda_{n-2}^{p^{n-2}-p^{k-1}}$. Let $(N_{n-1}(\epsilon)-1)/p$ be represented by a pair $(a,b) \in \mathbb{Z}[\zeta_{n-2}] \times A_{n-2}$. Then $a = (\tilde{N}_{n-1,1}(\epsilon)-1)/p = tp^{s+1}\lambda_{n-2}^{p^{n-2}-p^{k-1}}$. In $A_{n-2,1}$ a hence can be represented by a polynomial $a(x) = p^{s+1}(x-1)^{p^{n-2}-p^{k-1}}a_1(x)$ for some $a_1(x)$. By the expression for $\tilde{N}_{n-1,1}(\epsilon)$ and by the assumption, we get

$$b = \frac{N_{n-2}(\tilde{N}_{n-1,1}(\epsilon)) - 1}{p} = \frac{N_{n-2}(1 + tp^{s+2}\lambda_{n-2}^{p^{n-2}-p^{k-1}}) - 1}{p} = p^{s+1}b_1(x)$$

where $b_1(x) \equiv (x-1)^{p^{n-2}-p^{k-2}}b_2(x) \mod p$ for some $b_2(x)$. Define $b(x) := p^{s+1}b_1(x)$. We want to find a polynomial $f(x) \in A_{n-1}$ that represents (a,b), that is, maps to $a(x)$ and $b(x)$ in $A_{n-2,1}$ and A_{n-2} respectively. Note that

$$p = \frac{x^{p^{n-1}}-1}{x^{p^{n-2}}-1} + t(x)\frac{x^{p^{n-2}}-1}{x-1}$$

for some polynomial $t(x) \in \mathbb{Z}[x]$. Hence

$$a(x) - b(x) = \Big(\frac{x^{p^{n-1}}-1}{x^{p^{n-2}}-1} + t(x)\frac{x^{p^{n-2}}-1}{x-1}\Big)p^s((x-1)^{p^{n-2}-p^{k-1}}a_1(x) - b_1(x))$$

Then we can define a polynomial $f(x)$ by

$$\begin{aligned} f(x) : &= a(x) + p^s((x-1)^{p^{n-2}-p^{k-1}}a_1(x) - b_1(x))\frac{x^{p^{n-1}}-1}{x^{p^{n-2}}-1} = \\ &= b(x) + p^s((x-1)^{p^{n-2}-p^{k-1}}a_1(x) - b_1(x))t(x)\frac{x^{p^{n-2}}-1}{x-1}. \end{aligned}$$

Clearly, f maps to $a(x)$ and $b(x)$ respectively. We now finish the proof by observing that

$$\begin{aligned} f(x)/p^s &= p(x-1)^{p^{n-2}-p^{k-1}}a_1(x) + ((x-1)^{p^{n-2}-p^{k-1}}a_1(x) - b_1(x))\frac{x^{p^{n-1}}-1}{x^{p^{n-2}}-1} \equiv \\ &\equiv ((x-1)^{p^{n-2}-p^{k-1}}a_1(x) - (x-1)^{p^{n-2}-p^{k-2}}b_2(x))(x-1)^{p^{n-1}-p^{n-2}} = \\ &= (a_1(x) - (x-1)^{p^{k-1}-p^{k-2}}b_2(x))(x-1)^{p^{n-1}-p^{k-1}} \mod p. \end{aligned}$$

□

By setting $s=0$ we in the lemma above we immediately get the following theorem.

Theorem 5.10. *Let* $2 \leq n$ *and* $1 \leq k < n$. *Suppose* $\epsilon \in U_{n-1,p^n-p^k}$. *Then* $g_{n-1}((N_{n-1}(\epsilon)-1)/p) \equiv 0 \mod (x-1)^{p^{n-1}-p^{k-1}}$ *in* D_{n-1}

The following proposition is immediate by using that $g_{n-1}N_{n-1} = f_{n-1}$.

Proposition 5.11. *Let* $2 \leq n$, $1 \leq k < n$ *and let* $\epsilon \in U_{n-1,p^n-p^k} \setminus U_{n-1,p^n-p^{k-1}}$. *Then* $g_{n-1}((N_{n-1}((\epsilon-1)/p))) \equiv 0 \mod (x-1)^{p^{n-1}-p^k}$ *but* $g_{n-1}((N_{n-1}((\epsilon-1)/p))) \not\equiv 0 \mod (x-1)^{p^{n-1}-p^{k-1}}$ *in* D_{n-1}.

