# PICARD GROUPS OF INTEGER GROUP RINGS AND UNITS IN CYCLOTOMIC FIELDS

OLA HELENIUS AND ALEXANDER STOLIN

ABSTRACT. In 1977 Kervaire and Murthy presented 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 $V_n^+$. In a previous paper we gave the explicit structure of $\mathcal{V}_n^+$ under some different extra assumption on the semi-regular prime $p$. Here we extend this result to all semi-regular primes. We also present results on the structure of the real units in $\mathbb{Z}[\zeta_n]$, prove that the number of generators of $\mathcal{V}_n^+$ coincides with the number of generators of $\mathrm{Cl}^{(p)}\,\mathbb{Q}(\zeta_{n-1})$ and prove that the extra assumption about an explicit form of the elements generating all unramified extensions of $\mathbb{Q}(\zeta_n)$ of degree $p$ (which we used in the previous paper) is valid for all semi-regular primes.

## 1. INTRODUCTION

This paper is an extension of a previous paper, [H-S], from the authors. We refer you there for some history and more explicit notation.

Let $p$ be an odd semi-regular prime, let $C_{p^n}$ be the cyclic group of order $p^n$ and let $\zeta_n$ be a primitive $p^{n+1}$-th root of unity. Kervaire and Murthy prove in [K-M] that there is an exact sequence

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

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 $\mathrm{Char}(V_n^+)$ injects canonically in the $p$-component of the ideal class group of $\mathbb{Q}(\zeta_{n-1})$. The latter statement is proved with $V_n^+$ replaced by a group $\mathcal{V}_n^+$, where $V_n^+$ is a canonical quotient of $\mathcal{V}_n^+$ (which is obviously enough).

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

Under an extra assumption on the prime $p$ (concerning the Iwasawa-invariants of $p$), Ullom proved in 1978 in [U] that $V_n^+ \cong (\mathbb{Z}/p^n\mathbb{Z})^{r(p)} \oplus (\mathbb{Z}/p^{n-1}\mathbb{Z})^{\lambda - r(p)}$, where $\lambda$ is one of the Iwasawa invariants. In [H-S] we, among other things, proved that under a certain condition on the $p$-rank of the class groups $\mathrm{Cl}^{(p)}\,\mathbb{Q}(\zeta_n)$ (a weaker condition than the one Ullom uses) we have

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

The numbers $r_k$ are defined as the $\log_p$ of orders of certain groups of units in $\mathbb{Z}[\zeta_k]$ and our assumption is exactly that $r_k = \mathrm{rank}_p \, \mathrm{Cl}^{(p)}\,\mathbb{Q}(\zeta_k)$.

In this paper we will show that $\mathcal{V}_n^+$ is given by the formula above for all semi-regular primes. Throughout this paper we assume that $p$ is semi-regular.

## 2. $\mathcal{V}_n^+$ FOR SEMI-REGULAR PRIMES

We start by defining the numbers $r_n$ by

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

Here $U_{n,k}$ is the group of all real units in $\mathbb{Z}[\zeta_n]^*$ that are congruent to 1 modulo $\lambda_n^k$ where $\lambda_n = (\zeta_n - 1)$.

Our main theorem is, as mentioned, the following.

**Theorem 2.1.** *For every semi-regular prime $p$*

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

Before we can prove this we need to recall some notation from [H-S]. 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 [S1]) $\operatorname{Pic}\mathbb{Z}C_{p^n} \cong \operatorname{Pic}A_{0,n}$ for all $n \geq 1$ and this is why these rings are relevant for us. It is easy to see that there exists a pull-back diagram

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

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 $N_{k,l}$ are defined in [H-S], Proposition 2.1, and by Lemma 2.5 in the same paper we have an injection $\mathbb{Z}[\zeta_{k+l-1}]^* \to A^*_{k,l}$. In what follows, we identify $\mathbb{Z}[\zeta_{k+l-1}]^*$ with its image in $A^*_{k,l}$.

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

By abuse of notation we let for each group (or ring) $c$ denote the homomorphism defined by sending a generator $x$ to $x^{-1}$ (this is complex conjugation in $\mathbb{Z}[\zeta_n]$). We denote by $G^+$ the group of elements of $G$ invariant under $c$.

