THESIS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

On the Picard Group of Integer Group Rings

OLA HELENIUS

Department of Mathematics
CHALMERS UNIVERSITY OF TECHNOLOGY
GÖTEBORG UNIVERSITY
Göteborg, Sweden 2002

On the Picard Group of Integer Group Rings
OLA HELENIUS
ISBN 91-7291-125-5

Doktorsavhandlingar vid Chalmers tekniska högskola
Ny serie nr 1807
ISSN 0346-718x

Department of Mathematics
Chalmers University of Technology and
Göteborg University
SE-412 96 Götborg
Sweden
Telephone +46(0)31-772 1000

Chalmers University of Technology and Göteborg University
Göteborg, Sweden 2002

Abstract

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

$$0 \to V_n^- \times V_n^+ \to \operatorname{Pic} \mathbb{Z}C_{p^{n+1}} \to \operatorname{Pic} \mathbb{Z}C_{p^n} \times \operatorname{Cl} \mathbb{Z}[\zeta_n] \to 0,$$

where V_n^- is known explicitly. In this thesis we deal with some problems regarding V_n^+. This group is a quotient of a group denoted $\mathcal{V}_n^+$ and a conjecture of Kervaire and Murthy from 1977 states the two groups are isomorphic. The conjecture also states that these groups are in fact isomorphic to the p-component of $\operatorname{Cl} \mathbb{Z}[\zeta_{n-1}]$.

In the first paper in this thesis we introduce a new technique and give a new proof of the known result that $\mathcal{V}_n^+$, and hence also V_n^+, is trivial when p is a regular prime. The proof is based on a generalization to $\mathbb{Z}[\zeta_n]$ of Kummer's famous result stating that a unit in $\mathbb{Z}[\zeta_0]$ congruent to 1 modulo p is a p-th power of another unit if p is a regular prime.

In the second paper we consider the structure of $\mathcal{V}_n^+$ and its relations with V_n^+ under three various assumptions on the prime p. All these assumptions are valid for all primes up to 4.000.000 and no primes for which the assumptions fail are known. Under two of these assumptions we prove that $V_n^+ \cong \mathcal{V}_n^+$.

In the third paper we give an exact formula for $\mathcal{V}_n^+$ under the most general assumption, namely that p is semi-regular, which by Vandiver's conjecture should be all primes. We also prove that $\mathcal{V}_n^+$ and $\operatorname{Cl}^{(p)} \mathbb{Z}[\zeta_{n-1}]$ have the same number of generators, which can be considered as a "weak version" of the Kervaire-Murthy conjecture that $\mathcal{V}_n^+ \cong \operatorname{Cl}^{(p)} \mathbb{Z}[\zeta_{n-1}]$.

In the final paper we discuss a family of rings $A_{k,l}$ which in some sense fit in between $\mathbb{Z}C_{p^n}$ and $\mathbb{Z}[\zeta_n]$. Under one of our assumptions above we give 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.

Keywords: Picard group, Grothendieck group, integer group ring, cyclic group p-group, cyclotomic field, class group, Kummer's lemma, semi-regular prime.

2000 AMS Subject classification: 11R65, 11R18, 19A31.

This thesis consists of an introduction and the four papers

[**H1**] O. Helenius, *Kummer's Lemma and Picard Groups of Integer Group Rings*
Theme Issue on Commutative Algebra, Arabian Journal of Science and Engineering Volume 26 (2001), Number 1C, 107-118.

[**H-S1**] 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 2001:72, Chalmers University of Technology, 2001.

[**H2**] O. Helenius, *On the Picard Group of some Polynomial Rings*
Preprint 2001:74, Chalmers University of Technology, 2001.

ACKNOWLEDGEMENT

I would like to thank my advisor Alexander Stolin for his friendship and support during the years we have worked together. Without him this thesis would not have seen the light of day and through our collaboration I have learnt more about mathematics than I thought possible. Alexanders enthusiasm and ability to see things in a positive way have been a constant when other things have changed.

