ON THE PICARD GROUP OF SOME POLYNOMIAL RINGS

OLA HELENIUS

ABSTRACT. Let ζ_n be a primitive p^{n+1}th root of unity and let C_{p^n} be the cyclic group of order p^n. There exists an exact sequence

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

V_n^- is explicitly known and when p is semi-regular and satisfies some mild extra assumptions, so is V_n^+. In this paper we study rings $A_{k,l} := \mathbb{Z}[x]/(p_{k,l}(x))$, where $p_{k,l}(x) = (x^{p^{k+l}} - 1)/(x^{p^k} - 1)$ which in some sense fits in between $\mathbb{Z}C_{p^{n+1}}$ and $\mathbb{Z}[\zeta_n]$. For each such ring $A_{k,l}$ we exhibit an exact sequence

$$0 \to V_{k,l}^+ \oplus V_{k,l}^- \to \operatorname{Pic} A_{k,l} \to \operatorname{Cl} \mathbb{Q}(\zeta_{k+l-1}) \oplus \operatorname{Pic} A_{k,l-1} \to 0$$

and calculate $V_{k,l}^+$ and $V_{k,l}^-$ explicitly when p is semi-regular and satisfies one extra assumption.

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. Kervaire and Murthy prove in the article [K-M] 1977, that there exists an exact sequence

$$0 \to V_n^+ \oplus V_n^- \to \operatorname{Pic} \mathbb{Z}C_{p^{n+1}} \to \operatorname{Cl} \mathbb{Q}(\zeta_n) \oplus \operatorname{Pic} \mathbb{Z}C_{p^n} \to 0, \tag{1.1}$$

where

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

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

In [U2], Ullom proved under an extra assumption on the prime p, that

$$V_n^+ \cong (\frac{\mathbb{Z}}{p^n\mathbb{Z}})^{r(p)} \oplus (\frac{\mathbb{Z}}{p^{n-1}\mathbb{Z}})^{\lambda - r(p)}, \tag{1.2}$$

1991 *Mathematics Subject Classification.* 11R65, 11R21, 19A31.

Key words and phrases. Picard Groups, Integral Group Rings.

where λ is one of the Iwasawa-invariants of p and $r(p)$ is the index of regularity of p, that is the number of Bernoulli numbers B_i, $i = 1, 2, \ldots, p-3$ with nominators (in reduced form) divisible by p.

In the articles [H-S] and [H-S2] we use that fact that $\operatorname{Pic} \mathbb{Z}C_{p^n} \cong \operatorname{Pic} \frac{\mathbb{Z}[x]}{((x^{p^n}-1)/(x-1))}$ and concentrate our efforts on $\frac{\mathbb{Z}[x]}{((x^{p^n}-1)/(x-1))}$. Among other things we re-prove Ulloms result using a different technique and also find the exact structure of $\mathcal{V}_n^+$ for all semi-regular primes. An important part of our technique is that we use not only the ring $\frac{\mathbb{Z}[x]}{((x^{p^n}-1)/(x-1))}$ but also $\frac{\mathbb{Z}[x]}{((x^{p^{k+l}}-1)/(x^k-1))}$ for different l and k. It is hence a natural question for us to consider $\operatorname{Pic} \frac{\mathbb{Z}[x]}{((x^{p^{k+l}}-1)/(x^{p^k}-1))}$ and to try to find a sequence corresponding to 1.1 and groups $V_{k,l}$. In this paper we will complete this task for semi-regular primes satisfying one extra assumption, namely that for all n, the p-part of the ideal class group of $\mathbb{Q}(\zeta_n)$ has p-rank equal to $r(p)$. It is known this assumption holds for all primes $p < 4.000.000$.

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

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

It is easy to see that there exists a pull-back diagram

(1.3)
$$\begin{tikzcd}
A_{k,l+1} \arrow[r, "i_{k,l+1}"] \arrow[d, "j_{k,l+1}"'] & \mathbb{Z}[\zeta_{k+l}] \arrow[d, "f_{k,l}"] \arrow[dl, "N_{k,l}"] \\
A_{k,l} \arrow[r, "g_{k,l}"] & D_{k,l}
\end{tikzcd}$$

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 multiplicative "norm" maps $N_{k,l}$, which make lower right triangle of the diagrams commute, are defined in [H-S], Proposition 2.1. By Lemma 2.5 in the same paper we have an injection $\varphi_{k,l} : \mathbb{Z}[\zeta_{k+l-1}]^* \to A_{k,l}^*$. By using the pull-back above with l replaced by $l-1$ we see that every element of $A_{k,l}$ can be represented as a pair $(a, b) \in \mathbb{Z}[\zeta_{k+l-1}] \times A_{k,l-1}$. The injection $\varphi_{k,l}$ is defined by $\varphi_{k,l}(\epsilon) = (\epsilon, N_{k,l-1}(\epsilon)$. In what follows, we identify $\mathbb{Z}[\zeta_{k+l-1}]^*$ with its image in $A^*_{k,l}$. The pull-back 1.3 induces a Maier-Vietoris exact sequence

$$\mathbb{Z}[\zeta_{k+l}]^* \times A^*_{k,l} \to D^*_{k,l} \to \operatorname{Pic} A_{k,l+1} \to \operatorname{Pic}\mathbb{Z}[\zeta_{k+l}] \times \operatorname{Pic} A_{k,l} \to \operatorname{Pic} D_{k,l},$$

