ON THE KERVAIRE-MURTHY CONJECTURES

OLA HELENIUS AND ALEXANDER STOLIN

ABSTRACT. Let p be a semi-regular prime, let C_{p^n} be a group of order p^n and let ζ_n be a primitive p^{n+1}-th root of unity. In the present paper we consider the following exact sequence, which can be extracted from the Mayer-Vietoris exact sequence

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

In 1977 Kervaire and Murthy established an exact structure for V_n^-, proved that $\operatorname{Char}(V_n^+) \subseteq \operatorname{Char}(\mathcal{V}_n^+) \subseteq \operatorname{Cl}^{(p)}(\mathbb{Q}(\zeta_{n-1}))$, where V_n is a canonical quotient of $\mathcal{V}_n$, and conjectured that $\operatorname{Char}(V_n^+) \cong (\mathbb{Z}/p^n\mathbb{Z})^r$, where r the index of irregularity of p.

We prove that under a certain extra condition on p, $\mathcal{V}_n \cong \operatorname{Cl}^{(p)}(\mathbb{Q}(\zeta_{n-1})) \cong (\mathbb{Z}/p^n\mathbb{Z})^r$ and $V_n \cong \bigoplus_{i=1}^r (\mathbb{Z}/p^{n-\delta_i}\mathbb{Z})$, where δ_i is 0 or 1.

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 nice 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} by the cyclic group of order p^n and let ζ_n be a primitive p^{n+1}-th root of unity. Kervaire and Murthy 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 $\mathbb{Q}(\zeta_{n-1})$.

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

Their starting point is the Mayer-Vietoris exact sequence associated to the pull-back

$$\begin{array}{ccc} \frac{\mathbb{Z}[X]}{(X^{p^{n+1}}-1)} & \longrightarrow & \mathbb{Z}[\zeta_n] \\ \downarrow & & \downarrow \\ \frac{\mathbb{Z}[X]}{(X^{p^n}-1)} & \longrightarrow & \frac{\mathbb{F}_p[X]}{(X^{p^n}-1)} \end{array}$$

Let R^* denote the group of units in a ring R. V_n is defined as the cokernel

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

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 $\mathcal{V}_n := \mathbb{F}_p[x]/(x^{p^n}-1))^*/\operatorname{Im}\{\mathbb{Z}[\zeta_n]^* \to \mathbb{F}_p[x]/(x^{p^n}-1))^*\}$ instead. They make extensive use of Iwasawa- and class field theory to prove that $\operatorname{Char}(\mathcal{V}_n^+) \subseteq \operatorname{Cl}^{(p)}(\mathbb{Q}(\zeta_{n-1}))$. 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.

$$V_n = \mathcal{V}_n$$

and

$$\operatorname{Char}(\mathcal{V}_n^+) \cong \left(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\right)^r,$$

where r is the index of irregularity of the prime p.

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 this paper we will prove that under an extra condition on the semi-regular prime p, $\operatorname{Char}(\mathcal{V}_n^+) \cong \operatorname{Cl}^{(p)}\mathbb{Q}(\zeta_{n-1}) \cong \left(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\right)^r$. We will also give some information on conjecture number one and prove that $\operatorname{Char}(V_n^+) \cong \bigoplus_i^r \left(\frac{\mathbb{Z}}{p^{n-\delta_i}\mathbb{Z}}\right)$, where $\delta_i \in \{0, 1\}$.

2. Construction of Norm maps

In this section, we construct certain multiplicative maps. In some sense, these maps are the key to the result on Picard groups in the following section.

For $k \geq 0$ and $i \geq 1$, let $A_{k,i} := \mathbb{Z}[x]/(\frac{x^{p^{k+i}}-1}{x^{p^k}-1})$. Note that $A_{n,1} \cong \mathbb{Z}[\zeta_n]$. Before we start we need to do some observations. First, for each $k \geq 0$ and $i \geq 1$ we have a pull-back diagram

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

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

We want to prove the following result.