I would also like to thank all other people, faculty and staff, that have made my years at the departement of Mathematics such a nice time. A special thanks goes to my friends and colleagues Samuel Bengmark and Laura Fainsilber and to the man who first got me interested in mathematics, Juliusz Brzezinski. I also thank Per Salberger for interesting conversations.

A thanks also goes to my current and former fellow Ph-D students for making coffee breaks and lunches such a fun time, Elise Björkholdt, Martin Brundin, Patrik Lundström, Niklas Lindholm, Anette Wiberg, Magnus Wängefors, and all others. A "surf's up" goes to Martin Adiels for a lot of nice windsurfing conversations in the lunch room.

On a more personal note I would like to thank my wife Gisela for her support during that last five years, especially since our son Sigge was born three months ago.

Ola Helenius

Göteborg January 2002

ON THE PICARD GROUP OF INTEGER GROUP RINGS

OLA HELENIUS

1. Introduction to K-groups and Picard groups

This thesis is made up of this introduction and the four papers [H1], [H-S], [H-S2] and [H2], the middle two joint with Alexander Stolin. We concern ourselves with Picard groups of integer group rings. Specifically we try to find information about the Picard group of $\mathbb{Z}C_{p^n}$, where C_{p^n} denotes the cyclic group of order p^n. Inside the algebraic framework in which we work, Picard groups and K_0-groups have a lot in common and most mathematicians that have worked on our problem before us have formulated it in the language of K_0-groups. In this introduction we will first give a very brief survey on the history of Picard- and K_0-groups as well as the history of our particular problem. We then go on and write down some definitions and basic results on Picard- and K-groups to give the non-expert reader a clue about what kind of objects we deal with. Finally we give an overview of the four papers that make up this thesis, what kind of techniques we use and what kind of results we prove.

In retrospective, papers by Higman 1940 ([Hig]) and Whitehead 1939 ([Wh]) are considered the first steps towards K-theory. The techniques used by Grothendieck 1958 ([BSG]) in his proof of the generalized Riemann Roch Theorem involves the functor K, now known as K_0, and can maybe be considered the real start of the subject. In 1961 Atiayh and Hirzebruch introduced topological K-theory ([A-H]) and this turned out to be a very fruitful theory leading to the proving of many topological results. Algebraic K-theory first imitated its topological predecessor but then quickly spread into domains where topology plays no central role. K-theoretical methods were used to prove results in the theory of C^*-algebras, number theory and non-commutative algebra. Several authors were involved in the development but Hyman Bass was maybe the most influential and his book *Algebraic K-theory*, [B], is still a very important source of information.

There are many (different) ways of defining higher K-groups of a ring, but here we only concern ourselves with the Grothendieck group K_0 and the Whitehead group K_1. Let A be a ring. In this thesis all rings will be commutative with

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

identity and all ring homomorphism will map 1 to 1. The group K_0A can be seen as the group of (differences of isomorphism classes of) projective finitely generated A-modules. An A-module P is called projective if there exists an A-module Q such that $P \oplus Q$ is free. A module M is called finitely generated if there exists a finite subset N of M such that $RN = M$. It is easy to see that a module P is finitely generated and projective if and only if there exists a module Q such that $P \oplus Q \cong A^n := \bigoplus_{i=1}^{n} A$ for some natural number n. Formally, if P and Q are such modules we let brackets denote the isomorphism class and define an operation by

$$[P] + [Q] := [P \oplus Q].$$

The set of all isomorphism classes with this operation is a monoid. The group K_0A is defined as the quotient of the free abelian group generated by this monoid modulo the subgroup generated by all expressions $[P] + [Q] - [P \oplus Q]$. It is easy to see that every element of K_0A can be represented as [P]-[Q] for some suitably chosen P and Q.