Since $D_{k,l}$ is local, $\operatorname{Pic} D_{k,l} = 0$ and since $\mathbb{Z}[\zeta_{k+l}]$ is a Dedekind ring, $\operatorname{Pic}\mathbb{Z}[\zeta_{k+l}] \cong \operatorname{Cl}\mathbb{Z}[\zeta_{k+l}]$. By letting $V_{k,l}$ be the cokernel

$$V_{k,l} := \frac{D^*_{k,l}}{\operatorname{Im}\{\mathbb{Z}[\zeta_{k+l}]^* \times A^*_{k,l} \to D^*_{k,l}\}}$$

we get an exact sequence

$$0 \to V_{k,l} \to \operatorname{Pic} A_{k,l+1} \to \operatorname{Cl}\mathbb{Z}[\zeta_{k+l}] \times \operatorname{Pic} A_{k,l} \to 0. \tag{1.4}$$

To find $V_{k,l}$ we start by splitting this group in "positive" and "negative" parts. For this we use the map c. By abuse of notation we let c act on all our rings $\mathbb{Z}[n]$, $A_{k,l}$ and $D_{k,l}$. On $\mathbb{Z}[\zeta_n]$, c is just complex conjugation. On the other rings c is the homomorphism induced by $x \mapsto x^{-1}$ (for $x = x_{k,l} \in A_{k,l}$ and $\bar{x}_{k,l} \in D_{k,l}$). If B is a ring (or group) upon which c act, we define $B^+ = \{b \in B : c(b) = b\}$ and $B^- = \{b \in B : c(b) = b^{-1}\}$. It is easy to see that c commute with all maps in diagram 1.3, hence extends to $V_{k,l}$, so we can define $V^+_{k,l}$ and $V^-_{k,l}$ in the obvious ways.

It turns out that the calculation of $V^-_{k,l}$ is easy and reasonably straightforward. Once we have found the structure of the group $D^{*-}_{k,l}$ the result follows from a generalization of Kummer's famous result that a unit in $\mathbb{Z}[\zeta_0]^*$ can be written as a real unit times a power of ζ_0.

When it comes to $V^+_{k,l}$ we run into more trouble. We first consider a group $\mathcal{V}^+_{k,l}$ such that $V^+_{k,l}$ is a canonical quotient of $\mathcal{V}^+_{k,l}$ (see section 3 for a definition). We then show that $\mathcal{V}^+_{k,l} \cong \mathcal{V}^+_{0,k+l}$. Here we use a result from [H-S] that tells us that a unit in $D^{*+}_{k,l}$ congruent to 1 modulo a sufficiently high power of $(\bar{x}-1)$ is actually the image of an element from $A^{*+}_{k,l}$. After this, of course, we need only use the structure of $\mathcal{V}^+_{0,k+l}$, which we also calculated in [H-S], to get our hands on $\mathcal{V}^+_{k,l}$.

Finally we prove that $V^+_{k,l} = \mathcal{V}^+_{k,l}$ by a direct construction.

2. Structure of $D_{k,l}$ and $V^-_{k,l}$

We start off with some preliminary results.

Proposition 2.1.

$$V_{k,l} = \frac{D^*_{k,l}}{\operatorname{Im}\{A^*_{k,l} \to D^*_{k,l}\}}$$

Proof. $f_{k,l} = N_{k,l} \circ g_{k,l}$. □

We now zoom in on the structure of $D^*_{k,l}$. Clearly any element of $D_{k,l}$ can be represented by $a_0 + a_1(x-1) + \ldots + a_{p^{k+l}-p^k-1}(x-1)^{p^{k+l}-p^k-1}$, $a_i \in \mathbb{F}_p$, $(x-1)^{p^{k+l}-p^k} = 0$, so $|D_{k,l}| = p^{p^{k+l}-p^k}$. Every element with $a_0 = 0$ is nilpotent and hence not a unit. Since, clearly, $a_0 \neq 0$ is a unit we see that every element with $a_0 \neq 0$ is a unit, so $|D^*_{k,l}| = (p-1)p^{p^{k+l}-p^k-1}$. $\mathbb{F}_p^* \subset D^*_{k,l}$, so $D^*_{k,l} \cong \mathbb{F}_p^* \times \tilde{D}^*_{k,l}$, where $\tilde{D}^*_{k,l}$ is a p-group of order $p^{p^{k+l}-p^k-1}$. Since the map c has order 2 we also get $\tilde{D}^*_{k,l} = \tilde{D}^{*-}_{k,l} \times \tilde{D}^{*+}_{k,l}$ (for convenience we use the notation $\tilde{D}^{*+}_{k,l}$ instead of the maybe more correct $(\tilde{D}^*_{k,l})^+$).