Let $\omega : U_{n-1,p^n-p^{n-1}} \to D^+_{n-1}$ be defined by $\omega(\gamma) := g_{n-1}((N_{n-1}(\gamma)-1)/p)$.

Lemma 5.12. *ω is a homomorphism*

Proof. Suppose ϵ and γ belong to $U_{n-1,p^n-p^{n-1}}$. Then $N_{n-1}(\gamma) \equiv 1 \mod p$ in A_{n-1} because

$$N_{n-1}(\gamma) = (\tilde{N}_{n-1,1}(\gamma), \tilde{N}_{n-1,2}(\gamma), \dots, \tilde{N}_{n-1,n-1}(\gamma))$$

and $\tilde{N}_{n-1,k}(\gamma) \equiv 1 \mod p^2$ for all $k = 1, 2, \dots, n-1$. Hence

$$\begin{aligned} \omega(\epsilon\gamma) &\equiv \frac{N_{n-1}(\epsilon\gamma)-1}{p} = \frac{N_{n-1}(\gamma)N_{n-1}(\epsilon) - N_{n-1}(\epsilon) + N_{n-1}(\epsilon) - 1}{p} \equiv \\ &\equiv N_{n-1}(\gamma)\frac{N_{n-1}(\epsilon)-1}{p} + \frac{N_{n-1}(\gamma)-1}{p} \equiv \\ &\equiv \frac{N_{n-1}(\epsilon)-1}{p} + \frac{N_{n-1}(\gamma)-1}{p} = \omega(\epsilon) + \omega(\gamma) \mod p \end{aligned}$$

□

Note that if $\epsilon \in U_{n-1,p^n-1}$ then $\omega(\epsilon) = 0$. This can be shown using similar, but simpler, methods as we did in the proof of Lemma 5.9. We can hence define

$$\tilde{\omega} : \frac{U_{n-1,p^n-p^{n-1}}}{U_{n-1,p^n-1}} \to D^+_{n-1}.$$

Now, if $a \in D^+_{n-1}$, let $\mathcal{O}(a)$ be the maximal power of $(x - x^{-1})$ that devides a. In this language we can combine Thereom 5.10 and Proposition 5.11 to the following lemma.

Lemma 5.13. *Let $2 \leq n$, $1 \leq k < n$ and let $\epsilon \in U_{n-1,p^n-p^k} \setminus U_{n-1,p^n-p^{k-1}}$. Then $p^{n-1} - p^k \leq \mathcal{O}(\tilde{\varphi}(\epsilon)) < p^{n-1} - p^{k-1} \leq \mathcal{O}(\tilde{\omega}(\epsilon))$.*

Proposition 5.14. *The map $\tilde{\Phi} := \tilde{\varphi} - \tilde{\omega}$ is an isomorphism.*

Proof. By Proposition 5.7 $\tilde{\varphi}$ is an isomorphism. Hence there exists (classes of) units $\epsilon_i, i = 1, 2, \ldots, (p^{n-1} - 1)/2$ such that the set $\tilde{\varphi}(\epsilon_i)$ forms a basis for D^+_{n-1}. If $a \in D^+_{n-1}$ there exist unique a_i such that $a = \sum_{i=1}^{(p^{n-1}-1)/2} a_i\tilde{\varphi}(\epsilon_i)$. To prove the Proposition it is enough to show that the map

$$\sum_{i=1}^{(p^{n-1}-1)/2} a_i\tilde{\varphi}(\epsilon_i) \mapsto \sum_{i=1}^{(p^{n-1}-1)/2} a_i(\tilde{\varphi}(\epsilon_i) - \tilde{\omega}(\epsilon_i))$$

is invertible. Consider the matrix M for this map in the basis $\{(x - x^{-1})^{2j}\}$. Obviously this matrix can be written $I - M'$, where I is the identity matrix and M' is induced by $\tilde{\varphi}(\epsilon_i) \mapsto \tilde{\omega}(\epsilon_i)$. By Lemma 5.13 the matrix M' is a lower triangular matrix with zeros on the diagonal. This means M is lower triangular with ones on the diagonal and hence invertible. □