The group K_1A can be seen as a group of infinite matrices. Let $\mathrm{GL}(n, A)$ be the group of $n \times n$ invertible matrices. For each $n = 1, 2, \ldots$, consider the embedding of $\mathrm{GL}(n, A)$ into $\mathrm{GL}(n + 1, A)$ defined by

$$H \mapsto \begin{pmatrix} H & 0 \\ 0 & 1 \end{pmatrix}$$

for $H \in \mathrm{GL}(n, A)$. Define the group $GL(A)$ as the union of the sequence

$$\mathrm{GL}(1, A) \subset \mathrm{GL}(2, A) \subset \mathrm{GL}(3, A) \subset \cdots .$$

A matrix in $GL(A)$ is called elementary if it coincides with the identity matrix except for a single off-diagonal entry. It can be shown that the multiplicative group $E(A)$ generated by the elementary matrices coincides with the commutator subgroup of $GL(A)$. We define the group K_1A as the quotient $GL(A)/E(A)$. If $f : A \to A'$ is a ring homomorphism we can in the obvious way define a group homomorphism $f_* : K_1A \to K_1A'$.

For more facts about these groups and proofs of the statements above, see [M], [Si] and [B].

Picard groups are an important concept in algebraic geometry. If X is scheme (or a ringed space), an invertible sheaf is defined to be a sheaf of locally free $\mathcal{O}_X$-modules of rank 1. The Picard group, $\operatorname{Pic} X$, of X is then defined as the group of isomorphism classes of invertible sheaves on X under the operation $\otimes$, the tensor product of sheaves. One can show that $\operatorname{Pic} X$ can be expressed as the cohomology group $H^1(X, \mathcal{O}_X)$ and if X is a an integral scheme, then $\operatorname{Pic} X$ is isomorphic to $\operatorname{CaCl} X$, the Cartier class group of X. Hence, if X is a noetherian, integral, separated locally factorial scheme, then $\operatorname{Pic} X \cong \operatorname{Cl} X$, the group of Weil

divisors of X modulo linear equivalence. The latter statement holds for example if X is a (complete non-singular) curve over an algebraically closed field.

The "geometric" definition of the Picard group carries over to our algebraical setting but instead of considering sheaves of $\mathcal{O}_X$-modules we simplify a bit and simply considers modules over a commutative ring with identity element (denoted 1).

An A-module M is called invertible if it satisfies any of the following equivalent conditions:

i) M is projective and finitely generated of constant rank 1.
ii) $\widehat{M} \otimes_A M \cong A$, where $\widehat{M} := \mathrm{Hom}_A(M, A)$.
iii) There exists an A-module N with $N \otimes_A M \cong A$.

To define the local rank of A, let $\mathfrak{p}$ be a prime ideal of A and let $A_\mathfrak{p}$ denote the localization of A at $\mathfrak{p}$. If M is an A-module the localization $M_\mathfrak{p}$ of M at $\mathfrak{p}$ is isomorphic to $A_\mathfrak{p} \otimes_A M$. Suppose M is finitely generated and projective. Then, since $A_\mathfrak{p}$ is a local ring, $M_\mathfrak{p}$ is a free, finitely generated $A_\mathfrak{p}$-module and hence $M_\mathfrak{p} \cong A_\mathfrak{p}^n$ for some n. We can hence define $\mathrm{rank}_\mathfrak{p}(M) = n$. M is said to have constant rank if $\mathrm{rank}_\mathfrak{p}(M)$ is constant over all prime ideals $\mathfrak{p}$ of A.

If A is a commutative ring with identity, we define $\mathrm{Pic}\, A$ as the group of isomorphism classes of invertible modules under the tensor product $\otimes_A$. The identity element of the Picard group is the class of A, considered as a module over itself, and the inverse of the class of P is the class of $\widehat{P}$, where $\widehat{P} := \mathrm{Hom}_A(M, A)$.