It is easy to see that we can also use $(x - x^{-1})^i$, $i = 0, 1, \ldots, p^{k+l} - p^k - 1$, as a basis for $D^*_{k,l}$ over $\mathbb{F}_p$. Using this basis we see that

$$\tilde{D}^{*-}_{k,l} = \{1 + a_1(x-x^{-1}) + a_3(x-x^{-1})^3 + \ldots + a_{p^{k+l}-p^k-1}(x-x^{-1})^{p^{k+l}-p^k-1}\}$$

and

$$\tilde{D}^{*+}_{k,l} = \{1 + a_2(x-x^{-1})^2 + a_4(x-x^{-1})^4 + \ldots + a_{p^{k+l}-p^k-2}(x-x^{-1})^{p^{k+l}-p^k-2}\}$$

so $|D^{*-}_{k,l}| = p^{(p^{k+l}-p^k)/2}$ and $|D^{*+}_{k,l}| = p^{(p^{k+l}-p^k)/2-1}$. For later use we need to find the exact structure of $\tilde{D}^{*-}_{k,l}$. By the structure theorem for Abelian groups,

$$\tilde{D}^{*-}_{k,l} \cong \prod_{i=1}^{k+l} C_{p^i}^{s_i} \tag{2.1}$$

for some s_i. Observe that if

$$u = 1 + a_1(x-x^{-1}) + a_3(x-x^{-1})^3 + \ldots + a_{p^{k+l}-p^k-1}(x-x^{-1})^{p^{k+l}-p^k-1},$$

then

$$u^p = 1 + a_1(x-x^{-1})^p + a_3(x-x^{-1})^{3p} + \ldots + a_{p^{k+l-1}-p^{k-1}-1}(x-x^{-1})^{p^{k+l}-p^k-p}.$$

Hence if $u^p = 1$ we must have $a_1 = a_3 = \ldots = a_{p^{k+l-1}-p^{k-1}-1} = 0$ so the subset of elements in $\tilde{D}^{*-}_{k,l}$ of order p has order $p^{((p^{k+l}-p^k-1)-(p^{k+l-1}-p^{k-1}-1))/2} = p^{(p^{k+l}-p^k-p^{k+l-1}+p^{k-1})/2}$. Similarly, if we let o_i denote the number of elements of order p^i or less we get

$$\begin{aligned}
\log_p o_1 &= (\frac{p^{k+l}-p^k}{2}) - (\frac{p^{k+l-1}-p^{[k-1]}}{2}) \\
\log_p o_2 &= (\frac{p^{k+l}-p^k}{2}) - (\frac{p^{k+l-2}-p^{[k-2]}}{2}) \\
&\vdots \\
\log_p o_{k+l-1} &= (\frac{p^{k+l}-p^k}{2}) - (\frac{p-1}{2}) \\
\log_p o_{k+l} &= \frac{p^{k+l}-p^k}{2}
\end{aligned}$$

where $[m] = (m + |m|)/2$ for an integer m. By comparing this with 2.1 we can find the exponents s_i by.

$$\begin{aligned}
s_1 &= 2\log_p o_1 - \log_p o_2 \\
s_2 &= 2\log_p o_2 - \log_p o_1 - \log_p o_3 \\
s_3 &= 2\log_p o_3 - \log_p o_2 - \log_p o_4 \\
&\vdots \\
s_{k+l-1} &= 2\log_p o_{k+l-1} - \log_p o_{k+l-2} - \log_p o_{k+l} \\
s_{k+l} &= \log_p o_{k+l} - \log_p o_{k+l-1}
\end{aligned}$$

which gives us

$$\begin{aligned}
s_1 &= \frac{p^{k+l}-p^k}{2} - 2\frac{p^{k+l-1}-p^{[k-1]}}{2} + \frac{p^{k+l-2}-p^{[k-2]}}{2} \\
s_2 &= \frac{p^{k+l-1}-p^{[k-1]}}{2} - 2\frac{p^{k+l-2}-p^{[k-2]}}{2} + \frac{p^{k+l-3}-p^{[k-3]}}{2} \\
&\vdots \\
s_{k+l-2} &= \frac{p^3-p^{[-l+3]}}{2} - 2\frac{p^2-p^{[-l+2]}}{2} + \frac{p-1}{2} \\
s_{k+l-1} &= \frac{p^2-p^{[-l+2]}}{2} - 2\frac{p-1}{2} \\
s_{k+l} &= \frac{p-1}{2}
\end{aligned}$$

We summarize this and some other facts proved above in a proposition.

Proposition 2.2. $|D_{k,l}| = p^{p^{k+l}-p^k}$, $|D^+_{k,l}| = p^{(p^{k+l}-p^k)/2}$, $|\tilde{D}^*_{k,l}| = p^{p^{k+l}-p^k-1}$. $|D^{*-}_{k,l}| = p^{(p^{k+l}-p^k)/2}$ *and* $|D^{*+}_{k,l}| = p^{(p^{k+l}-p^k)/2-1}$. *Moreover,*

$$\tilde{D}^{*-}_{k,l} \cong \prod_{i=1}^{k+l} C^{s_i}_{p^i},$$

where

$$s_i = \frac{p^{k+l-i+1} - p^{[k-i+1]}}{2} - 2\frac{p^{[k+l-i]} - p^{[k-i]}}{2} + \frac{p^{[k+l-i-1]} - p^{[k-i-1]}}{2}$$

for $i = 1, 2, \ldots, k+l$.

The following lemma, sometimes called Kummer's Lemma, is well known. A proof can be found in for example [W], p 3.

Lemma 2.3. *For every unit* $\epsilon \in \mathbb{Z}[\zeta_n]^*$ *there exists a natural number* k *and a unit* $\epsilon_r \in \mathbb{Z}[\zeta_n]^{*+}$ *such that* $\epsilon = \epsilon_r \zeta_n^k$.

We now generalize this to the rings $A_{k,l}$.

Proposition 2.4. *For every unit* $e \in A^*_{k,l}$ *there exists a natural number* k *and a unit* $e_r \in A^{*+}_{k,l}$ *such that* $e = e_r x^k_{k,l}$.