In our setting, $\mathcal{V}_n^+$ is defined by

$$\mathcal{V}_n^+ := \frac{\tilde{D}_n^{*+}}{g_n(U_{n-1,1})}, \tag{2.2}$$

where $\tilde{D}_n^{*+}$ is the group of all units in $D_n^{*+}$ congruent to 1 modulo $(x-1)$.

Note that this definition is not the same as the one used in [K-M]. They instead look at

$$\mathcal{V}'_n := \frac{(\mathbb{F}_p[x]/(x^{p^n}-1))^*}{\operatorname{Im}\{\mathbb{Z}[\zeta_n]^* \to (\mathbb{F}_p[x]/(x^{p^n}-1))^*\}} \tag{2.3}$$

The confusion regarding the two definitions of $\mathcal{V}_n$ is cleared up by the following.

**Proposition 2.2.** *The definitions of $\mathcal{V}_n$ and $\mathcal{V}'_n$ (2.3 and 2.2) coincide.*

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

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

is commutative and $N$ (which is the restriction of the usual norm-map) is surjective when $p$ is semi-regular (a well known fact) the proposition follows. □

We now introduce some techniques from [K-M].

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

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

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

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

Considered as a map $\alpha'_n : \mathcal{V}'_{n-1} \to \mathcal{V}'_n$ this map acts as $(\mathbb{F}_p[x]/(x-1)^{p^{n-1}})^* \ni x_{n-1} \mapsto x_n^p \in (\mathbb{F}_p[x]/(x-1)^{p^n})^*$. Since $\mathcal{V}'_n \cong \mathcal{V}_n$ (see Proposition 2.2) we can consider this as a homomorphism $\alpha_n : \mathcal{V}_{n-1} \to \mathcal{V}_n$. Clearly we then get that $\alpha$ is induced by $x_{n-1} \to x_n^p$ Note however, that $x_{n-1} \mapsto x_n^p$ does not induce a homomorphism $D_{n-1}^* \to D_n^*$.

**Lemma 2.3.** *The map $\alpha_n$ is injective on $\mathcal{V}_{n-1}^+$.*

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

$$\Phi_{K_n} : I_0(K_n) \to Gal(M_n/K_n),$$

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

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

1) $Gal^+(M_n/K_n) \cong Gal^+(M_n/L_n) \cong \mathcal{V}_n^+$
2) $M_{n-1} \cap K_n = K_{n-1}$ (lemma 4.4).

Obviously the field extension $K_n/K_{n-1}$ induces a natural homomorphism

$$Gal(M_{n-1}/K_{n-1}) \cong (I_0(K_{n-1})/H_{n-1})^{(p)} \to (I_0(K_n)/H_n)^{(p)} \cong Gal(M_n/K_n)$$

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

To see this note that $F^{-1}(\Phi'_{K_n}(s)) = \Phi_{K_{n-1}}(N_{K_n/K_{n-1}}(s))$ for any $s \in I_0(K_n)$. If $s \in H_n$ then without loss of generality $s = 1 + \lambda_n^{p^n} t$, $t \in \mathbb{Z}[\zeta_n]$, and thus, $N_{K_n/K_{n-1}}(s)) = 1 + pt_1$ for some $t_1 \in \mathbb{Z}[\zeta_{n-1}]$. Now it is clear that $\Phi'_{K_n}(s) = 0$ since $\Phi_{K_{n-1}}(1 + pt_1) = 0$ (0 is the identical automorphism).

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

$$\begin{array}{ccc} & & Gal(M_{n-1}/K_{n-1}) \\ & \swarrow^{\alpha_n} & \downarrow F \\ Gal(M_n/K_n) & \longrightarrow & Gal(M_{n-1}K_n/K_n) \end{array}$$

If $\alpha_n(a) = 0$ then $F(a) = 0$ and $a = 0$ because $F$ is an isomorphism which proves the lemma. □

**Proof of Theorem 2.1.** 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 $n-1$. Lemma 3.10 in [H-S] tells us that we have a surjection $\pi_n : \mathcal{V}_n^+ \to \mathcal{V}_{n-1}^+$ and Proposition 3.11 in [H-S] that $\ker \pi_n$ isomorphic to $C_p^{r_{n-1}}$. Suppose $1+(x_{n-1}-1)^k$ is non-trivial in $\mathcal{V}_{n-1}^+$. Since