The terminology *invertible* can be explained and this explanation also give a connection between the Picard group and K_0. First note that we can supply K_0A with a ring structure using the tensor product. By using the unique homomorphism $i : \mathbb{Z} \to A$ we get a homomorphism $i_\# : K_0\mathbb{Z} \to K_0A$ by sending a projective module P over $\mathbb{Z}$ to $i_\#P := A \otimes_\mathbb{Z} P$. One can show that every finitely generated projective module over $\mathbb{Z}$ (or any principal ideal domain R or field F for that matter) is free and that two free modules $\mathbb{Z}^r$ and $\mathbb{Z}^s$ (R^r and R^s or F^r and F^s) are isomorphic if $r = s$. Hence $K_0\mathbb{Z} \cong \mathbb{Z}$ (and $K_0R \cong \mathbb{Z}$ and $K_0F \cong \mathbb{Z}$). Since A is commutative we can also always find a homomorphism j from A to a field or skew field F. Since $j_\# i_\#$ is an isomorphism we get a direct sum decomposition $K_0A = \mathrm{Im}\, i_\# \oplus \ker j_\#$ where the first summand is free cyclic. $\ker j_\#$ is an ideal in the ring K_0A which is denoted $\tilde{K}_0A$ and called the projective class groups of A. Clearly we have

$$K_0A \cong \mathbb{Z} \oplus \tilde{K}_0A. \tag{1.1}$$

In the ring, K_0A, consider the multiplicative group of units $1 + \tilde{K}_0A$. One can show that two finitely generated projective modules, P and Q generate the same element in K_0A if and only if they are stably isomorphic, $P \oplus A^r \cong Q \oplus A^r$ for some r. Moreover one can show that two invertible modules are stably isomorphic if and only if they are isomorphic, This means we have an embedding of $\operatorname{Pic} A$ into the group of units of K_0A, so the elements in the Picard group are really invertible elements in the ring K_0A. One can also show the following results:

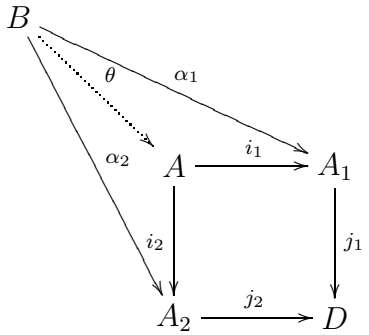
Proposition 1.1. *If $A = \mathbb{Z}C_{p^n}$, then $\operatorname{Pic} A \cong \tilde{K}_0A$. If A is a Dedekind ring $\tilde{K}_0A \cong \operatorname{Pic} A \cong \operatorname{Cl} A$.*

Moreover we also know that $K_0A \cong \mathbb{Z}$ when A is a field or a PID and this also holds when A is a local ring.

Proposition 1.2. *If A a principal ideal domain, a field or a local ring, then $K_0A \cong \mathbb{Z}$ and hence $\tilde{K}_0A = 0$ and $\operatorname{Pic} A = 0$.*

We will now define a pullback of a ring which we will use to extract some exact sequences involving K- and Picard groups.

Let A_1, A_2 and D be commutative rings with unity and let $j_k : A_k \mapsto D,\ k = 1, 2$ be homomorphisms. A ring A and homomorphisms $i_k : A \mapsto A_k,\ k = 1, 2$, is called a pullback (of A_1 and A_2 over D) if the following condition holds. For all rings B and maps $\alpha_k : B \mapsto A_k,\ k = 1, 2$ such that the outer part of the diagram below commutes, there is a unique θ such that the whole diagram commutes.



If A is a pullback of A_1 and A_2 over D we will call the rectangular part of the diagram above a pullback diagram. It is easy to see that a pullback is unique up to isomorphism. One can show that

$$A = \{(a_1, a_2) \in A_1 \times A_2 \,:\, j_1(a_1) = j_2(a_2)\}$$

is a pullback of A_1 and A_2 over D. Often we will identify any pullback with A defined above. If A is a commutative ring with unity and α and β ideals in A,

then

$$\begin{array}{ccc} A/(\alpha\cap\beta) & \longrightarrow & A/\alpha \\ \downarrow & & \downarrow \\ A/\beta & \longrightarrow & A/(\alpha+\beta) \end{array} \tag{1.2}$$

is a pullback diagram. Pullbacks like this are the absolute starting point for all papers making up this thesis.