Proof. Induction with respect to l. If l equals 1, this in the lemma above. Fix $l \geq 1$ and suppose the statement holds in $A^*_{k,l-1}$ (for all k). Consider the diagram 1.3 and let $e_{k,l+1} \in A^*_{k,l+1}$ be represented by $(\epsilon', e') \in \mathbb{Z}[\zeta_{k+l}]^* \times A^*_{k,l}$. By the assumption there exists $\epsilon'_r \in \mathbb{Z}[\zeta_{k+l}]^{*+}$ and $e'_r \in A^{*+}_{k,l}$ and integers k_1, k_2 such that $\epsilon' = \epsilon'_r \zeta^{k_1}_{k+l}$ and $e' = e'_r x^{k_2}_{k,l}$. Since the maps c commute with the pull-back diagram, $c((\epsilon'_r, e'_r)) = (\epsilon'_r, e'_r)$ and $(\epsilon', e') = (\epsilon'_r, e'_r)(\zeta^{k_1}_{k+l}, x^{k_2}_{k,l})$. $(\epsilon', e') \in A_{k,l+1}$ is equivalent to $f_{k,l}(\epsilon') = g_{k,l}(e')$ and also $c(f_{k,l}(\epsilon')) = c(g_{k,l}(e'))$. We hence get

$$\bar{x}^{k_1}_{k,l} f_{k,l}(\epsilon'_r) = \bar{x}^{k_2}_{k,l} g_{k,l}(e'_r)$$

and

$$\bar{x}^{-k_1}_{k,l} f_{k,l}(\epsilon'_r) = \bar{x}^{-k_2}_{k,l} g_{k,l}(e'_r)$$

which implies $\bar{x}^{2k_1}_{k,l} = \bar{x}^{2k_2}_{k,l}$ in $D_{k,l}$. Since $\bar{x}_{k,l} \in D^{*-}_{k,l}$, which is a p-group, this implies $\bar{x}^{k_1-k_2}_{k,l} = 1$. Now recall that $D^{*-}_{k,l}$ do have elements of order p^{k+l} by Proposition 2.2 and hence it is not hard to realize that $\bar{x}_{k,l}$ then must have order p^{k+l}. This means $k_2 \equiv k_1 \bmod p^{k+l}$ which in turn means that $\bar{x}^{k_2}_{k,l} = \bar{x}^{k_1}_{k,l}$. Now it follows that $e_r := (\epsilon'_r, e'_r) \in A^{*+}_{k,l+1}$ and since $x^{k_1}_{k,l+1} = (\zeta^{k_1}_{k+l}, x^{k_1}_{k,l})$ we get $e_{k,l+1} = e_r x^{k_1}_{k,l+1}$. □

We also have the following lemma.

Lemma 2.5. $\mathbb{F}_p^* \subset \mathrm{Im}\{A_{k,l}^* \to D_{k,l}^*\}$

Proof. Fix arbitrary $t \in \mathbb{F}_p^*$. By Fermat's little theorem, $t \equiv t^{p^{k+l}} \bmod p$. Consider $\frac{x^t-1}{x-1} \in A_{k,l}$. Choose $r, s \in \mathbb{Z}$ such that $tr - sp^{k+l} = 1$. Then

$$\begin{aligned}
\frac{x^t-1}{x-1}\frac{x^{1+sp^{k+l}}-1}{x^t-1} - 1 &= \frac{x^{1+sp^{k+l}}-1}{x-1} - 1 = \\
&= \frac{x^{1+sp^{k+l}}-x}{x-1} = x\frac{x^{sp^{k+l}}-1}{x-1} = \\
&= x(x^{s(p^{k+l}-1)} + \ldots + x + 1)\frac{x^{p^{k+l}}-1}{x-1} = \\
&= x(x^{s(p^{k+l}-1)} + \ldots + x + 1)\frac{x^{p^k}-1}{x-1} \cdot \frac{x^{p^{k+l}}-1}{x^{p^k}-1} = 0
\end{aligned}$$

in $A_{k,l}$. Since

$$\begin{aligned}
\frac{x^{1+sp^{k+l}}-1}{x^t-1} &= \frac{x^{tr}-1}{x^t-1} = \\
&= x^{t(r-1)} + \ldots + x^t + 1 \in A_{k,l}
\end{aligned}$$

this shows $\frac{x^t-1}{x-1} \in A_{k,l}^*$. Now,

$$\frac{x^t-1}{x-1} - t = x^{t-1} + \ldots + x + 1 - k = (x-1)f(x)$$

for some polynomial $f \in \mathbb{Z}[x]$. Hence, in $D_{k,l}$ we get

$$\begin{aligned}
g_{k,l}((\frac{x^t-1}{x-1})^{p^{k+l}}) - t &= g_{k,l}(\frac{x^t-1}{x-1})^{p^{k+l}} - t^{p^{k+l}} = \\
&= g_{k,l}(\frac{x^t-1}{x-1} - t)^{p^{k+l}} = (x-1)^{p^{k+l}} f(x)^{p^{k+l}} = 0
\end{aligned}$$

□

We are now ready to prove the first proposition about the structure of $V_{k,l}$.

