UNIT BASES IN INTEGER GROUP RINGS AND THE KERVAIRE-MURTHY CONJECTURES

OLA HELENIUS AND ALEXANDER STOLIN

ABSTRACT. In 1977 Kervaire and Murthy presented two conjectures regarding $K_0\mathbb{Z}C_{p^n}$, where C_{p^n} is the cyclic group of order p^n and p a semi-regular prime. There is a group V_n that injects into $\tilde{K}_0\mathbb{Z}C_{p^n} \cong \operatorname{Pic}\mathbb{Z}C_{p^n}$. V_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 conjectured that $V_n^+ \cong (\mathbb{Z}/p^n\mathbb{Z})^{r(p)}$, where $r(p)$ is the index of irregularity of the prime p and that $\mathcal{V}_n^+ \cong V_n^+$. Under an extra assumption on the prime p, Ullom proved in 1978 in [U2] 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 Murthy's first conjecture holds only when $\lambda = r(p)$. In the present paper we prove that under the same condition Ullom used, conjecture two always holds. We also discuss a different assumption on p regarding the p-rank of certain class groups in relation to the order of certain groups of units. Under this assumption, which is implied by Ullom's assumption, we give a complete characteristation of $\mathcal{V}_n^+$. Finally, in the case $\lambda = r(p)$ we reprove Ullom's result by first proving that $\mathcal{V}_n^+ \cong (\mathbb{Z}/p^n\mathbb{Z})^{r(p)}$ and then by a direct construction proving that $\mathcal{V}_n^+ \cong V_n^+$. This is done by constructing a special basis for a ring closely related to $\mathbb{Z}C_{p^n}$, consisting of units from a number field.

1. INTRODUCTION

In his talk at the International Congress of Mathematicians in Nice 1970, R.G Swan named calculation of $K_0\mathbb{Z}\pi$ for various groups π as one of the important problems in algebraic K-theory. In the paper [K-M] published in 1977, M. Kervaire and M.P. Murthy took a big step towards solving Swans problem in the case when $\pi = C_{p^n}$ is a cyclic group of prime power order. Before explaining their results we recall that $K_0\mathbb{Z}\pi \cong \mathbb{Z} \oplus \tilde{K}_0\mathbb{Z}\pi$ and that $\tilde{K}_0\mathbb{Z}\pi \cong \operatorname{Pic}\mathbb{Z}\pi$. In this paper we will formulate the result in the language of Picard groups.

From now on, we let p be an odd semi-regular prime, let C_{p^n} be the cyclic group of order p^n and let ζ_n be a primitive p^{n+1}-th root of unity. Kervaire and Murthy

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

prove that there is an exact sequence

$$0 \to V_n^+ \oplus V_n^- \to \operatorname{Pic} \mathbb{Z}C_{p^{n+1}} \to \operatorname{Cl} \mathbb{Q}(\zeta_n) \oplus \operatorname{Pic} \mathbb{Z}C_{p^n} \to 0,$$

where

$$V_n^- \cong C_{p^n}^{\frac{p-3}{2}} \times \prod_{j=1}^{n-1} C_{p^j}^{\frac{(p-1)^2 p^{n-1-j}}{2}}.$$

and $\operatorname{Char}(V_n^+)$ injects canonically in the p-component of the ideal class group of $\mathbb{Q}(\zeta_{n-1})$.

The exact sequence originates as a Mayer-Vietoris sequence of a certain pull-back of rings. Explicitly, V_n is defined by

$$V_n := \frac{(\frac{\mathbb{F}_p[X]}{(X^{p^n}-1)})^*}{\operatorname{Im}\{\mathbb{Z}[\zeta_n]^* \times (\frac{\mathbb{Z}[X]}{(X^{p^n}-1)})^* \to (\frac{\mathbb{F}_p[X]}{(X^{p^n}-1)})^*\}},$$

where R^* denote the group of units in a ring R (see [K-M] for details). The homomorphism c defined by $X \mapsto X^{-1}$ in $(\frac{\mathbb{F}_p[X]}{(X^{p^n}-1)})^*$ extends to V_n and Kervaire and Murthy define $V_n^+ := \{v \in V_n \ : \ c(v) = v\}$ and $V_n^- := \{v \in V_n \ : \ c(v) = v^{-1}\}$. Getting the exact structure of V_n^- is then just a matter of a straightforward calculation. When they get to the part of the proof that concerns V_n^+ things get much harder, however. Kervaire and Murthy's solution is to consider the group $\mathcal{V}_n^+$ defined by

$$\mathcal{V}_n := \frac{\mathbb{F}_p[x]/(x^{p^n}-1))^*}{\operatorname{Im}\{\mathbb{Z}[\zeta_n]^* \to \mathbb{F}_p[x]/(x^{p^n}-1))^*\}}$$

instead. They make extensive use of Iwasawa- and class field theory to prove that $\operatorname{Char}(\mathcal{V}_n^+)$ injects canonically into $\operatorname{Cl}^{(p)}(\mathbb{Q}(\zeta_{n-1}))$. This is actually enough since V_n is a canonical quotient of $\mathcal{V}_n$ so clearly we have a canonical injection $\operatorname{Char}(V_n^+) \to \operatorname{Char}(\mathcal{V}_n^+)$

Kervaire and Murthy also formulate the following conjectures.

$$V_n^+ = \mathcal{V}_n^+ \tag{1.1}$$

$$\operatorname{Char}(V_n^+) \cong (\frac{\mathbb{Z}}{p^n\mathbb{Z}})^{r(p)}, \tag{1.2}$$

where $r(p)$ is the index of irregularity of the prime p and G^r denotes r copies of a group G.

In the case $n = 1$ both conjectures were proven in [K-M] for semi-regular primes and in [ST1] complete information, without any restriction on p was obtained by Stolin.