Proof of Theorem 5.2. The map $\tilde{\Phi}$ is obviously induced by Φ which hence must be surjective by prop 5.14. □

By Iwasawas theorem, there are numbers $\lambda \geq 0$, $\mu \geq 0$ and ν such that

$$|\operatorname{Cl}^{(p)} \mathbb{Q}(\zeta^-_{n-1}| = p^{\lambda(n-1)+\mu p^n+\nu}$$

for all n big enough. It has later been proved that $\mu = 0$, so for big n, $|\operatorname{Cl}^{(p)} \mathbb{Q}(\zeta_{n-1})^-| = p^{\lambda(n-1)+\nu}$. We get the following result as a direct consequence of the results of this part.

Proposition 5.15. *Let p be a semi-regular prime. Then all three of the Kervaire-Murthy conjectures hold if and only if $\lambda = r(p)$. Moreover, if $\lambda = r(p)$ then $\nu = r(p)$.*

The case $\lambda = r_1$

In [U] Ullom uses the following somewhat technical assumption on p.

Assumption 2. *The Iwasawa invariants λ_{1-i} satisfy $1 \leq \lambda_{1-i} \leq p-1$*

We refer you to [I] for notation. S. Ullom proves that if Assumption 2 holds then, for even i,

$$e_i V_n \cong \frac{\mathbb{Z}}{p^n\mathbb{Z}} \oplus (\frac{\mathbb{Z}}{p^{n-1}\mathbb{Z}})^{\lambda_{1-i}-1}. \tag{5.2}$$

This yields, under the same assumption, that

$$V_n^+ \cong (\frac{\mathbb{Z}}{p^n\mathbb{Z}})^{r(p)} \oplus (\frac{\mathbb{Z}}{p^{n-1}\mathbb{Z}})^{\lambda - r(p)}, \tag{5.3}$$

where

$$\lambda = \sum_{i=1,\, i \text{ even}}^{r(p)} \lambda_{1-i}$$

Hence, when $\lambda = r(p)$ we get that $V_n = (\mathbb{Z}/p^n\mathbb{Z})^{r(p)}$ as predicted by Kervaire and Murthy. Note however, that if $\lambda > r(p)$, then Kervaire and Murthy's conjecture fails. We will discuss some consequenses of Assumption 2. Since V_n^+ is a quotient of $\mathcal{V}_n^+$ applying this to $n = n_0 + 1$ yields

$$r_0 + \lambda n_0 \leq r_0 + r_1 + \ldots + r_{n_0} \leq r_0 + n_0 r_{n_0} \leq r_0 + n_0 \lambda.$$

This obviously implies that $r_k = \lambda$ for all $k = 1, 2, \ldots$ because $\{r_i\}$ is a non-decreasing sequence bounded by λ by Proposition 2.11 and hence we get the following

Lemma 5.16. *When Assumtion 2 holds $r_k = \lambda$ for all $k = 1, 2, \ldots$.*

The following theorem is now immediate.

Theorem 5.17. *If Assumtion 2 holds, then $\mathcal{V}_n^+ = V_n^+$.*

Keeping Theorem 4.1 in mind we immediately get the following corollary.

Corollary 5.18. *When Assumtion 2 holds,*

$$\mathrm{Cl}^{(p)}\, \mathbb{Q}(\zeta_{n-1}) \cong (\mathbb{Z}/p^n\mathbb{Z})^{r(p)} \oplus (\mathbb{Z}/p^{n-1}\mathbb{Z})^{\lambda - r(p)}$$

and $\lambda = r_1$ and $\nu = r_0 = r(p)$.