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

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

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

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

The maps $N_{k,i}$ 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 2.2. *For $k \geq 0$ and $i \geq 1$ we have*

i) $A_{k+1,i}$ is a free $A_{k,i}$-module under $x_{k,i} \mapsto x_{k+1,i}$.

ii) The norm map $N : A_{k+1,i} \to A_{k,i}$, 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 $j \leq i-1$. Let $\varphi = \varphi_{k+1,i} : \mathbb{Z}[\zeta_{k+i}] \to A_{k+1,i}$ be defined by $\varphi(a) = (a, N_{k+1,i-1}(a))$. It is clear that φ is multiplicative. From the lemma above we have a norm map $N : A_{k+1,i} \to A_{k,i}$. Define $N_{k,i} := N \circ \varphi$. It is clear that $N_{k,i}$ is multiplicative. Moreover, $N_{k,i}(\zeta_{k+i}) = N(\zeta_{k+i}, x_{k+1,i-1}) = N(x_{k+1,i}) = x_{k,i}$, 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

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

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

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 2.3. *The diagram*

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

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 $A_{k,i}$ can be represented as a pair $(a,b) \in \mathbb{Z}[\zeta_{k+i-1}] \times A_{k,i-1}$ and an element in $A_{k-1,i}$ can be represented as a pair $(c,d) \in \mathbb{Z}[\zeta_{k+i-2}] \times A_{k-1,i-1}$. If (a,b) represents an element in $A_{k,i}$ one can, directly from the definition, show that $N(a,b) = (N(a), N(b)) \in A_{k-1,i}$.

We now use induction on i. If $i = 1$ 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 $a \in \mathbb{Z}[\zeta_{k+i}]$ we have

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

and

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

By the induction hypothesis $N_{k,i-1} \circ N = N \circ N_{k+1,i-1}$ and this proves the lemma. $\square$

3. Mayer-Vietoris Exact Sequence for $\operatorname{Pic}\mathbb{Z}C_{p^n}$ for 2-regular Primes

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 $n \geq 1$. Hence the Mayer-Vietoris exact sequence

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

associated to the pull-back diagram 2.1 can be used to find information concerning $\operatorname{Pic}\mathbb{Z}C_{p^n}$

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

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

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 still isomorphic. It is easy to see that $D_{0,n} \cong \mathbb{F}_p/(x-1)^{p^{n+1}-1}$. In this group, let $\bar{x}$ denote the class of x. and let $c : D_{0,n}^* \to D_{0,n}^*$ be the automorphism defined by $c(\bar{x}) = \bar{x}^{-1}$. By abuse of notation we also denote the induced map on V_n by c. Define $V_n^+ := \{v \in V_n \ : \ c(v) = v\}$ and $V_n^- := \{v \in V_n \ : \ c(v) = v^{-1}\}$.

We continue with a theorem about the structures of the groups $D_{k,i}^*$. First, let $c : D_{k,i}^* \to D_{k,i}^*$ be the group homomorphism defined by $c(\bar{x}) = \bar{x}$, where $\bar{x}$ denotes the class of x in $D_{k,i}^* \cong \mathbb{F}_p[x]/(x-1)^{p^{k+i}-p^k}$. Clearly, $\mathbb{F}_p^* \subset D_{k,i}^*$ and by the structure theorem for abelian groups, $D_{k,i}^* = \mathbb{F}_p^* \oplus \tilde{D}_{k,i}^*$ where $\tilde{D}_{k,i}^*$ is a p-group. Now define

$$\tilde{D}_{k,i}^{*+} := \{u \in \tilde{D}_{k,i}^* \ : \ c(u) = u\}$$

and

$$\tilde{D}_{k,i}^{*-} := \{u \in \tilde{D}_{k,i}^* \ : \ c(u) = u^{-1}\}.$$

Since $\tilde{D}_{k,i}^*$ is an finite abelian group of odd order and since c has order 2 we get

$$D_{k,i}^* \cong \mathbb{F}_p^* \oplus \tilde{D}_{k,i}^{*+} \oplus \tilde{D}_{k,i}^{*-}.$$

Proposition 3.1. $|\tilde{D}_{0,n-1}^{*+}| = p^{\frac{p^{n-1}-3}{2}}$ *and* $|\tilde{D}_{0,n-1}^{*-}| = p^{\frac{p^{n-1}-1}{2}}$.

