ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 32, Number 4, Winter 2002

ON KERVAIRE AND MURTHY'S CONJECTURE

OLA HELENIUS AND ALEXANDER STOLIN

ABSTRACT. Let p be a semi-regular prime, let C_{p^n} be a cyclic group of order p^n and let ζ_n be a primitive p^{n+1}th root of unity. There is a short exact sequence

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

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

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

1. Introduction. 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. For $k \geq 0$ and $i \geq 1$, let $A_{k,i} := \mathbf{Z}[x]/((x^{p^{k+i}}-1)/(x^{p^k}-1))$ and $D_{k,i} := A_{k,i} \bmod p$. Note that $A_{n,1} \cong \mathbf{Z}[\zeta_n]$. By a generalization of Rim's theorem (see for example [**1**]), $\operatorname{Pic} \mathbf{Z}C_{p^n} \cong \operatorname{Pic} A_{0,n}$ for all $n \geq 1$. It is well known that there exists a pull-back diagram (Cartesian square)

$$\begin{array}{ccc} A_{0,n+1} & \longrightarrow & \mathbf{Z}[\zeta_n] \\ \downarrow & & \downarrow \\ A_{0,n} & \longrightarrow & D_{0,n} := \dfrac{A_{0,n}}{pA_{0,n}} \end{array}$$

and an associated Mayer-Vietoris exact sequence

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

1991 AMS *Mathematics Subject Classification.* 11R65, 11R21, 19A31.
Key words and phrases. Picard groups, integral group rings.
Received by the editors on August 7, 2001, and in revised form on

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

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

we get an exact sequence

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

It is easy to see that $D_{0,n}\cong \mathbf{F}_p[x]/(x-1)^{p^n-1}$. 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 $V_n^-:=\{v\in V_n : c(v)=v^{-1}\}$.

In [**2**], Kervaire and Murthy prove that $V_n=V_n^+\times V_n^-$ and that $V_n^-\cong D_{0,n}^*/(\langle\bar{x}\rangle D_{0,n}^{*+})$. They also calculate the exact structure of V_n^- to be

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

These results can be proved using fairly elementary techniques. However, Kervaire and Murthy also prove that, when p is semi-regular, there is a canonical injection

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

where $\operatorname{Cl}^{(p)}\mathbf{Q}(\zeta_{n-1})$ is the p-component of the ideal class group of $\mathbf{Q}(\zeta_{n-1})$. In [**2**] this is proved using Iwasawa theory. In fact Kervaire and Murthy use a slightly different approach than the one we indicated above since they start with the pull-back diagram

$$\begin{array}{ccc}\mathbf{Z}C_{p^{n+1}} & \longrightarrow & \mathbf{Z}[\zeta_n]\\ \big\downarrow & & \big\downarrow\\ \mathbf{Z}C_{p^n} & \longrightarrow & \dfrac{\mathbf{F}_p[x]}{(x^{p^n}-1)}.\end{array}$$

Their equivalent to V_n is

$$V_n' := \frac{\left(\frac{\mathbf{F}_p[x]}{(x^{p^n}-1)}\right)^*}{\operatorname{Im}\left\{\mathbf{Z}[\zeta_n]^* \times (\mathbf{Z}C_{p^n})^* \to \left(\frac{\mathbf{F}_p[x]}{(x^{p^n}-1)}\right)^*\right\}}$$

but it is easy to show that $V_n \cong V_n'$ so we will denote both groups V_n. What Kervaire and Murthy really prove is that the statement holds with V_n' replaced by the group

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

This is enough since V_n' is a canonical quotient of $\mathcal{V}_n'$. Hence we have a canonical surjection $\mathcal{V}_n' \to V_n'$ and the dual map $\operatorname{Char} V_n' \to \operatorname{Char} \mathcal{V}_n'$ is a canonical injection.

In this paper we will show that, with an extra condition on the semi-regular prime p, $\operatorname{Char} \mathcal{V}_n \cong \operatorname{Cl}^{(p)}\mathbf{Q}(\zeta_{n-1})$. Our definition of $\mathcal{V}_n$ differs from the one in [**2**] since we start out with a different pull-back diagram. Proposition 3.4 shows that the two definitions produce isomorphic groups.