Example 1.3. *If we put* $A=\mathbb{Z}[x]$, $\alpha=((x^{p^n}-1)/(x-1))$ *and* $\beta=(x-1)$ *we get* $\alpha\cap\beta=(x^{p^n}-1)$ *and* $\alpha+\beta=(x-1,p^n)$. *Since* $\mathbb{Z}[x]/(x-1)\cong\mathbb{Z}$ *and* $\mathbb{Z}[x]/(x-1,p^n)\cong\mathbb{Z}/p^n\mathbb{Z}$. *Moreover* $\mathbb{Z}C_{p^n}\cong\mathbb{Z}[x]/(x^{p^n}-1)$. *We hence have a pullback diagram*

$$\begin{array}{ccc} \mathbb{Z}C_{p^n} & \longrightarrow & \frac{\mathbb{Z}[x]}{\left(\frac{x^{p^n}-1}{x-1}\right)} \\ \downarrow & & \downarrow \\ \mathbb{Z} & \longrightarrow & \frac{\mathbb{Z}}{p^n\mathbb{Z}} \end{array} \tag{1.3}$$

for each $n=1,2,\ldots$.

Example 1.4. *Again, put* $A=\mathbb{Z}[x]$. *Let* $\alpha=((x^{p^{k+l+1}}-1)/(x^{p^{k+l}}-1))$ *and* $\beta=((x^{p^{k+l}}-1)/(x^{p^k}-1))$. *Then,* $\alpha\cap\beta=((x^{p^{k+l+1}}-1)/(x^{p^k}-1))$ *and* $\alpha+\beta=((x^{p^{k+l}}-1)/(x^{p^k}-1),p)$. *Since* $\mathbb{Z}[x]/((x^{p+l+1}-1)/(x^{p^{k+l}}-1))\cong\mathbb{Z}[\zeta_{k+l}]$, *where* ζ_{k+l} *is a primitive* p^{k+l+1}*th root of unity, we have a pullback diagram*

$$\begin{array}{ccc} \frac{\mathbb{Z}[x]}{\left(\frac{x^{p^{k+l+1}}-1}{x^{p^k}-1}\right)} & \longrightarrow & \mathbb{Z}[\zeta_{k+l}] \\ \downarrow & & \downarrow \\ \frac{\mathbb{Z}[x]}{\left(\frac{x^{p^{k+l}}-1}{x^{p^k}-1}\right)} & \longrightarrow & \frac{\mathbb{F}_p[x]}{\left(\frac{x^{p^{k+l}}-1}{x^{p^k}-1}\right)} \end{array} \tag{1.4}$$

Following Milnor, we now indicate how starting from a pullback diagram

$$\begin{array}{ccc} A & \xrightarrow{i_1} & A_1 \\ {\scriptstyle i_2}\downarrow & & \downarrow{\scriptstyle j_1} \\ A_2 & \xrightarrow{j_2} & D \end{array} \tag{1.5}$$

and projective (finitely generated) modules P_1 and P_2 over A_1 and A_2 respectively, one can extract projective (finitely generated) modules over D and A and get a commutative square of additive groups where each group has a module structure over the corresponding ring in the pullback diagram. We will need to make the extra assumption that j_1 or j_2 is surjective. For a full treatment of the matters below we refer to [M].