In 1978 Ullom proved in [U2] that under a certain condition on the Iwasawa invariants associated to the semi-regular prime p, conjecture 1.2 holds. More explicitly the assumption is the following.

Assumption 1. *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 1 holds then, for even i,

$$e_i V_n \cong \frac{\mathbb{Z}}{p^n\mathbb{Z}} \oplus (\frac{\mathbb{Z}}{p^{n-1}\mathbb{Z}})^{\lambda_{1-i}-1}. \tag{1.3}$$

This yields, under the same assumption, that

$$V_n^+ \cong (\frac{\mathbb{Z}}{p^n\mathbb{Z}})^{r(p)} \oplus (\frac{\mathbb{Z}}{p^{n-1}\mathbb{Z}})^{\lambda - r(p)}, \tag{1.4}$$

where

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

Hence, when $\lambda = r$ we get 1.2. Note however, that if $\lambda > r$, then conjecture 1.2 is false.

In this paper we concentrate on conjecture 1.1, which we will prove under the same assumption on the λ_{1-i}'s Ullom uses. In contrast to what happens to conjecture 1.2 we prove that 1.1 hold even if $\lambda > r$ (only assuming Assumption 1). We also discuss two different assumptions, both concerning the p-rank of certain class groups. Under the weaker one of these assumptions we calculate the structure of $\mathcal{V}_n^+$. Under the stronger we prove both Kervaire-Murthy conjectures by constructing a certain basis for a p-adic completion of $\mathbb{Z}C_{p^n}^+ := \{a \in \mathbb{Z}C_{p^n} \ : \ c(a) = a\}$, where c is the canonical involution of $\mathbb{Z}C_{p^n}$ defined above.

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 pull-back 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

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

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 pull-back diagram

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

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 pull-back 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, $\operatorname{Pic} \mathbb{Z}[\zeta_n] \cong \operatorname{Cl} \mathbb{Z}[\zeta_n]$. 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

$$0 \to V_n \to \operatorname{Pic} A_{0,n+1} \to \operatorname{Cl} \mathbb{Z}[\zeta_n] \oplus \operatorname{Pic} A_{0,n} \to 0.$$

Note that definition of V_n is slightly different from the one from [K-M] but the two groups are isomorphic. 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 $(a_l, \ldots, a_m, \ldots, a_0)$ 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*

$$\begin{array}{ccc} & & \mathbb{Z}[\zeta_{k+l}] \\ & \overset{N_{k,l}}{\swarrow} & \Big\downarrow {\scriptstyle f_{k,l}} \\ A_{k,l} & \xrightarrow{g_{k,l}} & D_{k,l} \end{array}$$

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

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

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 the proof we notice an immediate consequence of the commutativity of the diagram in Proposition 2.1.

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

Proof. 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 $x_{k,l} \mapsto x_{k+1,l}$.
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 statement will follow from the lemma below.

Lemma 2.4. *The diagram*

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

is commutative

Proof. 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 $N(a,b) = (N(a), N(b)) \in A_{k-1,l}$. We now use induction on l. If $l = 1$ the statement is well known. Suppose the diagram corresponding to the one above, but with i replaced by $i-1$, is commutative for all k. If $a \in \mathbb{Z}[\zeta_{k+l}]$ we have

$$N(N_{k,l}(a)) = N(N((a, N_{k+1,l-1}(a))) = ((N(N(a)), N(N(N_{k+1,l-1}(a))))$$

and

$$N_{k-1,l}(N(a)) = (N(N(a)), N(N_{k,l-1}(N(a)))).$$

By the induction hypothesis $N_{k,l-1} \circ N = N \circ N_{k+1,l-1}$ 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 $\epsilon \mapsto (\epsilon, N_{k,l}(e))$. 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. $\ker(g_{k,l}|_{\mathbb{Z}[\zeta_{k+l-1}]^*}) = \{\epsilon \in \mathbb{Z}[\zeta_{k+l-1}]^* \,:\, \epsilon \equiv 1 \mod \lambda_{k+l-1}^{p^{k+l}-p^k}\}$

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 $a \equiv 1 \mod p$ in $\mathbb{Z}[\zeta_{k+l-1}]$, $N_{k,l-1}(a) \equiv 1 \mod p$ in $A_{k,l-1}$ and that $f_{k,l-1}\big(\frac{a-1}{p}\big) = g_{k,l-1}\big(\frac{N_{k,l-1}(a)-1}{p}\big)$. 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 necessary information.

If for example $l = 2$, we get after just one step $a \equiv 1 \mod p$ in $\mathbb{Z}[\zeta_{k+1}]$, $N(a) \equiv 1 \mod p$ and $N(\frac{a-1}{p}) \equiv \frac{N(a)-1}{p} \mod p$ 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 $N(a) \equiv 1 \mod p^2$ and hence that $N(\frac{a-1}{p}) \equiv 0 \mod p$. By analyzing how the norm acts one can show that this means that $a \equiv 1 \mod \lambda_k^{p^{k+2}-p^k}$

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 $A_l := A_{k,l}$, $D_l := D_{k,l}$, $g_l := g_{k,l}$, $f_l := f_{k,l}$, $i_l := i_{k,l}$, $j_l := j_{k,l}$ and $N_l := N_{k,l}$.

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] since, by Lemma 3.3, $N : \mathbb{Z}[\zeta_n]^* \to \mathbb{Z}[\zeta_{n-1}]^*$ is surjective when p i semi-regular.

3. On Conjecture 2

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 3.1. *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.

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

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 3.1 we will state and a lemma, which is well-known.