Remark . In [**3**] Ullom proves that, under a certain extra condition on the semi-regular prime p, $V_n^+ \cong (\mathbf{Z}/p^n\mathbf{Z})^r \oplus (\mathbf{Z}/p^{n-1}\mathbf{Z})^{\lambda-r}$ where λ is one of the Iwasawa invariants of p.

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.

Before we start we need to make some observations. First, for each $k \geq 0$ and $i \geq 1$, we have a pull-back diagram

$$\begin{tikzcd} A_{k,k+1} \arrow[r, "i_{k,i+1}"] \arrow[d, "j_{k,i+1}"'] & \mathbf{Z}[\zeta_{k+i}] \arrow[d, "f_{k,i}"] \\ A_{k,i} \arrow[r, "g_{k,i}"'] & D_{k,i} \end{tikzcd}$$

An element $a \in A_{k,i+1}$ can be uniquely represented as a pair $(a_i, b_i) \in \mathbf{Z}[\zeta_{k+i}] \times A_{k,i}$. 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 $a_m \in \mathbf{Z}[\zeta_{k+m}]$. In the rest of this paper we will identify an element of $A_{k,i+1}$ with both of its representations as a pair or an $(i+1)$-tuple.

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

We want to prove the following result.

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

$$\begin{tikzcd} & \mathbf{Z}[\zeta_{k+i}] \arrow[dl, "N_{k,i}"'] \arrow[d, "f_{k,i}"] \\ A_{k,i} \arrow[r, "g_{k,i}"'] & D_{k,i} \end{tikzcd}$$

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

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

The maps $N_{k,i}$ will be constructed inductively. If $i = 1$ and k is arbitrary, we have $A_{k,1} \cong \mathbf{Z}[\zeta_k]$ 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 $x_{k,i} \mapsto x_{k+1,i}^p$.*

(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 [**4**] and proofs can be found there.

Now suppose $N_{k,j}$ is constructed for all k and all $j \leq i-1$. Let $\varphi = \varphi_{k+1,i} : \mathbf{Z}[\zeta_{k+i}] \to A_{k+1,i}$ 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, $N_{k,i}(\zeta_{k+i}) = N(\zeta_{k+i}, x_{k+,i-1}) = N(x_{k+1,i}) = x_{k,i}$, 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 the following is observed

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

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*

$$\begin{tikzcd}
\mathbf{Z}[\zeta_{k+i}] \arrow[r, "N"] \arrow[d, "N_{k,i}"'] & \mathbf{Z}[\zeta_{k+i-1}] \arrow[d, "N_{k-1,i}"] \\
A_{k,i} \arrow[r, "N"'] & A_{k-1,i}
\end{tikzcd}$$

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

$$\begin{aligned}
N(N_{k,i}(a)) &= N\big(N((a, N_{k+1,i-1}(a))\big) \\
&= \big(N(N(a)), N(N(N_{k+1,i-1}(a)))\big)
\end{aligned}$$

and

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

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 $\operatorname{Pic}\mathbf{Z}C_{p^n}$ **for** 2**-regular primes.** We start 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 $c(\bar{x}) = \bar{x}^{-1}$ where $\bar{x}$ denotes the class of x in $D^*_{k,i} \cong \mathbf{F}_p[x]/(x-1)^{p^{k+i}-p^k}$. Clearly $\mathbf{F}^*_p \subset D^*_{k,i}$ and, by the structure theorem for abelian groups, $D^*_{k,i} = \mathbf{F}^*_p \oplus \tilde{D}^*_{k,i}$ 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 a finite abelian group of odd order and since c has order 2, we get