First consider a ring homomorphism $f : A \to A'$. If M is a projective (finitely generated) A-module, then we can define a projective (finitely generated) A'-module $f_\# M := A' \otimes_A M$. We can also define a A-linear map $f_* : M \to f_\# M$ by $f_*(m) = 1 \otimes m$. Now return to the pullback diagram above and suppose that there exists a D-module isomorphism $h : j_{1\#} P_1 \to j_{2\#} P_2$. Define

$$M = M(P_1, P_2, h) := \{(p_1, p_2) \in P_1 \times P_2 \ : \ hj_1(p_1) = j_2(p_2)\}.$$

We get a A-module structure on M by setting

$$a(p_1, p_2) = (i_1(a)p_1, i_2(a)p_2).$$

The following results are Theorem 2.1, 2.2 and 2.3 of [M].

Proposition 1.5. *Let M be the module constructed above. Then,*

i) M is projective over A and if P_1 and P_2 are finitely generated over A_1 and A_2 respectively, then M is finitely generated over A.
ii) Every projective A-module is isomorphic to $M(P_1, P_2, h)$ for some suitably chosen P_1, P_2 and h.
iii) The modules P_1 and P_2 are naturally isomorphic to $i_{1\#}M$ and $i_{2\#}M$ respectively.

This gives us a commutative diagram of additive groups

$$\begin{array}{ccc} M & \longrightarrow & P_1 \\ \downarrow & & \downarrow{\scriptstyle hj_{1*}} \\ P_2 & \xrightarrow{j_{2*}} & j_{2\#}P_2 \end{array}$$

The definition of pullbacks for abelian groups is similar to the one for rings. It is easy to see that our in commutative square M is actually a pullback of P_1 and P_2 over $j_{2\#}P_2$.

We are now ready to present the (K_1, K_0)-Mayer-Vietoris Sequence, originally obtained by Milnor. The reason why the sequence below bears the name Mayer-Vietoris is the resemblance with the Mayer-Vietoris long exact sequence of algebraic topology (see for example [R] p. 177).

Proposition 1.6. *Consider the pullback diagram of rings (1.5) with j_1 or j_2 surjective. There is an exact sequence of additive groups*

$$K_1A \xrightarrow{\alpha_1} K_1A_1 \oplus K_1A_2 \xrightarrow{\beta_1} K_1D \xrightarrow{\partial} K_0A \xrightarrow{\alpha_0} K_0A_1 \oplus K_0A_2 \xrightarrow{\beta_0} K_0D.$$

The homomorphisms α_i and β_i, $i = 0, 1$, are defined by

$$\begin{aligned} \alpha_1(a_1) &= (i_{1*}(a_1), i_{2*}(a_1)) \\ \beta_1(b_1, c_1) &= j_{1*}(b_1) - j_{2*}(c_1) \\ \alpha_0(a_0) &= (i_{1*}(a_0), i_{2*}(a_0)) \\ \beta_0(b_0, c_0) &= j_{1*}(b_0) - j_{2*}(c_0) \end{aligned}$$

for $a_i \in K_iA$, $b_i \in K_iA_1$ and $c_i \in K_iA_2$. To define ∂ we first observe that an element d of K_1D can be represented by a matrix in $\mathrm{GL}(n, D)$ for some n. This matrix determines an isomorphism h_d from the free D-module $j_{1\#}A_1^n$ to the free D-module $j_{2\#}A_2^n$. Let $M = M(A_1^n, A_2^n, h_d)$ and define

$$\partial(d) = [M] - [A^n] \in K_0A.$$

The verification that ∂ is a well defined homomorphism and that the sequence is exact is routine. We will now indicate how one can obtain from the (K_0, K_1)-Mayer-Vietoris sequence a similar sequence involving unit groups and Picard groups.