Proposition 2.6. *$V_{k,l}^- = \tilde{D}_{k,l}^{*-} / < \bar{x}_{k,l} >$ and $V_{k,l}^+ = \tilde{D}_{k,l}^{*+} / (g_{k,l}(A_{k,l}^*) \cap \tilde{D}_{k,l}^{*+})$.*

Proof. The first statement follows directly by Lemma 2.4 since $\bar{x}_{k,l}$ is clearly in $\tilde{D}_{k,l}^{*-}$. The second statement follows by Lemma 2.5. □

3. The structure of $\mathcal{V}^+_{k,l}$ and $V^+_{k,l}$

In the quest for $V^+_{k,l}$ a main role will be played by a close relative to $V^+_{k,l}$, namely

$$\mathcal{V}^+_{k,l} := \frac{\tilde{D}^{*+}_{k,l}}{\mathrm{Im}\{\tilde{\mathbb{Z}}[\zeta_{k+i-1}]^{*+} \to \tilde{D}^{*+}_{k,l}\}},$$

where $\tilde{\mathbb{Z}}[\zeta_{k+i-1}]^{*+}$ consists of units congruent to 1 modulo $(\zeta_{k+i-1}-1)$. Recall that we identify $\mathbb{Z}[\zeta_{k+l-1}]^*$ with its image in $A^*_{k,l}$ under the injection $\varphi_{k,l} : \mathbb{Z}[\zeta_{k+l-1}]^* \to A^*_{k,l}$, $\varphi_{k,l}(\epsilon) = (\epsilon, N_{k,l-1}(\epsilon))$ (see Lemma 2.5 in [H-S]).

Our main goal for now is to find the structure of $\mathcal{V}^+_{k,l}$. We will see that it is closely related to the structure of $\mathcal{V}^+_n$ which we have found in [H-S] (for semi-regular primes with some extra condition) and [H-S2] (for all semi-regular primes). In this paper we will do this under the following assumption, which is Assumption 3 in [H-S]. We will continue to call it Assumption 3 even though we don not use any assumptions 1 and 2 here. Recall that $r(p)$ denotes the index of regularity of p.

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

This holds for example if the Iwasawa invariant λ satisfy $\lambda = r(p)$ which follows from, for instance, certain congruence assumptions on Bernoulli numbers (see page 202 in [W]) which calculations have shown holds for all $p < 4000000$.

Under this assumption we can prove the following theorem.

Theorem 3.1. *If p is semi-regular and Assumption 3 holds, then* $\mathcal{V}^+_{k,l} \cong \mathcal{V}^+_{0,k+l}$.

Let $D^{*+}_{k,l}(s)$ denote the group of real units congruent to 1 modulo $(\bar{x}_{k,l} - \bar{x}^{-1}_{k,l})^s$.

Proof. By using the identifications

$$\varphi_{0,k+l} : \mathbb{Z}[\zeta_{k+l-1}]^* \to A^*_{0,k+l}$$

and

$$\varphi_{k,l} : \mathbb{Z}[\zeta_{k+l-1}]^* \to A^*_{k,l}$$

we get a commutative diagram

$$\begin{tikzcd}
 & \mathbb{Z}[\zeta_{k+l-1}]^* \arrow[dl, "g_{0,k+l}"'] \arrow[dr, "g_{k,l}"] & \\
D^*_{0,k+l} \arrow[rr, "\bar{\rho}"'] & & D^*_{k,l}
\end{tikzcd}$$

where $\bar{\rho}$ is the natural surjection. We hence get an induced surjection

$$\tilde{\rho} : \mathcal{V}^+_{0,k+l} := \frac{\tilde{D}^{*+}_{0,k+l}}{g_{0,k+l}(\tilde{\mathbb{Z}}[\zeta_{k+l-1}]^*)} \to \frac{\tilde{D}^{*+}_{k,l}}{g_{k,l}(\tilde{\mathbb{Z}}[\zeta_{k+l-1}]^*)} =: \mathcal{V}^+_{k,l}.$$

Suppose $a \in \tilde{D}^{*+}_{k,l}$ is trivial in $\mathcal{V}^+_{k,l}$, that is $a = g_{k,l}(\epsilon)$ for some $\epsilon \in \tilde{\mathbb{Z}}[\zeta_{k+l-1}]^*$, and that $a = \bar{\rho}(b)$. Then

$$\bar{\rho}(b) = a = g_{k,l}(\epsilon) = \bar{\rho}((g_{0,k+l}(\epsilon))$$

in $\tilde{D}^{*+}_{k,l}$ which implies

$$bg_{0,k+l}(\epsilon^{-1}) \in D^{*+}_{0,k+l}(p^{k+l} - p^k).$$

By Corollary 4.7 of [H-S] we have (when Assumption 3 holds) that

$$\frac{\tilde{D}^{*+}_{0,k+l}(2s)}{g_{0,k+l}(\tilde{\mathbb{Z}}[\zeta_{k+l-1}]^*) \cap \tilde{D}^{*+}_{0,k+l}(2s)}$$

is trivial whenever $2s > p^{k+l} - 2p^{k+l-1}$. Since $p^{k+l} - p^k \geq p^{k+l} - p^{k+l-1} > p^{k+l} - 2p^{k+l-1}$ this implies $bg_{0,k+l}(\epsilon^{-1}) = g_{0,k+l}(\epsilon')$ for some $\epsilon' \in \tilde{\mathbb{Z}}[\zeta_{k+l-1}]^*$ which means b is trivial in $\mathcal{V}^+_{0,k+l}$. In other words, $\tilde{\rho}$ is injective and hence an isomorphism. □

By Theorem 4.3 in [H-S] we have that when Assumption 3 holds, $\mathcal{V}^+_n \cong C^{r(p)}_{p^n}$. We hence get the following corollary of Theorem 3.1.