Proof. $\tilde{D}_{0,n-1}^*$ can be presented as $\{1+a_1(x-x^{-1})+\ldots+a_{p^{n-1}-2}(x-x^{-1})^{p^{n-1}-2}\}$. Since $c((x-x^{-1})^j) = (-1)^j(x-x^{-1})^j$ it is not hard to see that $\tilde{D}_{0,n-1}^{*-}$ can be represented as $\{1+a_1(x-x^{-1})+a_3(x-x^{-1})^3+\ldots+a_{p^{n-1}-2}(x-x^{-1})^{p^{n-1}-2}\}$. Hence $|\tilde{D}_{0,n-1}^{*-}| = p^{\frac{p^{n-1}-1}{2}}$ and since $|\tilde{D}_{0,n-1}^*| = p^{p^{n-1}-2}$ we get $|\tilde{D}_{0,n-1}^{*+}| = p^{\frac{p^{n-1}-3}{2}}$. □

We will now use our norm maps from section 2 to get an inclusion of $\mathbb{Z}[\zeta_{k+i-1}]^*$ into $A_{k,i}^*$. Define $\varphi_{k,i} : \mathbb{Z}[\zeta_{k+i-1}]^* \to A_{k,i}^*$ be the injective group homomorphism defined by $\epsilon \mapsto (\epsilon, N_{k,i}(e))$. By proposition 2.1, $\varphi_{k,i}$ is well defined. For future use we record this in a lemma.

Lemma 3.2. *Let $B_{k,i}$ be the subgroup of $A_{k,i}^*$ consisting of elements $(1,b)$, $b \in A_{k,i-1}^*$. Then $A_{k,i}^* \cong \mathbb{Z}[\zeta_{k+i-1}]^* \times B_{k,i}$*

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

We now need a technical lemma which is Theorem I.2.7 in [ST3].

Lemma 3.3. $\ker(g_{k,i|_{\mathbb{Z}[\zeta_{k+i-1}]^*}}) = \{\epsilon \in \mathbb{Z}[\zeta_{k+i-1}]^* \, : \, \epsilon \equiv 1 \mod \lambda_{k+i-1}^{p^{k+i}-p^k}\}$

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

If for example $i = 2$, 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 one gets 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 $a \equiv 1 \mod \lambda_k^{p^{k+2}-p^k}$

We now go back to the calculation of the Picard groups. What we would really like is to get an expression for the group V_n, defined in the introduction. As we described in the introduction Kervaire and Murthy have shown that $V_n = V_n^- \times V_n^+$, given an explicit formula for V_n^- and shown that when p is semi-regular there exists a canonical injection $\mathrm{Char}(V_n^+) \to \mathrm{Cl}^{(p)}\,\mathbb{Z}[\zeta_{n-1}]$. As mentioned in the introduction Kervaire and Murthy construct a canonical injection $\mathrm{Char}(\mathcal{V}_n^+) \to \mathrm{Cl}^{(p)}\,\mathbb{Z}[\zeta_{n-1}]$, where $\mathcal{V}_n$ is a group such that V_n is a canonical quotient of $\mathcal{V}_n$ (giving a canonical injection $\mathrm{Char}(V_n^+) \to \mathrm{Char}(\mathcal{V}_n^+)$).

In this section we will show that under a certain condition on the semi-regular prime p, the injection $\mathrm{Char}(\mathcal{V}_n^+) \to \mathrm{Cl}^{(p)}\,\mathbb{Z}[\zeta_{n-1}]$ is an isomorphism. This will follow as a corollary to theorem 3.5, which is the main theorem of this section.