Lemma 3.3. *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 3.1. 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

$$\begin{aligned} |\frac{U_{n-1,1}}{U_{n-1,p^n-1}}| &= |\frac{U_{n-1,1}}{U_{n-1,p^{n-1}-1}}||\frac{U_{n-1,p^{n-1}-1}}{U_{n-1,p^{n-1}+1}}||\frac{U_{n-1,p^{n-1}+1}}{U_{n-1,p^n-1}}| = \\ &= |\frac{U_{n-1,1}}{U_{n-1,p^{n-1}-1}}||\frac{U_{n-1,p^{n-1}-1}}{U_{n-1,p^{n-1}+1}}||\frac{U_{n-1,p^{n-1}+1}/(U_{n-1,p^{n-1}+1})^p}{U_{n-1,p^n-1}/(U_{n-1,p^{n-1}+1})^p}| = \\ &= |\frac{U_{n-1,1}}{U_{n-1,p^{n-1}-1}}||\frac{U_{n-1,p^{n-1}-1}}{U_{n-1,p^{n-1}+1}}||\frac{U_{n-1,p^{n-1}+1}}{(U_{n-1,p^{n-1}+1})^p}||\frac{U_{n-1,p^n-1}}{(U_{n-1,p^{n-1}+1})^p}|^{-1} \end{aligned} \tag{3.1}$$

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 3.1.

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 3.1. 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

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

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 3.3 we have a commutative diagram

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

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

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

This finally gives

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

which is what we wanted to show.

□

Recall that $\lambda_k\mathbb{Z}[\zeta_{k+1}] = \lambda^p_{k+1}$ as ideals in $\mathbb{Z}[\zeta_{k+1}]$. By Lemma 3.2, 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

$$\frac{U_{k,p^{k+1}-1}}{(U_{k,p^k+1})^{(p)}} \to \frac{U_{k+1,p^{k+2}-1}}{(U_{k+1,p^{k+1}+1})^{(p)}}. \tag{3.2}$$

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 3.2 is injective. This shows that the sequence $\{r_k\}$ non-decreasing.

Since it is known by for example [K-M] that $|\mathcal{V}_1^+| = p^{r_0}$, by induction and Proposition 3.1 we now immediately get:

Proposition 3.4. $|\mathcal{V}_n^+| = p^{r_0+r_1+\ldots+r_{n-1}}$.

On the other hand, recall that [K-M] provide us with an injection of $\mathrm{Char}(\mathcal{V}_n^+)$ into $\mathrm{Cl}^{(p)}(\mathbb{Q}(\zeta_{n-1}))^-$, the p-component of the class group of $\mathbb{Q}(\zeta_{n-1})$. This shows that the number of elements in $\mathcal{V}_n^+$ is bounded by the number of elements in $\mathrm{Cl}^{(p)}(\mathbb{Q}(\zeta_{n-1}))^-$. By Iwasawa's theorem, there are numbers $\lambda \geq 0$, $\mu \geq 0$ and ν such that $|\mathrm{Cl}^{(p)}(\mathbb{Q}(\zeta_{n-1})^-| = p^{\lambda(n-1)+\mu p^n+\nu}$ for all n big enough. It has later been proved that $\mu = 0$. This immediately implies the following proposition.

Proposition 3.5. *There is a number n_0 such that for $n \geq n_0$, $|\mathcal{V}_n^+| \leq p^{\lambda(n-1)+\nu}$*

By comparing the sequences $\{r_0 + r_1 + \ldots + r_{n-1}\}$ and $\{\lambda(n-1)+\nu\}$ for big n, remembering that r_k is non-decreasing, we now obtain the following

Proposition 3.6. *$r_k \leq \lambda$ for all k and that there exists a number N such that $r_{N+k} = r_N$ for all $k \geq 0$.*

Now recall that if Assumption 1 is satisfied, then 1.4 holds so

$$|V_n^+| = p^{r_0 n+(\lambda-r_0)(n-1)} = p^{\lambda(n-1)+r_0}.$$

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 $k = 1, 2, \ldots$.

Lemma 3.7. *When Assumption 1 holds $r_k = \lambda$ for all $k = 1, 2, \ldots$.*

The following theorem is now immediate.

Theorem 3.8. *If Assumption 1 holds, then $\mathcal{V}_n^+ = V_n^+$.*

We end this section by discussing another type of assumption on the semi-regular prime p.

Assumption 2. $\text{rank}_p(\text{Cl}^{(p)}(\mathbb{Q}(\zeta_n))^-) = r_n$.

This assumption always holds for $n = 0$. Note that by the proof of Proposition 4.1, the $\text{rank}_p(\text{Cl}^{(p)}(\mathbb{Q}(\zeta_n))^-)$ is always greater or equal to r_n. Under Assumption 1 it follows from [K-M] and [U2] that $\text{rank}_p(\text{Cl}^{(p)}(\mathbb{Q}(\zeta_n))^-) = \lambda$ when $n = 1, 2, \ldots$. This and Lemma 3.7 means that Assumption 1 implies Assumption 2. It is worth noting that Assumption 2 implies that the character group of S_n/pS_n, where $S_n = \text{Cl}^{(p)}(\mathbb{Q}(\zeta_n))^-$, is generated by units from $U_{n,p^{n+1}-1}$.

Again, recall that $r_0 = r(p)$ and that the sequence $\{r_k\}$ is non-decreasing.

Theorem 3.9. *If Assumption 2 holds*

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

Before the proof we need some results.

Lemma 3.10. *There exists a surjection* $\pi_n : \mathcal{V}_n^+ \to \mathcal{V}_{n-1}^+$.

Proof of Lemma 3.10. 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 $\mathcal{V}_n^+ \to \mathcal{V}_{n-1}^+$. □

Proposition 3.11. *For any semi-regular prime* p, $\ker \pi_n \cong (\mathbb{Z}/p\mathbb{Z})^{r_{n-1}}$.