5.1. An application to units in $\mathbb{Z}[\zeta_n]$.

The techniques we have developed also lead to some conclusions about the group of units in $\mathbb{Z}[\zeta_n]^*$. From the previous results we know that

$$\mathcal{V}_{n+1}^{+} = \frac{\tilde{D}_{n+1}^{*+}}{g_{n+1}(U_{n,1})} \cong \frac{\tilde{D}_{n+1}^{*+}}{\frac{U_{n,2}}{U_{n,p^{n+1}-1}}}$$

Let $s_{n,p^{n+1}-1} = |U_{n,1}/U_{n-1,p^{n+1}-1}|$. A naive first guess would be that $s_{n,p^{n+1}-1} = \frac{p^{n+1}-1-2}{2} = \frac{p^{n+1}-3}{2}$ which is the maximal value of this number. Incidentally, this maximal value equals $|\tilde{D}_{n+1}^{*+}|$. In this case we say that $U_{n,1}/U_{n,p^{n+1}-1}$ is full, but this happens if and only if p is a regular prime. In other words $\mathcal{V}_{n+1}^{+}$ is trivial if and only if p is regular. This fact is by the way proved directly in [H]. For non-regular (but as before semi-regular) primes what happens is that there are "missed places" in $U_{n,1}/U_{n,p^{n+1}-1}$. We define $2k$ as a missed place (at level n) if $U_{n,2k}/U_{n,2k+2}$ is trivial. Lemma 2.9 reads $U_{n,p^{n+1}-1} = U_{n,p^{n+1}+1}$ and hence provides an instant example of a missed place, namely $p^{n+1}-1$. It follows from our theory that every missed place corresponds to a non-trivial element of $\mathcal{V}_{n+1}^{+}$. Recall that $\mathbb{Z}[\zeta_{n-1}]^*$ is identified with its image in A_n. We will now prove that the map $g_n : \mathbb{Z}[\zeta_{n-1}]^* \to D_n^*$ respects the filtrations λ_{n-1}^k and $(x-1)^k$.

Proposition 5.19. *Let $1 \le s \le p^n - 1$ and $\epsilon \in \mathbb{Z}[\zeta_{n-1}]^*$. Then $\epsilon \in U_{n-1,s}$ if and only if $g_n(\epsilon) \in D_{n,(s)}^*$.*

Using this Proposition we see that an element of $D_{n+1,(2s)}^{*+}$ which is non-trivial in $\mathcal{V}_{n+1}^{+}$ corresponds to a missed place $2s$ at level n.

Proof. To show that $g_n(\epsilon) \in D_{n,(s)}^*$ implies $\epsilon \in U_{n-1,s}$ we can use the same technique as in the proof of Theorem I.2.7 in [ST3] (also see Lemma 2.6). For the other direction, first note that is $s \le p^n - p^{n-1}$ the statement follows directly from the commutativity of the diagram

(5.4)
$$\begin{array}{ccc} A_n^* & \longrightarrow & \mathbb{Z}[\zeta_{n-1}]^{*+} \\ \big\downarrow \text{mod } p & & \big\downarrow \text{mod } p \\ D_n^* \cong \left(\frac{\mathbb{F}_p[x]}{(x-1)^{p^n-1}}\right)^* & \longrightarrow & \left(\frac{\mathbb{F}_p[x]}{(x-1)^{p^n-p^{n-1}}}\right)^* \end{array}$$

What is left to prove is that $\epsilon \in U_{n-1,s}$ implies $g_n(\epsilon) \in D_{n,(s)}^*$ also for $p^n - p^{n-1} \le s \le p^n - 1$. For technical reason we will prove that if $\epsilon \in U_{n-1,p^n-p^k+r}$ for some $1 \le k \le n-1$ and $0 \le r \le p^k - p^{k-1}$ then $g_n(\epsilon) \in D_{n,(p^n-p^k+r)}^*$. Note that $\epsilon \in U_{n-1,p^n-1}$ is equivalent to $g_n(\epsilon) = 1 \in D_n^*$ by Lemma 2.6. Suppose $\epsilon = 1 + t\lambda_{n-1}^{p^n-p^k+r}$ for some $t \in \mathbb{Z}[\zeta_{n-1}]$. By Lemma 5.9 we get $N_{n-1}(\epsilon) = 1 + t'p(x-1)^{p^{n-1}-p^{k-1}}$ for some $t' \in A_{n-1}$. In A_n,

$$p = \frac{x^{p^n}-1}{x^{p^{n-1}}-1} + t(x)\frac{x^{p^{n-1}}-1}{x-1}$$

for some polynomial $t(x)$. In A_n consider the element

$$p(t(x-1)^{p^{n-1}-p^k+r} - t'(x-1)^{p^{n-1}-p^{k-1}}) =$$
$$= (\frac{x^{p^n}-1}{x^{p^{n-1}}-1} + t(x)\frac{x^{p^{n-1}}-1}{x-1})(t(x-1)^{p^{n-1}-p^k+r} - t'(x-1)^{p^{n-1}-p^{k-1}}).$$