In our setting the group $\mathcal{V}_n$ is defined as

$$\mathcal{V}_n := \frac{\tilde{D}^*_{0,n}}{\operatorname{Im}\{\tilde{\mathbb{Z}}[\zeta_{n-1}]^* \to \tilde{D}^*_{0,n}\}},$$

where $\tilde{\mathbb{Z}}[\zeta_{n-1}]^*$ are the group of all units ϵ such that $\epsilon \equiv 1 \bmod \lambda_{n-1}$.

We now need to define the condition on the prime mentioned in the introduction. For more information on this, see [W]. Let B_i be the i-th Bernoulli number and $B_{i,\chi}$ be the generalized i-th Bernoulli number associated to a character χ. Let ω be the Teichmüller character. If p is a semi-regular prime, let $i_1, \ldots, i_r$ be the even r indices such that $2 \leq i \leq p-3$ and $p|B_i$. If

$$B_{1,\omega^{i-1}} \not\equiv 0 \bmod p^2$$

and

$$\frac{B_i}{i} \not\equiv \frac{B_{i+p-1}}{i+p-1} \bmod p^2$$

for all $i \in \{i_1, \ldots, i_r\}$ then we will call p 2-regular. The number $r = r(p)$ is called the index of irregularity. In [W], p202, the following result is proved.

Theorem 3.4. *If p is a semi regular 2-regular prime and r the index of irregularity, then $\mathrm{Cl}^{(p)}\, \mathbb{Q}(\zeta_{n-1}) \cong (\mathbb{Z}/p^n\mathbb{Z})^r$.*

The main step in our approach to the Kervaire-Murthy conjectures is the following theorem.

Theorem 3.5. *Let p be an odd semi-regular prime and let $r = r(p)$ be the index of irregularity. Then $|\mathcal{V}_n^+| = p^{rn}$.*

It is worth noting that calculations have shown that every prime $p < 4000000$ is 2-regular.

For $n \geq 0$ and $k \geq 0$, define

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

Before the proof of the theorem we need some lemmas about these unit groups. We let U^p denote the group of p-th powers of elements in U.

Proposition 3.6. *Let p be an odd semi-regular, prime and let $r = r(p)$ be the index of irregularity of p. Then $\left|\frac{U^+_{n,p^{n+1}-1}}{(U^+_{n,p^n+1})^p}\right| = p^r$ for all $n \geq 0$.*

We let $(\mathbb{Z}[\zeta_n])_{\lambda_n}$ denote the λ_n-adic completion of $(\mathbb{Z}[\zeta_n])$.

Lemma 3.7. *Let ϵ be a unit in $(\mathbb{Z}[\zeta_n])_{\lambda_n}$ with $\epsilon \equiv 1 \mod \lambda_n^{p^{n+1}+1}$, then there exists a unit γ in $(\mathbb{Z}[\zeta_n])_{\lambda_n}$ such that $\epsilon = \gamma^p$. Moreover, $\gamma \equiv 1 \mod \lambda_n^{p^n+1}$.*

Proof. We will use the λ_n-adic exponential and logarithmic functions, defined by power series in the usual way. It is well known that $\log(1+x)$ converges if $v_{\lambda_n}(x) \geq 1$ and that $\exp(x)$ converges if $v_{\lambda_n}(x) \geq p^n+1$, where v_{λ_n} denotes the valuation with respect to λ_n. Let $\epsilon = 1+x$. Then $v_{\lambda_n}(x) \geq p^{n+1}+1$ and hence $v_{\lambda_n}(x^k) \geq k(p^{n+1}+1)$. If $1 \leq k \leq p-1$ we get

$$v_{\lambda_n}(x^k/k) \geq k(p^{n+1}+1).$$

Now suppose $k \geq p$. Let ln be the usual natural logarithm. Let $k = lp^r$ where $l \in \mathbb{Z}$ and $(l,p)=1$, then $p^r \leq k$ and