Proof. Proposition 3.1 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 $\epsilon \in U_{n-2,1} \subset \mathbb{Z}[z_{n-2}]$. 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 3.3 that the norm map N_{n-1} restricted 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 pull-back 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 $D^{*+}_{n,(k)} := \{a \in D^{*+}_n : a \equiv 1 \bmod (x-1)^k\}$. Then

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

Now note that if $b \in D^{*+}_{n,(p^{n-1})}$, then $b^p = 1$ so such a unit clearly has order p. We will show that any unit $a \in D^{*+}_{n,(p^{n-1}-1)}$ can be written as $a = bg_1(\epsilon)^k$ for some $b \in D^{*+}_{n,(p^{n-1})}$, 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 $e_{p^{n-1}-1} \in \mathbb{Z}[z_{n-2}]$, not divisible by λ_{n-1}, and some $t \in \mathbb{Z}$. If $a = 1 + a_{p^{n-1}-1}(x_{n-1} - x_{n-1}^{-1})^{p^{n-1}-1} + \ldots \in D^{*+}_{n,(p^{n-1}-1)}$, $a_{p^{n-1}-1} \in \mathbb{F}_p^*$, choose k such that $ke_{p^{n-1}-1} \equiv a_{p^{n-1}-1} \mod p$. Then it is just a matter of calculations to show that $a = bg_1(\epsilon)^k$, where $b \in D^{*+}_{n,(p^{n-1})}$, which concludes the proof □

Proof of Theorem 3.9. 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 $n-1$. There are no elements in D^*_n with order greater than p^n and hence there are no elements in $\mathcal{V}^+_n$ with order greater than p^n. Since $\mathcal{V}^+_n$ is a p-group,

$$\mathcal{V}^+_n \cong \left(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\right)^{a_n} \oplus \left(\frac{\mathbb{Z}}{p^{n-1}\mathbb{Z}}\right)^{a_{n-1}} \oplus \ldots \oplus \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^{a_1}.$$

By Proposition 3.11 and the assumption we have an exact sequence

$$0 \to \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^{r_{n-1}} \to \bigoplus_{i=1}^{n} \left(\frac{\mathbb{Z}}{p^i\mathbb{Z}}\right)^{a_i} \to \bigoplus_{i=1}^{n-2} \left(\frac{\mathbb{Z}}{p^i\mathbb{Z}}\right)^{r_{(n-1)-i} - r_{(n-2)-i}} \oplus \left(\frac{\mathbb{Z}}{p^{n-1}\mathbb{Z}}\right)^{r_0} \to 0.$$

The injection from [K-M], $\mathcal{V}^+_n \to \operatorname{Char} \mathrm{Cl}^{(p)}(\mathbb{Q}(\zeta_{n-1}))^-)$ together with Assumption 2 means $\mathcal{V}^+_n$ has at most r_{n-1} generators. Hence $\mathcal{V}^+_n$ has exactly r_{n-1} generators and we get

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

□

4. The Kervaire-Murthy conjectures when $r_n = r(p)$

We now proceed by making a different assumption under we will give a constructive proof of the two Kervaire-Murthy conjectures.

Assumption 3. $\operatorname{rank}_p(\mathrm{Cl}^{(p)}(\mathbb{Q}(\zeta_n))^-) = r(p)$ *for all* n.

This holds for example if the Iwasawa invariant λ satisfy $\lambda = r(p) =: r$ which follows from, for instance, certain congruence assumptions on Bernoulli numbers (see page 202 in [W]). Under this assumption we can prove the following proposition.

Proposition 4.1. *Let p be an odd semi-regular, prime and let $r = r(p)$ be the index of irregularity of p. Suppose the Assumption 3 holds. Then $p^{r_n} := \left|\frac{U_{n,p^{n+1}-1}}{(U_{n,p^n+1})^p}\right| = p^r$ for all $n \geq 0$.*

Again, since it is proved in [K-M] that $\mathcal{V}_1^+ \cong (\mathbb{Z}/p\mathbb{Z})^r$, induction and Propositions 4.1 and 3.1 now gives us the following theorem.

Theorem 4.2. *When Assumption 3 holds, $|\mathcal{V}_n^+| = p^{nr}$.*

Proof of Proposition 4.1. By Lemma 3.2 we need to calculate the number $|U_{n,p^{n+1}+1}/(U_{n,p^n+1})^p|$. Denote the field $\mathbb{Q}(\zeta_n)$ by K_n and let L_n be the maximal unramified extension of K_n of period p. Clearly, $G_n := \mathrm{Gal}(L_n/K_n) = \mathrm{Cl}^{(p)}(K_n)/p\,\mathrm{Cl}^{(p)}(K_n)$. By the assumption $|G_n| = p^r$. It is known by Iwasawa theory that $G_n = G_n^-$. If $\epsilon \in U_{n,p^{n+1}+1}$ it follows from local considerations that the extension $K_n \subseteq K_n(\sqrt[p]{\epsilon})$ is unramified so $K_n(\sqrt[p]{\epsilon}) \subseteq L_n$. Using Kummer's pairing we get a bilinear map $G_n \times U_{n,p^{n+1}+1} \to \langle\zeta_0\rangle$, $(\sigma, \epsilon) \mapsto \sigma(\epsilon)\epsilon^{-1}$. The kernel on the right is obviously the group of all p-th powers in $U_{n,p^{n+1}+1}$ which is $(U_{n,p^n+1})^p$. It is enough to prove that the kernel on the left is trivial. Then, $\frac{U_{n,p^{n+1}+1}}{(U_{n,p^n+1})^p} \cong \mathrm{Char}(G_n^-)$. Since $|G_n^-| = p^r$ this proves the theorem. Suppose $< \sigma, \epsilon >= 1$ for all ϵ. If we can show that every unramified extension $K_n \subset L$ of degree p is given by $L = K_0(\gamma)$, where γ is a p-th root of some $\epsilon \in U_{n,p^{n+1}+1}$ we are done. Again, $|G_n^-| = p^r$, so there are r distinct unramified extensions of degree p. We now use induction. Let $n = 0$ and suppose $K_0 \subset L$ is an unramified extension of degree p. It is well known that such an extension can be generated by $\sqrt[p]{\epsilon}$ for some unit ϵ. If $\epsilon \in U_{0,s}$ and $\epsilon \notin U_{0,s+1}$, then local considerations show that $s \leq p-1$ implies that $K_0 \subset K_0(\sqrt[p]{\epsilon})$ is ramified. Hence $L = K_0(\sqrt[p]{\epsilon})$ where $\epsilon \in U_{0,p} = U_{0,p+1}$. Now suppose every unramified extension of K_{n-1} is given by a p-th root of a unit, that is we have r units $\epsilon_1, \ldots, \epsilon_r \in U_{n-1,p^n+1}$ such that each distinct extension E_i, $i = 1, 2, \ldots r$ is generated by a p-th root of ϵ_i. Consider ϵ_i as elements of K_n. A straightforward calculation shows that $\epsilon_i \in U_{n,p^{n+1}+1}$. Hence a p-th root of ϵ_i either generate an unramified extension of K_n of degree p or $\sqrt[p]{\epsilon_i} \in K_n$. The latter case can not hold since then we would get $E_i = K_n$ which is impossible since E_i is unramified over K_{n-1} while K_n is not. Hence we have found r distinct extension of K_n and this concludes the proof. □