By computing the right hand side and re-arrange the terms we get

$$f := tp(x-1)^{p^{n-1}-p^k+r} - \big(t(x-1)^{p^{n-1}-p^k+r} - t'(x-1)^{p^{n-1}-p^{k-1}}\big)\frac{x^{p^n}-1}{x^{p^{n-1}}-1} =$$
$$= t'(x-1)^{p^{n-1}-p^{k-1}} - b(x)\frac{x^{p^{n-1}}-1}{x-1}.$$

Using the two representations of f we see that $i_n(1+f) = \epsilon$ and $j_n(1+f) = N_{n-1}(\epsilon)$ so $1+f$ represents $(\epsilon, N_{n-1}(\epsilon))$ (which represents ϵ under our usual identification) in A_n. Since $\leq p^k - p^{k-1}$ we now get $g_n(1+f) \equiv 1 \bmod (x-1)^{p^{n-1}-p^k+r}$ in D_n as asserted. □

Theorem 2.14 and its proof now give us specific information about the missed places which we will formulate in a Theorem below. We start with a simple lemma.

Lemma 5.20. *Let $1 \leq s \leq n+1$ and $1 \leq k < s$. Then $p^s - p^k$ is a missed place at level n if and only if $s = n+1$ and $k = 1$.*

Proof. Let $\eta := \zeta_n^{(p^{n+1}+1)/2}$. Then $\eta^2 = \zeta_n$ and $c(\eta) = \eta^{-1}$. Define

$$\epsilon := \frac{\eta^{p^s+p^k} - \eta^{-(p^s+p^k)}}{\eta^{p^k} - \eta^{-(p^k)}}.$$

Clearly, ϵ is real and since

$$\epsilon = \eta^{-p^s}\frac{\zeta_n^{p^s+p^k}-1}{\zeta_n^{p^k}-1},$$

ϵ is a unit. By a calculation one can show that $\epsilon \in U_{n,p^s-p^k} \setminus U_{n,p^s-p^k+2}$. □

Define for $k = 0, 1, \ldots$ the k-strip as the numbers $p^k+1, p^k+3, \ldots, p^{k+1}-1$.

Theorem 5.21. *At level n we have the following*

1. *Let $0 \leq k \leq n$. In the k-strip there are exactly r_k missed places.*
2. *The missed places in the 0-strip are in one to one correspondence with the numbers $2i_1, \dots, 2i_{r_0}$ such that the numerator of the Bernoulli-number B_{2i_k} (in reduced form) is divisible by p.*
3. *Suppose $i_1, \dots, i_{r_k}$ are the missed places in the k-strip. Then $pi_1, \dots, pi_{r_k}$ are missed places in the $k+1$ strip. The other $r_{k+1} - r_k$ missed places in the $k+1$ strip are not divisible by p.*