$$v_{\lambda_n}(k) = (p^{n+1}-p^n)r \leq (p^{n+1}-p^n)(\ln(k)/\ln(p)).$$

With this in mind,

$$\begin{aligned} v_{\lambda_n}(x^k/k) - (p^{n+1}+1) \geq (k-1)(p^{n+1}+1) - (p^{n+1}-p^n)(\ln(k)/\ln(p)) = \\ = (p^{n+1}-p^n)\frac{k-1}{\ln(p)}\Big(\frac{(p^{n+1}+1)\ln(p)}{p^{n+1}-p^n} - \frac{\ln(k)}{k-1}\Big) > \\ > (p^{n+1}-p^n)\frac{k-1}{\ln(p)}\Big(\frac{\ln(p)}{p-1} - \frac{\ln(k)}{k-1}\Big) \geq 0, \end{aligned}$$

where the last inequality follows from the fact that $\frac{\ln(t)}{t-1}$ is strictly decreasing for $t \geq 2$. The calculation above shows that $v_{\lambda_n}(\log(1+x)) \geq p^{n+1}+1$. Hence $v_{\lambda_n}(\frac{1}{p}\log(1+x)) \geq p^n+1$ and we can define $\gamma := \exp(\frac{1}{p}\log(1+x))$. Trivially, $\gamma^p = \epsilon$ and since $pv_{\lambda_n}(\gamma) = v_{\lambda_n}(\gamma^p) = v_{\lambda_n}(\epsilon) \geq 0$, $\gamma \in (\mathbb{Z}[\zeta_n])_{\lambda_n}$. In the same way $\gamma^{-1} \in (\mathbb{Z}[\zeta_n])_{\lambda_n}$ so γ is a unit. To show that $\gamma \equiv 1 \mod \lambda_n^{p^n+1}$ we need to examine the sum

$$\exp(y) = \sum_{k=0}^{\infty} \frac{y^k}{k!},$$

where $y = \frac{1}{p}\log(1+x) \equiv 0 \mod \lambda_n^{p^n+1}$. If i is a natural number, the number of p-factors in $i!$ is given by $\left[\frac{i}{p}\right] + \left[\frac{i}{p^2}\right] + \ldots$, where $\left[a\right]$ stands for the integer part of a. Hence $v_{\lambda_n}(i!) < (p^{n-1}-p^n)\frac{i}{p-1}$ and $v_{\lambda_n}(\frac{y^k}{k!}) > k$. This shows that

$$\exp(y) \equiv \sum_{k=0}^{p^n-1} \frac{y^k}{k!} \mod \lambda_n^{p^n+1}.$$

To examine this sum it is enough to consider the worst case which is when $k = p^{n-1}$. By counting p-factors as above, we see that

$$v_{\lambda_n}(p^{n-1}!) = (p^{n+1}-p^n)(p^{n-2}+p^{n-3}+\ldots+p+1) = p^{2n-1}-p^n.$$

This finishes the proof since now

$$v_{\lambda_n}(\frac{y^{p^{n-1}}}{p^{n-1}!}) \geq p^{n-1}(p^n+1) - (p^{2n-1}-p^n) = p^n + p^{n-1} \geq p^n+1.$$

□

Proof of proposition 3.6. First, by lemma 2 in [ST1], $U^+_{n,p^{n+1}-1} = U^+_{n,p^{n+1}}$ and since the λ_n-adic valuation of $\epsilon - 1$ where ϵ is real is even, $U^+_{n,p^{n+1}} = U^+_{n,p^{n+1}+1}$. We hence need to evaluate $|\frac{U^+_{n,p^{n+1}+1}}{(U^+_{n,p^n+1})^p}|$. 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, $G_n := \mathrm{Gal}(L_n/K_n) = \mathrm{Cl}^{(p)}(K_n)/p\,\mathrm{Cl}^{(p)}(K_n)$, where $\mathrm{Cl}^{(p)}(K_n)$ is the p-Sylow subgroup of the class group of K_n.