Now recall that for $n = 1$ it is proved in [K-M] that $\mathcal{V}_1^+ \cong (\mathbb{Z}/p\mathbb{Z})^r$. Suppose the result holds for all $k \leq n$. Then $\mathcal{V}_{n-1}^+ \cong (\mathbb{Z}/p^{n-1}\mathbb{Z})^r$ and the surjection

$\pi_n : \mathcal{V}_n^+ \to \mathcal{V}_{n-1}^+$ from Lemma 3.10 means that $\mathcal{V}_n^+$ has at least r generators. By our assumption $\mathrm{Cl}^{(p)}\,\mathbb{Q}(\zeta_{n-1})$ has r generators and by using the injection $\mathrm{Char}\,\mathcal{V}_n^+ \to \mathrm{Cl}^{(p)}\,\mathbb{Q}(\zeta_{n-1})$ we get that $\mathcal{V}_n^+$ has at most, and hence by above exactly r generators. By Theorem 4.2 $|\mathcal{V}_n^+| = p^{rn}$. Since no elements in D_n^{*+} and hence no elements in $\mathcal{V}_n^+$ have order greater than p^n we now get the following theorem by induction.

Theorem 4.3. *Let p be a semi-regular prime and r the index of irregularity. If Assumption 3 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

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

Since N_{n-1} is additive $\mod p$ one can show with some simple calculations that Φ is a group homomorphism. See Lemmas 4.9 and 4.16 for details.

Explicitly, what we want to prove is the following.

Theorem 4.4. *If Assumption 3 holds, then Φ is a surjective group homomorphism.*

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

Corollary 4.5. *If Assumption 3 holds, then $V_n^+ = \mathcal{V}_n^+$*

Actually, what we need to prove the theorem and the corollary is the conclusion of Theorem 4.3 rather than Assumption 3 itself.

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 $\gamma \in A_{n-1}^{*+}$, $\gamma \equiv 1 \mod p$ 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

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

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

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

But the left hand side is exactly $\Phi(\epsilon)$ so the corollary really does follow from Theorem 4.4 □

We now proceed to start proving Theorem 4.4. 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_{2i_k} (in reduced form) is divisible by p.

Let $\bar{E_n} : D_n \to D_n^*$ be the truncated exponential map defined by

$$\bar{E_n}(y) = 1 + y + \frac{y^2}{2!} + \dots + \frac{y^{p-1}}{(p-1)!}$$

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

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

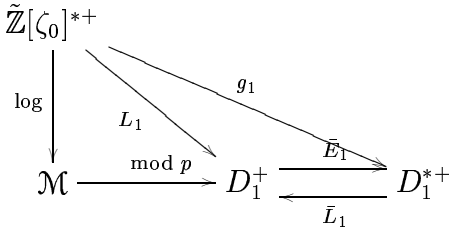
We also consider the usual λ-adic log-map defined by a power series as usual.

Denote the cyclotomic units of $\mathbb{Z}[\zeta_0]^{*+}$ by C_0^+. C_0^+ is generated by -1 and the units $\theta_j := \sin(j\pi/p)/\sin(\pi/p)$, $j = 2, \dots, (p-1)/2$. (Details can be found in [W] p 144.) We now follow [B-S], page 368-375. Let $\mathcal{M}$ be the group of real λ_0-adic integers with zero trace. By Lemma 1, page 368 of [B-S] there is a unique λ_0-adic integer $\tilde{\lambda}_0$ such that $\tilde{\lambda}_0 + p = 0$ and $\tilde{\lambda}_0 \equiv (\zeta_0 - 1) = \lambda_0 \mod \tilde{\lambda}_0^2$. Any $a \in \mathcal{M}$ can be uniquely presented as $a = \sum_{i=1}^{m-1} b_i \tilde{\lambda}_0^{2i}$, $m = (p-1)/2$. Consider the homomorphism $\Psi : \mathbb{Z}[\zeta_0]^* \to \mathcal{M}$ defined by $\epsilon \mapsto \log(\epsilon^{p-1})$. It turns out that $\Psi(\theta_j) = \sum_{i=1}^{m-1} b_{j,i} \tilde{\lambda}_0^{2i}$ where

$$b_{j,i} \equiv \frac{B_{2i}(1-j^{2i})}{(2i)!2i} \mod p \; 2 \le j \le m, \; 1 \le i \le m-1.$$