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

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

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

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

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

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

As an application of Theorem 2.1 we can get some results on the unit basis in $D_m$ previously obtained in [H-S] under an extra assumption. Let

$$U_{n,k} := \{\gamma \in \mathbb{Z}[\zeta_n]^* : \gamma = 1 \bmod (\lambda_n^k)\}$$

Define $\varphi_N : U_{n,p^{n+1}-p^{n-N}} \to D_{n-N}^+$ by

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

In [H-S], p. 24, it is proved that $\varphi_N$ is a homomorphism. The following corollary now follows immediately in the same way as Proposition 5.8 of [H-S]

**Corollary 2.4.** *Suppose $p$ is semi-regular. Let $N$ be as in Proposition 3.7 in* [H-S] *and let $n \geq N+1$. Then there exists a basis for $D_{n-N}^+$ consisting of elements $\varphi_N(\gamma)$ where $\gamma \in U_{n,p^{n+1}-p^{n-N}}$.*

Furthermore, since $D_{k,i} = A_{k,i}/(p)$, we can get a $p$-adic version of this result. Let

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

be the $p$-adic completion of $A_{k,i}$ and let $A_{k,i}^+$ be "the real elements" of $A_{k,i}$. Let $U_{n,k,(p)} := \{\text{real } \epsilon \in \mathbb{Z}_p[\zeta_n]^* : \epsilon \equiv 1 \bmod \lambda_n^k\}$ and let us define $\varphi'_N : U_{n,p^{n+1}-p^{n-N},(p)} \to (A_{0,n-N,(p)})^+$ by

$$\varphi'_N(\epsilon) = N_{0,n-N}(\frac{1}{p}\tilde{N}_{n,N}(\frac{\epsilon-1}{\lambda_n^{p^{n+1}-p^{n-N+1}}})).$$

where the norm-maps are the obvious $p$-adic extensions of our usual norm-maps.

**Corollary 2.5.** *Suppose $p$ is semi-regular. There exists a basis for $(A_{0,n-N,(p)})^+$ consisting of elements $\varphi'_N(\gamma)$ where $\gamma$ are global units, $\gamma \in U_{n,p^{n+1}-p^{n-N}}$.*

An interesting remark on Theorem 2.1 is that this result might be thought of as an indication on that Assumption 2 in [H-S] is true. We will prove this later in this paper and therefore we will find a number of generators of the $p$-part of $\mathrm{Cl}^{(p)}\mathbb{Q}(\zeta_n)$.

Another interesting remark is that for every semi-regular prime $\mathcal{V}_n^+$ is (isomorphic to) a subgroup of $\mathrm{Cl}^{(p)}\,\mathbb{Q}(\zeta_{n-1})$ (under the injection from [K-M]), a subgroup which we now by Theorem 2.1 now explicitly. Kervaire and Murphy also conjectures that $\mathcal{V}_n^+$ is actually isomorphic to $\mathrm{Cl}^{(p)}\,\mathbb{Q}(\zeta_{n-1})$. If this is true Theorem 2.1 of course would provide an explicit description of this class group.

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

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

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

Let $s_{n,p^{n+1}-1} = |U_{n,1}/U_{n-1,p^{n+1}-1}|$. A naive first guess would be that $s_{n,p^{n+1}-1} = \frac{p^{n+1}-1-2}{2} = \frac{p^{n+1}-3}{2}$ which is the maximal value of this number. Incidentally, this maximal value equals $|\tilde{D}_{n+1}^{*+}|$. In this case we say that $U_{n,1}/U_{n,p^{n+1}-1}$ is full, but this happens if and only if $p$ is a regular prime. In other words $\mathcal{V}_{n+1}^+$ is trivial if and only if $p$ is a regular. This fact is by the way proved directly in [H]. For non-regular (but as before semi-regular) primes, what happens is that there are "missed places" in $U_{n,1}/U_{n,p^{n+1}-1}$. We define $2k$ as a missed place (at level $n$) if $U_{n,2k}/U_{n,2k+2}$ is trivial. Lemma 3.2 in [H-S] reads $U_{n,p^{n+1}-1} = U_{n,p^{n+1}+1}$ and hence provides an instant example of a missed place, namely $p^{n+1}-1$. It follows from our theory that every missed place corresponds to a non-trivial element of $\mathcal{V}_{n+1}^+$. By Lemma 5.2 of [H-S] we have that for all $1 \leq 2s \leq p^{n+1}-1$, $\epsilon$ is in $U_{n,2s}$ if and only if an only if $g_{n+1}(\epsilon) \in D_{n+1}^{*+}(2s)$, where $D_{n+1}^*(k) = \{a : a = 1 \bmod (x_{n+1}-1)^k\}$. Theorem 2.1 and its proof hence give us specific information about the missed places which we will formulate in a Theorem below. We start with a simple lemma.