Corollary 3.2. *When Assumption 3 holds, $\mathcal{V}_{k,l} \cong C^{r(p)}_{p^{k+l}}$.*

The rest of this paper is devoted to proving the following theorem.

Theorem 3.3. *When Assumption 3 holds, $V^+_{k,l} = \mathcal{V}^+_{k,l}$.*

Proof. Any element of $A^{*+}_{k,l}$ can be presented as a pair $(\epsilon, e) \in \mathbb{Z}[\zeta_{k+l-1}] \times A_{k,l-1}$. Recall that we make $\mathbb{Z}[\zeta_{k+l-1}]^*$ a summand of $A^*_{k,l}$ by using the map $\varphi_{k,l} : \mathbb{Z}[\zeta_{k+l-1}]^* \to A^*_{k,l}$. We have $(\epsilon, e) = (\epsilon, N_{k,l-1}(\epsilon))(1, eN_{k,l-1}(\epsilon^{-1})) = \varphi_{k,l}(\epsilon)(1, eN_{k,l-1}(\epsilon^{-1}))$. What we need to show is hence that for all $(1, \gamma) \in A^{*+}_{k,l}$ there exists $\epsilon \in \mathbb{Z}[\zeta_{k+l-1}]^*$ such that

$$(1, \gamma) \equiv (\epsilon, N_{k,l-1}(\epsilon)) \bmod p.$$

This is equivalent to

$$\begin{aligned} \epsilon &\equiv 1 \bmod p \text{ in } \mathbb{Z}[\zeta_{k+l-1}] \\ N_{k,l-1}(\epsilon) &\equiv \gamma \bmod p \text{ in } A_{k,l-1} \\ N_{k,l-1}(\frac{\epsilon - 1}{p}) &\equiv \frac{N_{k,l-1}(\epsilon) - \gamma}{p} \bmod p \text{ in } A_{k,l-1}. \end{aligned}$$

The last condition comes from that $f_{k,l-1} = g_{k,l-1} \circ N_{k,l-1}$ (and $g_{k,l-1}$ is the surjection mod p) and we need to have

$$f_{k,l-1}((\epsilon-1)/p) = g_{k,l-1}((N_{k,l-1}(\epsilon)-\gamma)/p)$$

in $D_{k,l-1}$ for

$$(\frac{\epsilon-1}{p}, \frac{N_{k,l-1}(\epsilon)-\gamma}{p}) \in A_{k,l}$$

to hold. Since we assume $(1,\gamma) \in A_{k,l}$ we must have $g_{k,l-1}(\gamma) = f_{k,l-1}(1) = 1$ in $D_{k,l-1}$, that is, $\gamma \equiv 1 \bmod p$. What we need to prove is hence that for all $\gamma \in A^{*+}_{k,l-1}$ such that $\gamma \equiv 1 \bmod p$ there exists $\epsilon \in \mathbb{Z}[\zeta_{k+l-1}]^*$ with $\epsilon \equiv 1 \bmod p$ such that

$$N_{k,l-1}(\frac{\epsilon-1}{p}) - \frac{N_{k,l-1}(\epsilon)-1}{p} \equiv \frac{1-\gamma}{p} \bmod p. \tag{3.1}$$

Let $U_{n,k}$: {real $\epsilon \in \mathbb{Z}[\zeta_n]^*$: $\epsilon \equiv 1 \bmod \lambda_n^k$}, where $\lambda_n := (\zeta_n - 1)$. Recall that in $\mathbb{Z}[\zeta_{k+l-1}]^*$, $e \equiv 1 \bmod p$ is equivalent to $\epsilon \equiv 1 \bmod \lambda_n^{p^{k+l}-p^{k+l-1}}$. Consider the map $\Phi_{k,l-1} : U_{k+l-1,p^{k+l}-p^{k+l-1}} \to D^+_{k,l-1}$ defined by

$$\Phi_{k,l-1}(\epsilon) = N_{k,l-1}(\frac{\epsilon-1}{p}) - \frac{N_{k,l-1}(\epsilon)-1}{p} \bmod p.$$

If we can prove that $\Phi_{k,l-1}$ is a surjective group homomorphism, then we can obviously for any γ find ϵ such that 3.1 holds which in turn means Theorem 3.3 is proved. We will prove the surjectivity in Proposition 3.4 below and this ends the proof of the theorem. □

Proposition 3.4. *When Assumption 3 holds, $\Phi_{k,l-1}$ is a surjective group homomorphism for all $k \geq 0$ and $l \geq 2$.*

This result will follow from the following lemma which is the corresponding result for $k = 0$.

Lemma 3.5. *When Assumption 3 holds, $\Phi_{0,n-1}$ is a surjective group homomorphism for all $n \geq 2$.*

This is Theorem 4.4 in [H-S]. We will not re-prove it here, but for the sake of completeness we will give some indication of how the proof goes.