We see that there are exactly r $\tilde{\lambda}_0^{2i}$, namely $\tilde{\lambda}_0^{2i_k}$, such that $\tilde{\lambda}_0^{2i} \notin \Psi(C_0^+)$. Let $\tilde{g}_0 : \mathcal{M} \to D_1^+$ denote taking classes mod p. Then, for exactly the r indexes $i_1, i_2 \dots i_r$ we have $(\bar{x}_1 - 1)^{2i_k} \notin \tilde{g}_1(\Psi(C_0^+))$. Suppose $(x-1)^{2i_s} = \tilde{g}_1(\log \epsilon)$ for some $\epsilon \in \mathbb{Z}[\zeta_0]^{*+}$. Let h^+ be the class number of $\mathbb{Q}(\zeta_0)$. It is well known that $|\mathbb{Z}[\zeta_0]^{*+}/C_0^+| = h^+$. Hence there exists s, $(s,p) = 1$, such that $\epsilon^s \in C_0^+$ and u, v such that $1 = s(p-1)u + pv$. Then $\epsilon = \epsilon^{s(p-1)u+pv} = (\epsilon^s u)^{p-1}\epsilon^{pv}$ so $\log((\epsilon^s u)^{p-1}) = \log\epsilon - pv\log\epsilon \equiv \log\epsilon \equiv (x-1)^{2i_s}$, which is a contradiction. Hence $(x-1)^{2i_s} \notin g_1(\log \mathbb{Z}[\zeta_0]^{*+})$. The matrix for changing basis from $\{x_1 - 1\}$ to $\{x_1 - x_1^{-1}\}$ is upper triangular so we also get that$(x - x^{-1})^{2i_s} \notin g_1(\log \mathbb{Z}[\zeta_0]^{*+})$.

Since formally, $\exp(\log(1+y)) = 1+y$ it is not hard to see that $E_0(L_0(1+y)) \equiv 1+y \mod p$ 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_0 and do some simple calculations we get the proposition below. For $n \geq 1$ and $2 \leq 2s \leq p^n - 3$, define

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

Proposition 4.6. *The r elements $\bar{E}_1((x_1 - x_1^{-1})^{2i_k})$ generate $D_1^{*+}/g_1(\mathbb{Z}[\zeta_0]^{*+})$. Moreover, $t_{1,2s} = |\{B_{2i_k} : B_{2i_k} > 2s\}|$.*

We now want to lift this result to D_n^{*+}. From now on (excepting Lemma 4.13) we will denote the generator $x \in D_n$ by x_n.

Proposition 4.7. *Suppose Assumption 3 holds. Then the r elements $\bar{E}_n((x_n - x_n^{-1})^{2i_k})^{p^{n-1}}$ generate the group $\mathcal{V}_n^+ := D_n^{*+}/g_n(\mathbb{Z}[\zeta_{n-1}]^{*+})$. Moreover, $t_{n,2s} = |\{B_{2i_k} : p^{n-1}B_{2i_k} > 2s\}|$.*

Before the proof we state a corollary

Corollary 4.8. *If $2s \geq p^n - 3p^{n-1}$, then $t_{n,2s} = 0$.*

Proof. Induction on n. If $n = 1$ this is exactly Proposition 4.6. Suppose the statement holds for the index equal to $n-1$. The diagram

$$\begin{array}{ccc} \mathbb{Z}[\zeta_n]^{*+} & \longrightarrow & D_n^{*+} \\ \downarrow{\scriptstyle \tilde{N}_{n,1}} & & \downarrow \\ \mathbb{Z}[\zeta_{n-1}]^{*+} & \longrightarrow & D_{n-1}^{*+} \end{array} \tag{4.1}$$

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, $z_n^p \notin \operatorname{Im} \mathbb{Z}[\zeta_{n-1}]^*$. This follows from the fact that $\mathcal{V}_k^+ \cong (\mathbb{Z}/p^k\mathbb{Z})^r$. 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 the assumption and by above since $\bar{E_n}((x_n - x_n^{-1})^{2i_k})^{p^{n-2}}$ clearly map onto $\bar{E_n}((x_n - x_n^{-1})^{2i_k})^{p^{n-2}} \notin g_{n-1}(\mathbb{Z}[\zeta_{n-1}]^{*+})$. By 4.3 we have control over a full set of generators of $\mathcal{V}_n^+$ and the proposition follows. □

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 $\varphi(\gamma) = N_{n-1}\big(\frac{\gamma-1}{p}\big) \mod p$.

Lemma 4.9. *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}.*

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 $N_{n-1}(\epsilon) \equiv 1 \mod p$,

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

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 $\gamma \in U_{n-1,p^n-1}$. □

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

Proposition 4.10. *If Assumption 3 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 4.11. *Suppose Assumption 3 holds, Then*

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

Before the proof we need a lemma. Recall that $\mathbb{Z}[\zeta_{n-1}]^*$ is identified with its image in A_n^* under the map $\epsilon \mapsto (\epsilon, N_{n-1}(\epsilon))$.

Lemma 4.12. *Let $1 \le s \le p^n - p^{n-1}$. $\epsilon \in U_{n-1,s}$ if and only if $g_n(\epsilon) \in D_{n,(s)}^+$.*

Proof. We have a commutative diagram

$$\begin{array}{ccc} A_n^* & \longrightarrow & \mathbb{Z}[\zeta_{n-1}]^{*+} \\ \downarrow \text{mod } p & & \downarrow \text{mod } p \\ D_n^* \cong \left(\frac{\mathbb{F}_p[x]}{(x-1)^{p^n-1}}\right)^* & \longrightarrow & \left(\frac{\mathbb{F}_p[x]}{(x-1)^{p^n-p^{n-1}}}\right)^* \end{array} \tag{4.2}$$

induced by natural the surjection. The lemma follows directly. □

Proof of Proposition 4.11. Recall that $|D_{n-1}^+| = p^{\frac{p^{n-1}-1}{2}}$ so we need to prove that

$$\left|\frac{U_{n-1,p^n-p^{n-1}}}{U_{n-1,p^n-1}}\right| = p^{\frac{p^{n-1}-1}{2}}.$$

By the lemma above and Lemma 2.6 g_n induces a well defined and injective homomorphism

$$\frac{U_{n-1,p^n-p^{n-1}}}{U_{n-1,p^n-1}} \to D_{n,(p^n-p^{n-1})}^{*+}.$$

By Corollary 4.8 this map is surjective and hence an isomorphism. Since we trivially have $|D_{n,(p^n-p^{n-1})}^{*+}| = p^{\frac{p^{n-1}-1}{2}}$, this proves the Proposition. □

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

Lemma 4.13. *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 $\tilde{N}_{n,1}$, $1 \leq n, 1 \leq k < n$, 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 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 $s = 1$ we in the lemma above we immediately get the following theorem.