**Lemma 3.1.** *Let $1 \leq s \leq n+1$ and $1 \leq k < s$. Then $p^s - p^k$ is a missed place at level $n$ if and only if $s = n+1$ and $k = 1$.*

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

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

Clearly, $\epsilon$ is real and since

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

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

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

**Theorem 3.2.** *At level $n$ we have the following*

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

**Proof.** We know (from for example Proposition 4.6 of [H-S]) that we have $r_0$ missed places in the 0-strip at level 0 and that they correspond exactly to the indexes of the relevant Bernoulli numbers. An easy induction argument using the map $\pi_n$ to lift the generators of $\mathcal{V}_{n-1}^+$ to $\mathcal{V}_n^+$ show that we have $r_0$ missed places in the 0-strip at every level. This proves *2*. To prove *1* we now only need prove that the "new" missed places we get when we go from level $n-1$ to $n$ all end up in the $n$-strip. First, $p^n - 1$ can not be a missed place (at level $n$) by the lemma above. It follows from our theory that the "new" missed places correspond to the generators of $\mathcal{V}_{n+1}^+$ of exponent $p$. We need to show that each such generators $a_l$, $l = 1, \ldots, r_{n-1} - r_{n-2}$, belong to $D_{n+1}^{*+}(p^n + 1)$. Suppose for a contradiction that $a_l = 1 + t(x_{n+1} - 1)^s$, $s \leq p^n - 1$, is a "new" generator. Then $\pi_{n+1}(a_l)$ is neccesarily trivial in $\mathcal{V}_n^+$. Hence $1 + t(x_n - 1)^s = g_n(\epsilon)$ for some $\epsilon \in \mathbb{Z}[\zeta_{n-1}]^*$. But since the usual norm map $\tilde{N}_{n,1}$ is surjective (when $p$ is semi-regular) and by commutativity of diagram 4.1 of [H-S] we then get $a_l g_{n+1}(\epsilon')^{-1} = b$ for some $\epsilon' \in \mathbb{Z}[\zeta_n]^*$ and $b \in \ker\{\tilde{D}_n^{*+} \to \tilde{D}_{n-1}^{*+}\} = \tilde{D}_n^{*+}(p^n - 1)$. Since $p^n - 1$ is not a missed place $b = g_{n+1}(\epsilon'')$ for some some $\epsilon' \in \mathbb{Z}[\zeta_n]^*$. But this means $a_l$ is trivial in $\mathcal{V}_{n+1}^+$ which is a contradiction. We conclude that $a_l \in D_{n+1}^{*+}(p^n + 1)$.

To prove *3* we use the map $\alpha_n$ to see that a missed place $k$ at level $n-1$ lifts to a missed place $pk$ at level $n$. To prove the rest of *3* it is enough to prove that no "new" missed places are divisible by $p$ (since the rest follows inductively). As we did above it is enough to prove that if $a_l \in D_{n+1}^{*+}(s) \setminus D_{n+1}^{*+}(s+2)$ is a "new" generator of $\mathcal{V}_{n+1}^+$, then $p$ does not divide $s$. Now, a generator can always be chosen of the form $1 + (x_{n+1} - 1)^s$. Then an element of the form $1 + (x_{n+1} - 1)^{pk}$, with $k \notin \{i_1, \dots, i_{r_{n-1}}\}$ cannot be a missed place. This follows from the fact that if $k$ is not a missed place, then $1 + (x_n - 1)^k$ is trivial in $\mathcal{V}_n^+$ and since $\alpha_n$ is injective, $1 + (x_{n+1} - 1)^{pk} = \alpha_n(1 + (x_n - 1)^k)$ is also trivial in $\mathcal{V}_{n+1}^+$. □

## 4. Class groups and the Kervaire-Murthy conjectures

In this section we will prove that $\mathrm{Cl}\,\mathbb{Q}(\zeta_{n-1})(p) \cong \mathcal{V}_n^+/(\mathcal{V}_n^+)^p$. Here $A(p) := \{x \in A : x^p = 1\}$. It follows from Theorem 2.1 that $\mathcal{V}_n^+/(\mathcal{V}_n^+)^p$ has $r_{n-1}$ generators, and it was proved in [K-M] that $Char(\mathcal{V}_n^+)$ can be embedded into $\mathrm{Cl}^{(p)}\,\mathbb{Q}(\zeta_{n-1})$.