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

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 represented as $\{1+a_1(x-x^{-1})+\cdots+a_{p^{n-1}-2}(x-x^{-1})^{p^{n-1}-2}\}$. 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 $\{1+a_1(x-x^{-1})+a_3(x-x^{-1})^3+\cdots+a_{p^{n-1}-2}(x-x^{-1})^{p^{n-1}-2}\}$. Hence $|\tilde{D}^{*-}_{0,n-1}| = p^{(p^{n-1}-1)/2}$ and, since $|\tilde{D}^*_{0,n-1}| = p^{p^{n-1}-2}$, we get $|\tilde{D}^{*+}_{0,n-1}| = p^{(p^{n-1}-3)/2}$. $\square$

We will now use our norm maps from Section 2 to get an inclusion of $\mathbf{Z}[\zeta_{k+i-1}]^*$ into $A^*_{k,i}$. Define $\varphi_{k,i} : \mathbf{Z}[\zeta_{k+i-1}]^* \to A^*_{k,i}$ be the injective group homomorphism defined by $\varepsilon \mapsto (\varepsilon, N_{k,i}(\varepsilon))$. 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 $A^*_{k,i} \cong \mathbf{Z}[\zeta_{k+i-1}]^* \times B_{k,i}$.*

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

We now need a technical lemma which is Theorem I.2.7 in [**5**]. Let λ_n be the ideal $(\zeta_n - 1)$ in $\mathbf{Z}[\zeta_n]$.

Lemma 3.3. *$ker(g_{k,i_{|\mathbf{Z}[\zeta_{k+i-1}]^*}}) = \{\varepsilon \in \mathbf{Z}[\zeta_{k+i-1}]^* : \varepsilon \equiv 1 \bmod \lambda_{k+i-1}^{p^{k+i}-p^k}\}$.*

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

If for example $i = 2$, we get after just one step $a \equiv 1 \bmod p$ in $\mathbf{Z}[\zeta_{k+1}]$, $N(a) \equiv 1 \bmod p$ and $N((a-1)/p) \equiv (N(a)-1)/p \bmod p$ in $A_{k,1} \cong \mathbf{Z}[\zeta_k]$ 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 $\mathbf{Z}[\zeta_{k=1}]$ is divisible by p, one gets that $N(a) \equiv 1 \bmod p^2$ and hence that $N((a-1)/p) \equiv 0 \bmod p$. By analyzing how the norm acts, one can show that this means that $a \equiv 1 \bmod \lambda_k^{p^{k+2}-p^k}$.

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 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 $\operatorname{Char} V_n^+ \to \mathrm{Cl}^{(p)}\mathbf{Z}[\zeta_{n-1}]$. As also mentioned in the introduction, Kervaire and Murthy construct a canonical injection

$\operatorname{Char}\mathcal{V}_n^+ \to \mathrm{Cl}^{(p)}\mathbf{Z}[\zeta_{n-1}]$, where $\mathcal{V}_n$ is a group such that V_n is a canonical quotient of $\mathcal{V}_n$ (giving a canonical injection $\operatorname{Char} V_n^+ \to \operatorname{Char}\mathcal{V}_n^+$.

In this section we will show that, under a certain condition on the semi-regular prime p, the injection $\operatorname{Char}\mathcal{V}_n^+ \to \mathrm{Cl}^{(p)}\mathbf{Z}[\zeta_{n-1}]$ is an isomorphism. This will follow as a corollary to Theorems 3.5 and 3.6, which is the main theorem of this section. We define the group $\mathcal{V}_n$ as

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

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

Proposition 3.4. *Let p be a semi-regular prime. Then $\mathcal{V}_n^+ = \mathcal{V}_n'^+$.*

Proof. Lemma 3.9, in a slightly different notation, reads that the Norm $\tilde{N}_{n,1} : \tilde{\mathbf{Z}}[\zeta_n]^{*+} \to \tilde{\mathbf{Z}}[\zeta_{n-1}]^{*+}$ (the "+" superscript denotes the real units) is surjective, so

$$\frac{\tilde{D}^{*+}}{\operatorname{Im}\{\tilde{\mathbf{Z}}[\zeta_{n-1}]^{*+} \to \tilde{D}^{*+}_{0,n}\}} = \frac{\tilde{D}^{*+}_{0,n}}{\operatorname{Im}\{\tilde{\mathbf{Z}}[\zeta_n]^{*+} \to \tilde{D}^{*+}_{0,n}\}}.$$