Theorem 4.14. *Let $2 \le n$ and $1 \le k < n$. 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 4.15. *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 4.16. *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

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

and $\tilde{N}_{n-1,k}(\gamma) \equiv 1 \mod p^2$ for all $k = 1, 2, \ldots, n-1$. 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 4.13. 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 divides a. In this language we can combine Thereom 4.14 and Proposition 4.15 to the following lemma.

Lemma 4.17. *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 $p^n - p^k \leq \mathcal{O}(\tilde{\varphi}(\epsilon)) < p^n - p^{k-1} \leq \mathcal{O}(\tilde{\omega}(\epsilon))$.*

Proposition 4.18. *The map $\tilde{\Phi} := \tilde{\varphi} - \tilde{\omega}$ is an isomorphism.*

Proof. By Proposition 4.10 φ is an isomorphism. Hence there exists (classes of) units $\epsilon_i, i = 1, 2, \ldots, (p^{n-1} - 1)/2$ such that the set $\varphi(\epsilon_i)$ forms a basis for D^+_{n-1}.

If $a \in D^+_{n-1}$ there exist unique a_i such that $a = \sum_1^{(p^{n-1}-1)/2} a_i\varphi(\epsilon_i)$. To prove the Proposition it is enough to show that the map

$$\sum_1^{(p^{n-1}-1)/2} a_i\varphi(\epsilon_i) \mapsto \sum_1^{(p^{n-1}-1)/2} a_i(\varphi(\epsilon_i) - \omega(\epsilon_i))$$

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 $\varphi(\epsilon_i) \mapsto \omega(\epsilon_i)$. By Lemma 4.17 the matrix M' is a lower diagonal matrix with zeros on the diagonal. This means M is lower triangular with ones on the diagonal and hence invertible. □

Proof of Theorem 4.4. The map $\tilde{\Phi}$ is obviously induced by Φ which hence must be surjective by prop 4.18. □

5. Final remarks

We end this paper with some further discussion about how one can find a basis for the groups D^+_n. In the proof of Theorem 4.4 the main idea was that one could find a basis for D^+_n consisting of the image of certain elements from $\mathbb{Z}[\zeta_{n-2}]$ under a certain mapping. To be a bit more specific we can formulate this as a corollary to Proposition 4.10.

Corollary 5.1. *There is a basis for D^+_n consisting of elements $g_n(N_n(\frac{\epsilon-1}{p}))$, where $\epsilon \in U_{n,p^{n+1}-p^n}$.*

Recall that this was proved under Assumption 3 ($r_k = r(p)$ for all k). Now suppose Assumption 1 holds instead. Then, by Lemma 3.7, $r_k = \lambda$ for $k = 1, 2, \ldots$ and $r_0 = r(p)$. From Theorem 3.8 and Ullom's result we conclude $\mathcal{V}^+_k$ has λ generators for all $k \geq 2$ and all of these generators have exponent at least p^{k-1}. In particular, $\mathcal{V}^+_k(p) \cong (\mathbb{Z}/p\mathbb{Z})^\lambda$ and hence coincides with $ker\,\pi_k$ by Proposition 3.11 and Lemma 3.7. Here for any abelian p-group A we denote by $A(p^k)$ the subgroup generated by all elements of A of exponent p^k.

It follows from the proof of Proposition 3.11 that there exist λ elements $a_i = 1 + (x_2 - 1)^{p+s_i} \in D^{*+}_{2,(p+1)}$, $1 \leq s_i \leq p^2 - p - 3$, which generate $\mathcal{V}^+_2(p)$ (see the proof of Proposition 3.11 for the definition of $D^{*+}_{k,(t)}$).

The natural projection $D^{*+}_{3,(p+1)} \to D^{*+}_{2,(p+1)}$. induces the following exact sequence

$$0 \to ker\,\pi_3 \to \mathcal{V}^+_3(p^2) \to \mathcal{V}^+_2(p) \to 0$$

which reads as

$$0 \to (\mathbb{Z}/p\mathbb{Z})^{\lambda} \to (\mathbb{Z}/p^2\mathbb{Z})^{\lambda} \to (\mathbb{Z}/p\mathbb{Z})^{\lambda} \to 0.$$

Let us consider elements $b_i = 1 + (x_3 - 1)^{p+s_i} \in D^{*+}_{3,(p+1)}$. The commutativity of the diagram 4.1 implies that images of b_i are nontrivial in $\mathcal{V}_3^+$. Moreover, Proposition 3.11 implies again that b_i are not in $\ker \pi_3$ and therefore all b_i have exponent p^2 and generate $\mathcal{V}_3^+(p^2)$. Thus, we can conclude that $b_i^p = 1 + (x_3 - 1)^{p^2+ps_i}$ are not in the image of $\mathbb{Z}[\zeta_2]^*$. On the other hand $p^2+p \leq p^2+ps_i \leq p^3-3p$ and b_i^p generate

$$\ker \pi_3 = \frac{D^{*+}_{3,(p^2+1)}}{g_3(\mathbb{Z}[\zeta_2]^{*+}) \cap D^{*+}_{3,(p^2+1)}}.$$

Now by using the exact same technique as in the proof of Lemma 4.13 we can extend Lemma 4.12 to.