If $\epsilon \in U_{n,p^{n+1}+1}$, then it follows from lemma 3.7 that the extension $K_n \subseteq K_n(\sqrt[p]{\epsilon})$ is unramified and $K_n(\sqrt[p]{\epsilon}) \subseteq L_n$. Using Kummer's pairing we get a bilinear map $G_n \times U_{n,p^{n+1}+1} \to < \zeta_0 >$, $(\sigma, \epsilon) \mapsto \sigma(\epsilon)\epsilon^{-1}$. The kernel on the right is obviously the group of all p-th powers in $U_{n,p^{n+1}+1}$ which is $(U_{n,p^n+1})^p$. Suppose that the kernel on the left is trivial. Then, by a well known result, $\frac{U_{n,p^{n+1}+1}}{(U_{n,p^n+1})^p} \cong \mathrm{Char}(G_n)$ and hence $\frac{U^+_{n,p^{n+1}+1}}{(U^+_{n,p^n+1})^p} \cong \mathrm{Char}(G_n^-)$. But $(\mathrm{Cl}^{(p)}(K_n))^-$ is a p-group, and by results of Iwasawa, has r generators, so $|G_n^-| = p^r$ and this proves the theorem. So, we only need to prove that the kernel on the left is trivial (we can restrict ourselves to the $+$-part). 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 $s \le p-1$ 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 $\epsilon_1, \dots, \epsilon_r \in U^+_{n-1,p^n+1}$ such that every distinct extension E_i, $i = 1, 2, \dots r$ 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. □

Proof of theorem 3.5. We need to prove that $|\tilde{D}^{*+}_{0,n}|/|g_{0,n}(U_{n-1,1})| = p^{nr}$. We will prove this by induction on n. First, by Lemma 3.3, we have for any $n \geq 1$

$$g_{0,n}(U^+_{n-1,1}) \cong \frac{U^+_{n-1,1}}{U^+_{n-1,p^n-1}}.$$

Since $g_{0,n}(U^+_{n-1,1}) \subseteq g_{0,n}(\mathbb{Z}[\zeta_{n-1}]^{*+}) \subseteq \tilde{D}^{*+}_{0,n}$ the group $\frac{U^+_{n-1,1}}{U^+_{n-1,p^n-1}}$ is finite. Similarly $\frac{\mathbb{Z}[\zeta_{n-1}]^{*+}}{U^+_{p^{n-1}-1}}$ is finite. This shows that $|\frac{\mathbb{Z}[\zeta_{n-1}]^{*+}}{U^+_{n-1,1}}|$ is finite since

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

If $n = 1$, this and Dirichlet's theorem on units tells us that $U^+_{0,1}$ is isomorphic to $\mathbb{Z}^{\frac{p-3}{2}}$. By proposition 3.6

$$|\frac{U^+_{0,1}}{U^+_{0,p-1}}| = |\frac{U^+_{0,1}/(U^+_{0,1})^p}{U^+_{0,p-1}/(U^+_{0,1})^p}| = \frac{p^{\frac{p-3}{2}}}{p^r}.$$

This shows that

$$|D^{*+}_{0,n}|/|g_{0,1}(U^+_{n-1,1})| = p^r$$

so we have proved our statement for $n = 1$.

Now fix $n > 1$ and assume the statement of the theorem holds with n replaced by $n - 1$. We can write

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

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

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

Moreover, by proposition 3.6

$$|\frac{U^{+}_{n-1,p^{n}-1}}{(U^{+}_{n-1,p^{n-1}+1})^{p}}| = p^{r}$$

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 $<\epsilon> = U^{+}_{n-1,p^{n-1}-1}/U^{+}_{n-1,p^{n-1}+1}$. Since we know that 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

$$\begin{array}{ccc} & & \mathbb{Z}[\zeta_{n-1}]^{*} \\ & \swarrow^{N_{0,n-1}} & \downarrow f_{0,n-1} \\ A^{*}_{0,n-1} & \xrightarrow{g_{0,n-1}} & D^{*}_{0,n-1} \end{array}$$