Let

$$\alpha : \left(\frac{\mathbf{F}_p[x]}{(x-1)^{p^n}}\right)^{*+} \to \left(\frac{\mathbf{F}_p[x]}{(x-1)^{p^n-1}}\right)^{*+} = D^{*+}_{0,n}.$$

Obviously, $\ker\alpha$ is generated by units congruent to 1 mod $(\bar{x}-1)^{p^n-1}$. Consider the unit

$$\varepsilon := \frac{\eta^{p^{n-1}+1} - \eta^{-(p^{n-1}+1)}}{\eta - \eta^{-1}},$$

where $\eta := \zeta_{n-1}^{(p^n+1)/2}$. One can by a direct calculation show that $\varepsilon \equiv 1 \bmod \lambda_{n-1}^{p^{n-1}-1}$ but $\varepsilon \not\equiv 1 \bmod \lambda_{n-1}^{p^{n-1}}$. Hence $\ker\alpha \subset \operatorname{Im}\{\tilde{\mathbf{Z}}[\zeta_{n-1}]^{*+} \to \tilde{D}^{*+}_{0,n}\}$ and α induces an isomorphism $\mathcal{V}_n'^+ \to \mathcal{V}_n^+$. □

We now need to define the condition on the prime mentioned in the introduction. For more information on this, see [**6**]. Let B_i be the

ith Bernoulli number and $B_{i,\chi}$ the generalized ith Bernoulli number associated to a character χ. Let ω be the Teichmüller character. If p is a semi-regular prime, let $i_1, \dots, i_r$ be the even r indices such that $2 \le i \le p-3$ and p divides the numerator of B_i (in reduced form). 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 $i \in \{i_1, \dots, i_r\}$, then we will call p 2-regular. The number $r = r(p)$ is called the index of irregularity. In [**6**, p. 202], the following result is proved.

Theorem 3.5. *If p is a semi-regular 2-regular prime and r the index of irregularity, then $Cl^{(p)}\mathbf{Q}(\zeta_{n-1}) \cong (\mathbf{Z}/p^n\mathbf{Z})^r$.*

The following theorem can be considered the main result of this paper.

Theorem 3.6. *Let p be an odd semi-regular, 2-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 $n \ge 0$ and $k \ge 0$, define

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

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

Proposition 3.7. *Let p be an odd semi-regular, 2-regular prime, and let $r = r(p)$ be the index of irregularity of p. Then*

$$\left|\frac{U^+_{n,p^{n+1}-1}}{(U^+_{n,p^n+1})^p}\right| = p^r \quad \textit{for all } n \ge 0.$$

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

Lemma 3.8. *Let ε be a unit in $(\mathbf{Z}[\zeta_n])_{\lambda_n}$ with $\varepsilon \equiv 1 \bmod \lambda_n^{p^{n+1}+1}$; then there exists a unit γ in $(\mathbf{Z}[\zeta_n])_{\lambda_n}$ such that $\varepsilon = \gamma^p$. Moreover, $\gamma \equiv 1 \bmod \lambda_n^{p^n+1}$.*

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 $\varepsilon = 1+x$. 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

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

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

$$v_{\lambda_n}(k) = (p^{n+1} - p^n)r \geq (p^{n+1} - p^n)\left(\frac{\ln(k)}{\ln(p)}\right).$$

With this in mind,

$$\begin{aligned} v_{\lambda_n}\left(\frac{x^k}{k}\right) - (p^{n_1}+1) &\geq (k-1)(p^{n+1}+1) - (p^{n+1} - p^n)\left(\frac{\ln(k)}{\ln(p)}\right) \\ &= (p^{n+1} - p^n)\frac{k-1}{\ln(p)}\left(\frac{(p^{n+1}+1)\ln(p)}{p^{n+1}-p^n} - \frac{\ln(k)}{k-1}\right) \\ &> (p^{n+1} - p^n)\frac{k-1}{\ln(p)}\left(\frac{\ln(p)}{p-1} - \frac{\ln(k)}{k-1}\right) \geq 0, \end{aligned}$$