Proposition 1.7. *Let A be a ring. There exist surjective maps* $\det_0 : K_0A \to \operatorname{Pic} A$ *and* $\det_1 : K_1A \to A^*$

The proof of this can be found in [Si] p. 57 and p. 112. The map $\det_0$ is defined using exterior (or alternating) product $\bigwedge_A^n$ (see [L] p 731). If M is a projective finitely generated A-module of constant rank m, then $\bigwedge_A^n M$ is a projective finitely generated A-module of constant rank $\binom{m}{n}$. One can show that there exists subrings H and RK_0A of K_0A such that $K_0A \cong H \oplus RK_0A$, where every module in RK_0A can be presented as $[M] - [A^n]$ for some M and n. The map $\det_0$ is defined as the composition of the surjection $K_0A \to RK_0A$ with the map

$$RK_0A \to \operatorname{Pic} A \qquad [M] - [A^n] \mapsto \textstyle\bigwedge_A^m M,$$

where $m = \operatorname{rank} M$.

With our definition of K_1A we can define $\det_1 : K_1A \to A^*$ as the map induced by the usual determinant $GL(A) \to A^*$. This is well defined since any elementary matrix has trivial determinant.

Proposition 1.8. *Consider the pullback diagram of rings (1.5) with j_1 or j_2 surjective. The diagram*

$$\begin{array}{ccccccc}
K_1A & \xrightarrow{\alpha_1} & K_1A_1 \oplus K_1A_2 & \xrightarrow{\beta_1} & K_1D & \xrightarrow{\partial} & \\
\downarrow{\scriptstyle \det_1} & & \downarrow{\scriptstyle \det_1 \oplus \det_1} & & \downarrow{\scriptstyle \det_1} & & \\
A^* & \xrightarrow[\alpha_1]{} & A_1^* \oplus A_2^* & \xrightarrow[\beta_1]{} & D^* & \xrightarrow[\partial]{} & \\
\xrightarrow{\partial} & K_0A & \xrightarrow{\alpha_0} & K_0A_1 \oplus K_0A_2 & \xrightarrow{\beta_0} & K_0D & \\
& \downarrow{\scriptstyle \det_0} & & \downarrow{\scriptstyle \det_0 \oplus \det_0} & & \downarrow{\scriptstyle \det_0} & \\
\xrightarrow[\partial]{} & \operatorname{Pic} A & \xrightarrow[\alpha_0]{} & \operatorname{Pic} A_1 \oplus \operatorname{Pic} A_2 & \xrightarrow[\beta_0]{} & \operatorname{Pic} D &
\end{array}$$

is commutative and the rows are exact.

The bottom row is called the $(*, \mathrm{Pic})$-Mayer-Vietoris exact sequence corresponding to the pullback diagram 1.5. The maps in the this sequence are defined as follows:

$$\begin{aligned}
\alpha_1(a) &= (i_1(a), i_2(a)) \\
\beta_1(a_1, a_2) &= j_1(a_1) j_2(a_2)^{-1} \\
\alpha_0(P) &= (i_{1*}(P), i_{2*}(P)) \\
\beta_0(P_1, P_2) &= j_{1*}(P_1) j_{2*}(P_2)^{-1}
\end{aligned}$$

for $a \in A^*$, $a_i \in A_i^*$, $P \in \operatorname{Pic} A$ and $P_i \in \operatorname{Pic} A_i$. To define ∂ we first observe that an element d of D^* can be thought of as an isomorphism h between $j_{1\#}A_1 \cong D$ and $j_{2\#}A_2 \cong D$. Let $\partial(d) := M(A_1, A_2, h)$. The proof of the proposition can be found in [Si]. In all four papers in this thesis, the starting point will be the $(*, \mathrm{Pic})$-sequence associated to a pullback of the type from Example 1.4. As an illustration of how one can use this to find information on the Picard group of some ring we will prove the following result, which is a simple generalization of Rim's theorem.