Proof. We know from Proposition 5.4 that we have r_0 missed places in the 0-strip at level 0 and that they correspond exactly to the indexes of the relevant Bernoulli numbers. As in Proposition 5.5 an induction argument using the map π_n to lift the generators of $\mathcal{V}_{n-1}^+$ to $\mathcal{V}_n^+$ show that we have r_0 missed places in the 0-strip at every level and that a missed place k at level $n-1$ lift to missed places k and pk at level n. What is left to prove is that the "new" missed places we get when we go from level $n-1$ to n all end up in the n-strip and that no "new" missed places are divisible by p. First, $p^n - 1$ can not be a missed place (at level n) by the lemma above. It follows from our theory that the "new" missed places correspond to the generators of $\mathcal{V}_{n+1}^+$ of exponent p. We need to show that each such generators a_l, $l = 1, \dots, r_{n-1} - r_{n-2}$, belong to $D_{n+1,(p^n+1)}^{*+}$. Suppose for a contradiction that $a_l = 1 + t(x_{n+1} - 1)^s$, $t \neq 0$, $s < p^n - 1$, is a "new" generator. Then $\pi_{n+1}(a_l) = 1 + t(x_n - 1)^s$ is neccesarily trivial in $\mathcal{V}_n^+$ but not in $\tilde{D}_n^{*+}$. Hence $\pi_{n+1}(a_l) = g_n(\epsilon)$ for some $\epsilon \in \mathbb{Z}[\zeta_{n-1}]^*$. Since the usual norm map $\tilde{N}_{n,1}$ is surjective (when p is semi-regular) and by commutativity of diagram 5.1 we then get $a_l g_{n+1}(\epsilon')^{-1} = b$ for some $\epsilon' \in \mathbb{Z}[\zeta_n]^*$ and $b \in \ker\{\tilde{D}_{n+1}^{*+} \to \tilde{D}_n^{*+}\} = \tilde{D}_{n+1}^{*+}(p^n - 1)$. Since $p^n - 1$ is not a missed place, $b = g_{n+1}(\epsilon'')$ for some some $\epsilon'' \in \mathbb{Z}[\zeta_n]^*$. But this means a_l is trivial in $\mathcal{V}_{n+1}^+$ which is a contradiction. We conclude that $a_l \in D_{n+1,(p^n+1)}^{*+}$.

To prove no "new" missed places are divisible by p we need to show that if $a_l \in D_{n+1,(s)}^{*+} \setminus D_{n+1,(s+2)}^{*+}$ is a "new" generator of $\mathcal{V}_{n+1}^+$, then p does not divide s. Now, a generator can always be chosen of the form $1 + (x_{n+1} - 1)^s$. Then an element of the form $1 + (x_{n+1} - 1)^{pk}$, with $k \notin \{i_1, \dots, i_{r_{n-1}}\}$ cannot be a missed place. This follows from the fact that if k is not a missed place, then $1 + (x_n - 1)^k$ is trivial in $\mathcal{V}_n^+$ and since α_n is injective, $1 + (x_{n+1} - 1)^{pk} = \alpha_n(1 + (x_n - 1)^k)$ is also trivial in $\mathcal{V}_{n+1}^+$. □

References

[B-S] Borevich, Z.I. and Shafarevich, I.R, *Number theory.* Academic Press: London and New York, 1966.

[C-F] Cassels, J. W. S. and Fröhlich, A., *Algebraic Number Theory*, Academic Press, London and New York, 1967

[H] Helenius, Ola *Kummers Lemma and Picard Groups of Integer Group Rings* The Arabian Journal of Science and Engineering, Theme Issue: Commutative Algebra, 26 (2001) 107-118.

[H-S] O. Helenius and A. Stolin, *On the Kervaire-Murthy Conjectures* Preprint, Chalmers University of Technology, 2000.

[I] K. Iwasawa, *On $\mathbb{Z}_l$-extensions of algebraic number fields* Ann. of Math., 98 (1973), 246-326.

[K-M] Kervaire, M. A. and Murthy, M. P., *On the Projective Class Group of Cyclic Groups of Prime Power Order.* Comment. Math. Helvetici 52 (1977), 415-452.

[ST1] Stolin, Alexander. *An Explicit Formula for the Picard Group of the Cyclic Group of Order p^2.* Proceedings of the American Mathematical Society, Vol. 121 (1994), 375-383.

[ST2] Stolin, Alexander. *On the Picard Group of the Integer Group Ring of the Cyclic p-Group and Rings Close to It.* Proc. of the 2nd Int. Conf in Comm. Alg. 1997, 443-455.

[ST3] Stolin, Alexander. *On the Picard Group of the Integer Group Ring of the Cyclic p-Group and Certain Galois Groups.* Journal of Number Theory 72, 1998, 48-66.

[U] Ullom, S. *Class Groups of Cyclotomic Fields and Group Rings* London Math. Soc. (2) 17 (1978), no 2, 231-239.

[W] Washington, Lawrence C, *Introduction to Cyclotomic Fields* Springer Verlag, 1997.

Department of Mathematics, Chalmers University of Technology and Göteborg University, SE-41296 Göteborg, Sweden

E-mail address: `olahe@math.chalmers.se`, `astolin@math.chalmers.se`