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

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

where $y = (1/p)\log(1+x) \equiv 0 \bmod \lambda_n^{p^n+1}$. If i is a natural number, the number of p-factors in $i!$ is given by $[i/p] + [i/p^2] + \cdots$, where $[a]$ stands for the integer part of a. Hence

$$v_{\lambda_n}(i!) < (p^{n-1} - p^n)\Big(\frac{i}{(p-1)}\Big) \quad \text{and} \quad v_{\lambda_n}\Big(\frac{y^k}{k!}\Big) > k.$$

This shows that

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

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

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

This finishes the proof since now

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

Proof of Proposition 3.7. First, by Lemma 2 in [**1**], $U^+_{n,p^{n+1}-1} = U^+_{n,p^{n+1}}$ and since the λ_n-adic valuation of $\varepsilon - 1$ where ε is real is even, $U^+_{n,p^{n+1}} = U^+_{n,p^{n+1}+1}$. We hence need to evaluate $|U^+_{n,p^{n+1}+1}/(U^+_{n,p^n+1})^p|$. Denote the field $\mathbf{Q}(\zeta_n)$ by K_n and let L_n be the maximal elementary unramified extension of K_n. It is well known that $G_n := \mathrm{Gal}\,(L_n/K_n) = \mathrm{Cl}^{(p)}(K_n)/p\mathrm{Cl}^{(p)}(K_n)$, where $\mathrm{Cl}^{(p)}(K_n)$ is the p-Sylow subgroup of the class group of K_n. If $\varepsilon \in U_{n,p^{n+1}+1}$, then it follows from Lemma 3.8 that the extension $K_n \subseteq K_n(\sqrt[p]{\varepsilon})$ is unramified and $K_n(\sqrt[p]{\varepsilon}) \subset L_n$. Using Kummer's pairing we get a bilinear map $G_n \times U_{n,p^{n+1}+1} \to \langle\zeta_0\rangle$, $(\sigma,\varepsilon) \mapsto \sigma(\varepsilon)\varepsilon^{-1}$. The kernel on the right is obviously the group of all pth 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, $U_{n,p^{n+1}+1}/(U_{n,p^n+1})^p \cong \mathrm{Char}\,(G_n)$ and hence $U^+_{n,p^{n+1}+1}/(U^+_{n,p^n+1})^p \cong \mathrm{Char}\,(G_n^-)$. But, by 3.5, $|G_n^-| = p^r$ 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 $\langle\sigma,\varepsilon\rangle = 1$ 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 pth root of some $\varepsilon \in U_{n,p^{n+1}+1}$, we are done. Again, $|G_n^-| = p^r$, so there are r distinct (elementary) extensions. We now use induction. Let $n = 0$ and suppose $K_0 \subset L$ is an unramified extension of degree p. Since the extension is of degree p, we have $L = K_0(a)$ where $a^p = d$, $d \in K_0$. Since the extension is unramified, we must have $(d) = I^p$ for some ideal $I \subset \mathbf{Z}[\zeta_0]$ and $d \equiv 1 \bmod \lambda_0^{p-1}$. By, for example, Lemma 2 [**1**] and since d can be taken real, we get $d \equiv 1 \bmod \lambda_0^{p+1}$. By Theorem 3.8 [**5**], we get $I = (b)$ for some $b \in \mathbf{Z}[\zeta_0]$ so $d = \varepsilon b^p$ for some unit ε. As before, $\varepsilon \equiv 1 \bmod \lambda_0^{p+1}$ and γ can be chosen as any pth root of ε. Now suppose all unramified extension of K_{n-1} are given by units. Then we have r units $\varepsilon_1, \dots, \varepsilon_r \in U^+_{n-1,p^n+1}$ such that every distinct extension E_i, $i = 1, 2, \dots r$ is generated by a pth root of ε_i. Consider ε_i as elements of K_n. A straightforward calculation shows that $\varepsilon_i \in U^+_{n,p^{n+1}+1}$. Hence a pth root of ε_i either generates an unramified extension of K_n of degree p or $\sqrt[p]{\varepsilon_i} \in K_n$. The latter case cannot 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 extensions of K_n, and this concludes the proof. □

Note. The condition 2-regularity is a bit more than we need. If we examine the proof we see that we only use that the p-rank of $\mathrm{Cl}^{(p)}\mathbf{Q}(\zeta_n)$ is r, the index of regularity. 2-regularity provides us, via Theorem 3.5, with the stronger fact $\mathrm{Cl}^{(p)}\mathbf{Q}(\zeta_{n-1}) \cong (\mathbf{Z}/p^n\mathbf{Z})^r$.