We start by looking the first part of $\Phi_{0,n-1}$, namely $\varphi_{0,n-1} : U_{0,p^n-p^{n-1}} \to D^+_{0,n-1}$ defined by $\varphi_{0,n-1}(\epsilon) = N_{0,n-1}((\epsilon-1)/p)$. It is easy to prove, using our standard commutative diagram, that the kernel is U_{0,p^n-1} which by Lemma 3.2 in in [H-S] equals U_{0,p^n+1}. This gives us an injection

$$\tilde{\varphi}_{0,n-1} : \frac{U_{0,p^n-p^{n-1}}}{U_{0,p^n+1}} \to D^+_{0,n-1}.$$

We then prove that this map is an also surjective, that is, an isomorphism. This is done by showing that $(U_{0,p^n-p^{n-1}})/(U_{0,p^n+1})$ have the "correct" number of elements and this is one of the harder parts of the proof. In short, to prove this we use that we have (by definition) $r(p)$ indexes $i_1, i_2 \dots i_r$ among $1, 2 \dots (p-3)/2$ such that the nominator of the Bernoulli number B_{i_k} (in reduced form) is divisible by p. We prove that $\bar{E}_n((x_n - x_n^{-1})^{2i_k})$ generate the group $\mathcal{V}_{0,n}^{+} := D_{0,n}^{*+}/g_{0,n}(\mathbb{Z}[\zeta_{n-1}]^{*+})$ where $\bar{E}_n : D_{0,n} \to D_{0,n}^{*}$ is the truncated exponential map defined by

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

We first use some old number theoretical techniques to prove the result for $n = 1$ and then lift the result to arbitrary n. To make the lifting work it is vital that we already know that $\mathcal{V}_{0,n}^{+} \cong (\mathbb{Z}/p^n\mathbb{Z})^{r(p)}$. After this we use that we know "where" to find a set of generators of $\mathcal{V}_{0,n}^{+}$ to show that $D_{0,n}^{*+}(2s) \subset g_n(\mathbb{Z}[\zeta_{n-1}]^{*+})$ when $2s > p^n - 2p^{n-1}$. Since $\ker(g_{0,n}) = U_{n-1,p^n-1}^{+}$ (by Lemma 2.6, [H-S]) when $g_{0,n}$ is restricted to units, one can now show that $D_{0,n}^{*+}(2s) \cong U_{n-1,2s}^{+}/U_{n-1,p^n-1}^{+}$ if $2s > p^n - 2p^{n-1}$. Finally we set $2s = p^n - p^{n-1}$ and easily calculate the number of elements in $D_{0,n}^{*+}(p^n - p^{n-1})$ to be the "correct" one.

Now let $\omega_{0,n-1} : U_{n-1,p^n-p^{n-1}}^{+} \to D_{0,n-1}^{+}$ be defined by

$$\omega_{0,n-1}(\gamma) := g_{n-1}((N_{n-1}(\gamma) - 1)/p).$$

As before one can show that $\omega_{0,n-1}$ is a group homomorphism and that we get an induced map $\tilde{\omega}_{0,n-1} : (U_{0,p^n-p^{n-1}})/(U_{0,p^n+1}) \to D_{0,n-1}^{+}$ Since $\tilde{\varphi}_{0,n-1}$ is an isomorphism we can find units $\{\epsilon_i\} \subset U_{0,p^n-p^{n-1}}$ such that $\{\tilde{\varphi}_{0,n-1}(\epsilon_i)\}$ is a basis of $D_{0,n-1}^{+}$. We now consider the map induced by $\tilde{\varphi}_{0,n-1}(\epsilon_i) \mapsto \tilde{\varphi}_{0,n-1}(\epsilon_i) - \tilde{\omega}_{0,n-1}(\epsilon_i)$ (in the "standard" basis $(x - x^{-1})^{2i}$). After some pretty long calculations we finally manage to find some congruences on our norm maps which helps us conclude that the matrix for the map above is upper triangular with invertible elements on the diagonal, that is, invertible. This means that the map $\tilde{\varphi}_{0,n-1} - \tilde{\omega}_{0,n-1}$ is in particular surjective, which implies that $\Phi_{0,n-1} = \varphi_{0,n-1} - \omega_{0,n-1}$ is also surjective.

We are now ready to prove Proposition 3.4.

Proof of Proposition 3.4. We will show that $\Phi_{k,l-1} = \bar{\rho} \circ \Phi_{0,k+l-1}$, where $\bar{\rho} : D_{0,k+l-1} \to D_{k,l-1}$ is the natural surjection, which means that $\Phi_{k,l-1}$ is surjective (by Lemma 3.5) as a composition of surjective maps. It is enough to show that

$g_{k,l-1} \circ N_{k,l-1} = \bar{\rho} \circ g_{0,k+l-1} \circ N_{0,k+l-1}$. Consider the diagram

(3.2)
$$\begin{tikzcd}
 & A_{0,k+l-1} \arrow[r, "g_{0,k+l-1}"] \arrow[dd, "\rho"] & D_{0,k+l-1} \arrow[dd, "\bar{\rho}"] \\
\mathbb{Z}[\zeta_{k+l-1}] \arrow[ur, "N_{k,l-1}"] \arrow[dr, "N_{0,k+l-1}"'] & & \\
 & A_{k,l-1} \arrow[r, "g_{k,l-1}"'] & D_{k,l-1}
\end{tikzcd}$$