Lemma 5.2. *Let $1 \leq s \leq p^n - 1$. $\epsilon \in U_{n-1,s}$ if and only if $g_n(\epsilon) \in D^{+}_{n,(s)}$.*

This implies that

$$\ker \pi_3 = \frac{D^{*+}_{3,(p^2+1)}}{g_3(U_{2,\,p^2+1})}.$$

It follows that $D^{*+}_{3,(p^3-3p+2)} \subset g_3(\mathbb{Z}[\zeta_2]^*)$. Proceeding in the same way we obtain the following

Lemma 5.3. *Let $n \geq 3$. If $a \in D^{*+}_{n,(p^n-3p^{n-2}+2)}$, then $a \in g_n(\mathbb{Z}[\zeta_{n-1}]^*)$.*

From this lemma, just as in the proof of Proposition 4.11, we get the following proposition.

Proposition 5.4. *Suppose Assumption 1 holds. Then*

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

Now define $\varphi_2 : U_{n,p^{n+1}-p^{n-1}} \to D^{+}_{n-1}$ by $\varphi_2(\gamma) = g_{n-1}(N_{n-1}(\frac{1}{p}\tilde{N}_{n-1,1}(\frac{\gamma-1}{p})))$. We remind the reader that $\tilde{N}_{n-1,1}$ is the usual norm $\mathbb{Z}[\zeta_n] \to \mathbb{Z}[\zeta_{n-1}]$ and $N_{n-1} : \mathbb{Z}[\zeta_{n-1}] \to A_{n-1}$ is our "standard" multiplicative map. By observing that

$$\frac{1}{p}\tilde{N}_{n-1,1}(\frac{\gamma-1}{p}) = \tilde{N}_{n-1,1}(\frac{\gamma-1}{\lambda_n^{p^n-p^{n-1}}p})$$

and then using the proceeding exactly as in the proof of Lemma 4.9 we see that φ_2 is a homomorphism. A straightforward calculation gives us that $\ker \varphi_2 =$

$U_{n,p^{n+1}-1}$. We hence get an induced injective homomorphism

$$\tilde{\varphi_2} : \frac{U_{n,p^{n+1}-p^{n-1}}}{U_{n,p^{n+1}-1}} \to D^+_{n-1}.$$

Since

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

this map is surjective. Therefore we get the following proposition.

Proposition 5.5. *Suppose Assumption 1 holds. Then there exists a basis for D^+_{n-1} consisting of elements $\varphi_2(\gamma)$ where $\gamma \in U_{n,p^{n+1}-p^{n-1}}$.*

If we analyze the proof above we see that we really only require that $r_1 = r_2 = \text{rank}(\mathcal{V}^+_n)$, $n \geq 1$ ($\text{rank}(\mathcal{V}^+_n)$ is the number of generators of $\mathcal{V}^+_n$) for Proposition 5.5 to hold. We know from Proposition 3.6 that $r_N = r_{N+k}$ for some N and all k and if Assumption 2 is true, then $r_N = r_{N+k} = \text{rank}(\mathcal{V}^+_{N+k})$, $k \geq 0$. In this case it follows that we have the following exact sequence

$$0 \to ker\, \pi_{N+1} \to \mathcal{V}^+_{N+1}(p^2) \to \mathcal{V}^+_N(p) \to 0$$

and the following two statements are now straightforward.

Lemma 5.6. *Suppose Assumption 2 holds. Then $D^{*+}_{n,(p^n-3p^{n-N}+2)} \subset g_n(\mathbb{Z}[\zeta_{n-1}]^*)$ for $n \geq N+1$.*

Proposition 5.7. *Suppose Assumption 2 holds. Then*

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

for $n \geq N+1$.

Now define $\varphi_N : U_{n,p^{n+1}-p^{n-N}} \to D^+_{n-N}$ by

$$\varphi_N(\epsilon) = g_{n-N}(N_{n-N}(\frac{1}{p}\tilde{N}_{n,N}(\frac{\epsilon - 1}{\lambda_n^{p^{n+1}-p^{n-N+1}}}))).$$

As before, it is straightforward to control that φ_N is a homomorphism and that the kernel is $U_{n,p^{n+1}-1}$. We hence get an induced homomorphism

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

Since

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

this map is surjective and we get the following proposition.

Proposition 5.8. *Suppose Assumption 2 holds. Let N be as in Proposition 3.5 and let $n \geq N+1$. Then there exists a basis for D^+_{n-N} consisting of elements $\varphi_N(\gamma)$ where $\gamma \in U_{n,p^{n+1}-p^{n-N}}$.*

As a final note "on the side", it is not hard to show that V_n and $\mathcal{V}_n$ do not differ by too much even without any further assumption on p than semi-regularity. Recall from lemma 2.5 that $A_n^* \cong \mathbb{Z}[\zeta_{n-1}]^* \times B_n$. If $(1,\epsilon) \in B_n$, then $\epsilon \equiv 1 \bmod (p)$ and $\epsilon^p \equiv 1 \bmod (p^2)$ in A^*_{n-2}. This also means that $(\epsilon^p - 1)/p \equiv 0 \bmod (p)$ in A^*_{n-2} which is enough for $(1,e)^p \equiv (1,1) \bmod (p)$ in A^*_{n-1} to hold. By abuse of notation,

$$V_n^+ \cong \frac{\mathcal{V}_n^+}{\mathrm{Im}\{B_n \to \tilde{D}_n^*\}^+}$$

and $\mathrm{Im}\{B_n \to \tilde{D}_n^*\}^+$ consist of elements of exponent p.

References

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

[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. *Fine Structure of Class Groups of Cyclic p-groups*
Journal of Algebra 49 (1977) 112-124.

[U2] 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