It is clear that $f_{0,n-1}(U^{+}_{n-1,1}) \subseteq \tilde{D}^{*+}_{0,n-1}$ and that $g_{0,n-2}(U^{+}_{n-2,1}) \subseteq \tilde{D}^{*+}_{0,n-1}$. Recall that $A^{*}_{0,n-1} \cong \mathbb{Z}[\zeta_{n-2}]^{*} \oplus B$ and that the norm map $N_{0,n-1}$ acts like the usual norm map $N = \tilde{N}_{n-1,1} : \mathbb{Z}[\zeta_{n-1}]^{*} \to \mathbb{Z}[\zeta_{n-2}]^{*}$. It is well known that $N(\zeta_{n-1}) = \zeta_{n-2}$. By finding the constant term of the minimal polynomial $(x-1)^{p} - \zeta_{n-2}$ of λ_{n-1} we see that $N(\lambda_{n-1}) = \lambda_{n-2}$ and by a similar argument that $N(\zeta^{k}_{n-1} - 1) = \zeta^{k}_{n-2} - 1$ when $(k,p) = 1$. Since N is additive modulo p we get that $N_{0,n-1}(U^{+}_{n-1,1}) \subseteq U^{+}_{n-2,1}$. Hence we have a commutative diagram

$$\begin{array}{ccc} & & U^{+}_{n-1,1} \\ & \swarrow^{N} & \downarrow f \\ U^{+}_{n-2,1} & \xrightarrow{g} & \tilde{D}^{*+}_{0,n-1} \end{array}$$

We want to show that $f(U^{+}_{n-1,1}) = g(U^{+}_{n-2,1})$. Since $f(U^{+}_{n-1,1}) \subseteq g(U^{+}_{n-2,1})$ by commutativity of the diagram above, it is enough to show that N is surjective. In $\mathbb{Z}[\zeta_{j}]$, let $w_{j} := -\zeta_{j}^{\frac{p^{j+1}+1}{2}}$ and consider

$$\gamma_{j,l} := \frac{w_{j}^{l} - w_{j}^{-l}}{w_{j} - w_{j}^{-1}}.$$

If we fix $\zeta_j = e^{(2\pi\sqrt{-1}/p^{j+1})}$ we see that

$$\gamma_{j,l} := \frac{\sin(l\pi/p^{j+1})}{\sin(\pi/p^{j+1})}$$

and hence real. Moreover,

$$\gamma_{j,l} = w^{-l+1}\frac{\zeta_j^l - 1}{\zeta_j - 1}$$

so when $(l,p) = 1$ the $\gamma_{j,l}$ are units. Let J_j be the group of positive real units in $\mathbb{Z}[\zeta_j]$ and let $J_{0,j}$ be the subgroup generated by $\gamma_{j,l}$, $l \in \{2,3,\dots,(p^{j+1}-1)/2,\ (l,p)=1\}$. This is a well known construction and the details can be found in [W] p 144. Since $\gamma_{j,l}$ is real, it is congruent to a rational integer $a \mod (\lambda_j^2)$. Off course, $a \not\equiv 0 \mod (p)$. Hence $a^{p-1} \equiv 1 \mod (p)$ and this shows that $\gamma_{j,l}^{p-1} \equiv 1 \mod \lambda_j$. With $j = n-1$ this shows that $\gamma_{n-1,l}^{p-1} \in U_{n-1,1}^+$ and with $j = n-2$ that $\gamma_{n-2,l}^{p-1} \in U_{n-2,1}^+$. Now, a straightforward calculation shows that $N(\gamma_{n-1,l}^{p-1}) = \gamma_{n-2,l}^{p-1}$ so $J_{0,n-1}^{p-1} \subset N(U_{n-1,1}^+)$. Let $h^+ = h(\mathbb{Q}(\zeta_{n-2})^+)$ be the class number of $\mathbb{Q}(\zeta_{n-2})^+$. By corollary 10.6 on p. 187 of [W] $p|h(\mathbb{Q}(\zeta_{n-2})^+)$ implies $p|h(\mathbb{Q}(\zeta_0)^+)$ and since p is semi-regular we get that $(p,h^+) = 1$. By Theorem 8.2 on p. 145 of [W] we have