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

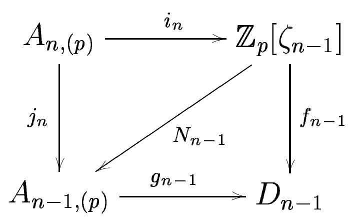
**Theorem 4.1.** *There exists an embedding* $\mathrm{Cl}\,\mathbb{Q}(\zeta_{n-1})(p) \to Char(V_n^+)$.

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

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

We have a commutative diagram

(4.1)




Considering pairs $(a, N_{n-1}(a))$, where $a \in \mathbb{Z}_p[\zeta_{n-1}]$, we can embed $\mathbb{Z}_p[\zeta_{n-1}]^*$ into $A^*_{n,(p)}$. In [S2] it was proved that $D_n^*$ is isomorphic to $\mathbb{Z}_p[\zeta_{n-1}]^*/U_{n-1,p^n-1,(p)}$. We hence have the following proposition

**Proposition 4.2.**

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

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

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

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

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

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

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

The action is independent of the choice of $q$ by the following reason: another generator of $\alpha^p$, which is 1 modulo $\lambda_{n-1}^2$, differs from "the old" $q$ by some unit $\gamma = 1 + \lambda_{n-1}^2 t_1$, and it can be easily verified that $\gamma$ is either real or $\gamma = \zeta_{n-1}^{pk}\gamma_1$ with a real unit $\gamma_1$. Hence we must consider $\tau_{\gamma q}(v)$ for real $\gamma$. In other words we have to prove that $(v,\gamma)_{\lambda_{n-1}} = 1$. But if the latter is untrue, then $(v,\gamma)_{\lambda_{n-1}} = \zeta_0$, which is not consistent with the action of the "complex conjugation" ($v$ and $\gamma$ are real, while $\zeta_0$ is not real).

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

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

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

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

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

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

The theorem is proved.

□

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

**Corollary 4.3.** $\mathrm{Cl}\,\mathbb{Q}(\zeta_{n-1})(p) \cong \mathcal{V}_n^+/(\mathcal{V}_n^+)^p \cong (\mathbb{Z}/p\mathbb{Z})^{r_{n-1}}$ *(see Section 2 for the definition of* $r_{n-1}$*).*

**Proof.** It remains to prove the second isomorphism only, which follows from Theorem 2.1. □

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

**Corollary 4.4.** *Any unramified extension of* $\mathbb{Q}(\zeta_{n-1}) = K_{n-1}$ *of degree* $p$ *is of the form* $K_{n-1}(\epsilon^{1/p})/K_{n-1}$*, where* $\epsilon$ *is a unit satisfying* $\epsilon = 1 + \lambda_{n-1}^{p^n+1}t$*.*

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

**Corollary 4.5.** *Let a unit* $\epsilon \in \mathbb{Z}[\zeta_{n-1}]^*$ *satisfy* $\epsilon \equiv r^p \mod \lambda_{n-1}^{p^n-1}$*. Then* $\epsilon = \gamma^p\gamma_1$ *with units* $\gamma, gamma_1$ *and* $\gamma_1 \equiv 1 \mod \lambda_{n-1}^{p^n+1}$*.*

## References

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

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

[H-S] O. Helenius and A. Stolin, *Unit Bases in Integer Group Rings and the Kervaire-Murthy Conjectures* Preprint, Chalmers University of Technology, 2001.

[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.

[S1] 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.

[S2] Stolin, Alexander. *On the Picard Group of the Integer Group Ring of the Cyclic $p$-Group and Rings Close to It.*
Commutative ring theory (Fs, 1995), Lecture Notes in Pure and Appl. Math., 185, Dekker, New York, 1997, pp. 443-455.

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

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