Before the proof of Theorem 3.6 we will state a lemma, which is well known.

Lemma 3.9. *If p is semi-regular $N_{n-1} : \mathbf{Z}[\zeta_{n-1}] \to A_{n-1}$ maps $U^+_{n-1,1}$ surjectively onto $U^+_{n-2,1}$.*

Basically, this follows from the fact that when p is semi-regular, the positive real units of $\mathbf{Z}[\zeta_{n-2}]$ modulo the cyclotomic units, has order prime to p, say s. A straightforward calculation shows that $N_{n-1}(U^+_{n-1,1})$ contains the $p-1$st powers of the cyclotomic units of

$\mathbf{Z}[\zeta_{n-2}]$. This means that an element $\varepsilon \in U^+_{n-2,1}$ to the power $2s(p-1)$ is contained in $N_{n-1}(U^+_{n-1,1})$. Since $2s(p-1)$ and p are co-prime, there exist u and v such that $\varepsilon = \varepsilon^{2s(p-1)u+pv} = (\varepsilon^{2s(p-1)})^u(\varepsilon^p)^v \in N_{n-1}(U^+_{n-1,1})$.

Proof of Theorem 3.6. 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 $g_{0,n}(U^+_{n-1,1}) \subseteq g_{0,n}(\mathbf{Z}[\zeta_{n-1}]^{*+}) \subseteq \tilde{D}^{*+}_{0,n}$ the group $U^+_{n-1,1}/U^+_{n-1,p^n-1}$ is finite. Similarly, $\mathbf{Z}[\zeta_{n-1}]^{*+}/U^+_{p^{n-1}-1}$ is finite. This shows that $|\mathbf{Z}[\zeta_{n-1}]^{*+}/U^+_{n-1,1}|$ is finite since

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

If $n=1$, this and Dirichlet's theorem on units tell us that $U^+_{0,1}$ is isomorphic to $\mathbf{Z}^{(p-3)/2}$. By Proposition 3.7,

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

This shows that

$$\frac{|D^{*+}_{0,1}|}{|g_{0,1}(U^+_{0,1})|} = p^r$$

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 have

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

By Dirichlet's theorem on units we have $(\mathbf{Z}[\zeta_{n-1}]^*) \cong \mathbf{Z}^{((p^n-p^{n-1})/2)-1}$. 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 $\mathbf{Z}^{((p^n-p^{n-1})/2)-1}$. The rest of the proof is devoted to the analysis of the four righthand factors of 3.1.

Obviously,

$$\frac{U^+_{n-1,p^{n-1}+1}}{(U^+_{n-1,p^{n-1}+1})^p} \cong \frac{\mathbf{Z}^{\frac{p^n-p^{n-1}}{2}-1}}{(p\mathbf{Z})^{\frac{p^n-p^{n-1}}{2}-1}} \cong C_p^{\frac{p^n-p^{n-1}}{2}-1}.$$

This shows that

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

Moreover, by Proposition 3.7,

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

We now turn to the second factor of the righthand side of 3.1. We will show that this number is p by finding a unit $\varepsilon \notin U^+_{p^{n-1}+1}$ such that

$$\langle\varepsilon\rangle = \frac{U^+_{n-1,p^{n-1}-1}}{U^+_{n-1,p^{n-1}+1}}.$$

Since we know that the pth 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 $\eta := \zeta^{(p^n+1)/2}$. Then $\eta^2 = \zeta$ and $c(\eta) = \eta^{-1}$. Let $\varepsilon := (\eta^{p^{n-1}+1} - \eta^{-(p^{n-1}+1)})/(\eta - \eta^{-1})$. Then $c(\varepsilon) = \varepsilon$ and one can show by direct calculations that ε is the unit we are looking for.