$$|\frac{J_{n-2}}{J_{0,n-2}}| = h^+.$$

Now take arbitrary $\epsilon \in U_{n-2,1}^+$. Then ϵ^2 is positive and hence an element of J_{n-2}. By the fact above there exists $s \in \mathbb{Z}$ such that $(s,p) = 1$ and $e^{2s} \in J_{0,n-2}$. This means that $e^{2s(p-1)} \in N(U_{n-1,1}^+)$. Since $(2s(p-1),p) = 1$ we can find $u, v \in \mathbb{Z}$ such that $2s(p-1)u + pv = 1$ so $\epsilon = \epsilon^{2s(p-1)u+pv} = (\epsilon^{2s(p-1)})^u(\epsilon^p)^v \in N(U_{n-1,1}^+)$. This shows that N is surjective.

We will now use our inductive hypothesis. This means that $|\tilde{D}_{0,n-1}^{*+}/g(U_{n-2,1}^+)| = p^{(n-1)r}$. It is easy to see that $\ker(f) = U_{n-1,p^{n-1}-1}^+$ so

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

and

$$|\frac{U_1^+}{U_{p^{n-1}-1}^+}| = |g(U_{n-2,1}^+)| = |\tilde{D}_{0,n-2}^{*+}|p^{-(n-1)r} = p^{\frac{p^{n-1}-3}{2}-(n-1)r}$$

by proposition 3.1 This finally gives

$$\begin{aligned} |\mathcal{V}_n^+| &= |\tilde{D}_{0,n}^{*+}||g(U_{n-1,1}^+)|^{-1} = \\ &= p^{\frac{p^n-3}{2}} \cdot p^{-\frac{p^{n-1}-3}{2}+(n-1)r} \cdot p^{-1} \cdot p^{-\frac{p^n-p^{n-1}}{2}+1} \cdot p^r = p^{nr} \end{aligned}$$

which is what we wanted to show. □

Recall that Kervaire and Murthy have proved that there exists a canonical injection $\mathrm{Char}(\mathcal{V}_n^+) \to \mathrm{Cl}^{(p)}\, \mathbb{Q}(\zeta_{n-1})$. By theorem 3.5 and theorem 3.4 the two groups have the same number of elements we get the following corollary

Corollary 3.8. *Let p be a semi regular 2-regular prime. Then* $\mathrm{Char}(\mathcal{V}_n^+) \cong \mathrm{Cl}^{(p)}\, \mathbb{Q}(\zeta_{n-1}) \cong (\mathbb{Z}/p^n\mathbb{Z})^r$.

Finally, it is not hard to show that V_n and $\mathcal{V}_n$ do not differ by too much. Recall from lemma 3.2 that $A_{0,n}^* \cong \mathbb{Z}[\zeta_{n-1}]^* \times B_{0,n}$. If $(1,\epsilon) \in B_{0,n}$, then $\epsilon \equiv 1 \bmod (p)$ and $\epsilon^p \equiv 1 \bmod (p^2)$ in $A_{0,n-2}^*$. This also means that $(\epsilon^p - 1)/p \equiv 0 \bmod (p)$ in $A_{0,n-2}^*$ which is enough for $(1,e)^p \equiv (1,1) \bmod (p)$ in $A_{0,n-1}^*$ to hold. By abuse of notation,

$$V_n^+ \cong \frac{\mathcal{V}_n^+}{\mathrm{Im}\{B_n \to \tilde{D}_{0,n}^*\}^+}$$

so the discussion above together with the preceding corollary yields the corollary below.

Corollary 3.9. $V_n \cong \bigoplus_{i=1}^r \mathbb{Z}/p^{n-\delta_i}\mathbb{Z}$, *where* $\delta_i \in \{0,1\}$ *for all* i

References

[G] Galovich, Steven, *The Class Group of a Cyclic p-group.* Journal of Algebra 30 (1974) 368-387.

[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.

[Rim] Rim, D.S., *Modules over Finite Groups* Annals of Mathemathica 69 (1959), 700-712.

[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, 28-66.

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

[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`