The square part is obviously commutative. It is hence enough to prove that the triangular part is commutative. Recall that an element $a \in A_{r,s}$ can be uniquely represented by a pair $(z_{r+s-1}, b) \in \mathbb{Z}_{[}\zeta_{r+s-1}] \times A_{r,s-1}$ Using this recursively we find that any element of $A_{k,l-1}$ can be uniquely represented by a $(l-1)$-tuple in $\mathbb{Z}[\zeta_{k+l-2}] \times \mathbb{Z}[\zeta_{k+l-2}] \times \ldots \times \mathbb{Z}[\zeta_k]$ and that any element of $A_{0,k+l-1}$ can be uniquely represented by a $(k+l-1)$-tuple in $\mathbb{Z}[\zeta_{k+l-2}] \times \mathbb{Z}[\zeta_{k+l-2}] \times \ldots \times \mathbb{Z}[\zeta_0]$. As before we consider the tuple-representations as identifications. If $a = (z_{k+l-2}, z_{k+l-2}, \ldots, z_0) \in A_{0,+l-1}$ (with $z_j \in \mathbb{Z}[\zeta_j]$) we have that $\rho(a) = (z_{k+l-2}, z_{k+l-2}, \ldots, z_k)$. 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. By Proposition 2.1 of [H-S] we have that

$$\begin{aligned}
\rho(N_{0,k+l-1}(a)) &= \rho((\tilde{N}_{k+l-1,1}(a), \ldots, \tilde{N}_{k+l-1,l-1}(a), \ldots, \tilde{N}_{k+l-1,k+l-1}(a))) = \\
&= (\tilde{N}_{k+l-1,1}(a), \tilde{N}_{k+l-1,2}(a), \ldots, \tilde{N}_{k+l-1,l-1}(a)) = \\
&= N_{k,l-1}(a)
\end{aligned}$$

which completes the proof. □

4. Conclusions and Discussion

We can now summarize and write down the main theorem of this paper. Recall that $[m] := (m + |m|)/2$.

Theorem 4.1. *Let p be a semi-regular prime satisfying Assumption 3. Then there exists an exact sequence*

$$0 \to V_{k,l}^{+} \oplus V_{k,l}^{-} \to \operatorname{Pic} A_{k,l} \to \operatorname{Cl} \mathbb{Q}(\zeta_{k+l-1}) \oplus \operatorname{Pic} A_{k,l-1} \to 0,$$

where

$$V_{k,l}^{+} \cong C_{p^{k+l}}^{r(p)}$$

and

$$V_{k,l}^{-} \cong \prod_{i=1}^{k+l} C_{p^i}^{t_i},$$

where

$$t_i = \frac{p^{k+l-i+1} - p^{[k-i+1]}}{2} - 2\frac{p^{[k+l-i]} - p^{[k-i]}}{2} + \frac{p^{[k+l-i-1]} - p^{[k-i-1]}}{2}$$

for $i = 1, 2, \ldots, k+l$. *and* $t_{k+l} = \frac{p-3}{2}$.

Proof. The exact sequence is just the sequence 1.4. The structure of $V_{k,l}^{+}$ follows directly by Theorem 3.3 and Corollary 3.2. By Proposition 2.6,

$$V_{k,l}^{-} = \frac{\tilde{D}_{k,l}^{*+}}{< \bar{x}_{k,l} >}.$$

The structure of $\tilde{D}_{k,l}^{*+}$ can be found in Lemma 2.2. Since there exists elements of order p^{k+l} in $\tilde{D}_{k,l}^{*-}$ it is easy to see that $\bar{x}_{k,l}$ must have order p^{k+l} which yields the structure of $V_{k,l}^{-}$. □

One can ask the question if Assumption 3 really is necessary. The structure of $V_{k,l}^{-}$ holds for all primes, so here lies no problem. Regarding the +-part, we prove in [H-S2] that

$$\mathcal{V}_{0,n}^{+} \cong C_{p^n}^{r_0} \oplus C_{p^{n-1}}^{r_1 - r_0} \oplus \ldots \oplus C_{p}^{r_{n-1} - r_{n-2}},$$

where the numbers r_i are given by the order of certain groups of units in $\mathbb{Q}(\zeta_i)$ and r_0 can be shown to equal $r(p)$ (see [H-S] for details). When Assumption 3 holds, all r_i equal $r(p)$ which gives us $\mathcal{V}_{0,n}^{+} \cong C_{p^n}^{r(p)}$ as mentioned. When we in the present paper show that $\mathcal{V}_{k,l}^{+} \cong \mathcal{V}_{0,k+l}^{+}$ we for technical reasons use Assumption 3 but we still conjecture that

$$\mathcal{V}_{k,l}^{+} \cong C_{p^{k+l}}^{r_0} \oplus C_{p^{k+l-1}}^{r_1 - r_0} \oplus \ldots \oplus C_{p}^{r_{k+l-1} - r_{k+l-2}}$$

for each semi-regular prime. Showing that $\mathcal{V}_{k,l}^{+} = V_{k,l}^{+}$ without using Assumption 3 seems to be harder and this result is not known even in the case $k = 0$.

References

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

[H-S] O. Helenius and A. Stolin, *Unit Bases in Integer Group Rings and the Kervaire-Murthy Conjectures*
Preprint 2001:40, Chalmers University of Technology, 2001.

[H-S2] O. Helenius and A. Stolin, *Picard Groups of Integer Group Rings and Units in Cyclotomic Fields*
Preprint 2001:75, Chalmers University of Technology, 2001.

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

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

[U2] Ullom, S. *Class Groups of Cyclotomic Fields and Group Rings*
London Math. Soc. (2) 17 (1978), no 2, 231-239.

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

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

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