We now want to calculate

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

Consider the commutative diagram

$$\begin{tikzcd}
 & \mathbf{Z}[\zeta_{n-1}]^* \arrow[dl, "N_{0,n-1}"'] \arrow[d, "f_{0,n-1}"] \\
A^*_{0,n-1} \arrow[r, "g_{0,n-1}"'] & D^*_{0,n-1}
\end{tikzcd}$$

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 $A^*_{0,n-1} \cong \mathbf{Z}[\zeta_{n-2}]^* \oplus B_{0,n-1}$ and that the norm map $N_{0,n-1}$ acts like the usual norm map $N = \tilde{N}_{n-1,1} : \mathbf{Z}[\zeta_{n-1}]^* \to \mathbf{Z}[\zeta_{n-2}]^*$. 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

$$\begin{tikzcd}
 & U^+_{n-1,1} \arrow[dl, "N"'] \arrow[d, "f"] \\
U^+_{n-2,1} \arrow[r, "g"'] & \tilde{D}^{*+}_{0,n-1}
\end{tikzcd}$$

By Lemma 3.9, 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

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

and

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

by Proposition 3.1. This finally gives

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

which is what we wanted to show. □

Recall that Kervaire and Murthy have proved that there exists a canonical injection $\operatorname{Char}\mathcal{V}^+_n \to \mathrm{Cl}^{(p)}\mathbf{Q}(\zeta_{n-1})$. By Theorem 3.6 and Theorem 3.5, the two groups have the same number of elements, so we get the following corollary

Corollary 3.10. *Let p be a semi-regular 2-regular prime. Then* $\operatorname{Char}\mathcal{V}^+_n \cong \mathrm{Cl}^{(p)}\mathbf{Q}(\zeta_{n-1}) \cong (\mathbf{Z}/p^n\mathbf{Z})^r$.

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 $A^*_{0,n} \cong \mathbf{Z}[\zeta_{n-1}]^* \times B_{0,n}$. If $(1,\varepsilon) \in B_{0,n}$, then $\varepsilon \equiv 1 \bmod (p)$ and $\varepsilon^p \equiv 1 \bmod (p^2)$ in $A^*_{0,n-2}$. This also means that $(\varepsilon^p - 1)/p \equiv 0 \bmod (p)$ 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,

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

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

Corollary 3.11.

$$V_n \cong \bigoplus_{i=1}^{r} \frac{\mathbf{Z}}{p^{n-\delta_i}\mathbf{Z}}, \quad \textit{where } \delta_i \in \{0,1\} \quad \textit{for all } i.$$

REFERENCES

1. Alexander Stolin, *An explicit formula for the Picard group of the cyclic group of order* p^2, Proc. Amer. Math. Soc. **121** (1994), 375–383.

2. M.A. Kervaire and M.P. Murthy, *On the projective class group of cyclic groups of prime power order*, Comment. Math. Helv. **52** (1977), 415–452.

3. S. Ullom, *Class groups of cyclotomic fields and group rings*, London Math. Soc. (2) **17** (1978), 231–239.

4. Alexander Stolin, *On the Picard group of the integer group ring of the cyclic* p*-group and rings close to it*, in *Commutative ring theory*, Lecture Notes in Pure Appl. Math. **185**, Dekker, New York, 1997, 443–455.

5. ———, *On the Picard group of the integer group ring of the cyclic* p*-group and certain Galois groups*, J. Number Theory **72** (1998), 48–66.

6. Lawrence C. Washington, *Introduction to cyclotomic fields*, Springer-Verlag, New York, 1997.

Department of Mathematics, Chalmers University of Technology and Göteborg University, SE-41296, Göteborg, Sweden
E-mail address: olahe@math.chalmers.se

Department of Mathematics, Chalmers University of Technology and Göteborg University, SE-41296, Göteborg, Sweden
E-mail address: astolin@math.chalmers.se