Proposition 1.9. *For all $n = 1, 2, \ldots$ we have*

$$\operatorname{Pic} \mathbb{Z}C_{p^n} \cong \operatorname{Pic} \big(\mathbb{Z}[x]/\big(\frac{x^{p^n} - 1}{x - 1}\big)\big).$$

Proof. Consider the pullback from Example 1.3. The corresponding $(*, \mathrm{Pic})$-Mayer-Vietoris exact sequence reads

$$\mathbb{Z}C_{p^n}^* \to \mathbb{Z}^* \times \big(\frac{\mathbb{Z}[x]}{\big(\frac{x^{p^n}-1}{x-1}\big)}\big)^* \to \big(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\big)^* \to \mathrm{Pic}\,\mathbb{Z}C_{p^n} \to$$
$$\to \mathrm{Pic}\,\mathbb{Z} \times \mathrm{Pic}\,\frac{\mathbb{Z}[x]}{\big(\frac{x^{p^n}-1}{x-1}\big)} \to \mathrm{Pic}\,\frac{\mathbb{Z}}{p^n\mathbb{Z}}.$$

Since $\mathbb{Z}$ is a Dedekind principal ideal domain, $\mathrm{Pic}\,\mathbb{Z} = 0$ and since $\mathbb{Z}/p^n\mathbb{Z}$ is local $\mathrm{Pic}\,\mathbb{Z}/p^n\mathbb{Z} = 0$. This yields the exact sequence

$$\{1,-1\} \times \big(\frac{\mathbb{Z}[x]}{\big(\frac{x^{p^n}-1}{x-1}\big)}\big)^* \xrightarrow{\beta} \big(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\big)^* \to \mathrm{Pic}\,\mathbb{Z}C_{p^n} \xrightarrow{\alpha} \mathrm{Pic}\,\frac{\mathbb{Z}[x]}{\big(\frac{x^{p^n}-1}{x-1}\big)} \to 0$$

and if we can prove that β is surjective, exactness gives us that α is an isomorphism which is what we want to show. Obviously, it is enough to show that

$$\Big(\frac{\mathbb{Z}[x]}{\big(\frac{x^{p^n}-1}{x-1}\big)}\Big)^* \to \big(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\big)^*,\ x \mapsto 1$$

is surjective. Fix $k \in (\mathbb{Z}/p^n\mathbb{Z})^*$. Consider

$$\frac{x^k-1}{x-1} \in \frac{\mathbb{Z}[x]}{\big(\frac{x^{p^n}-1}{x-1}\big)}$$

which easily can be shown to map to $k \in (\mathbb{Z}/p^n\mathbb{Z})^*$. We need to show that $(x^k-1)/(x-1)$ is a unit. Since $(k,p) = 1$ we can find integers r and s such that $ks - p^nr = 1$. Moreover,

$$\begin{aligned}\frac{x^{1+p^nr}-1}{x^k-1} &= \frac{x^{ks}-1}{x^k-1} = \\ &= x^{k(s-1)} + x^{k(s-2)} + \ldots + x^k + 1 \in \frac{\mathbb{Z}[x]}{\big(\frac{x^{p^n}-1}{x-1}\big)}\end{aligned}$$

and since

$$\begin{aligned}\frac{x^k-1}{x-1}\frac{x^{1+p^nr}-1}{x^k-1} &= \frac{x^{1+p^nr}-1}{x-1} = \\ &= 1 + x(x^{p^n(r-1)} + \ldots + x^{p^n} + 1)\frac{x^{p^n}-1}{x-1} = 1 \in \frac{\mathbb{Z}[x]}{\big(\frac{x^{p^n}-1}{x-1}\big)}\end{aligned}$$

which proves our statement. □

Calculating K_0G, for various groups G is important because of applications in algebraic topology. For example, Suppose X is a topological space with fundamental group π, dominated by a finite CW-complex. C.T.C. Wall defined in [Wa1] and [Wa2] a "generalized Euler characteristic", $\chi(X)$, which is an element

of $K_0\mathbb{Z}\pi$ and showed that X has the homotopy type of a CW-complex if and only if $\chi(X)$ is an integer.

2. A Summary of this Thesis

Let p be an odd prime. Recall that C_{p^n} denotes the cyclic group of order p^n and that ζ_n is a primitive p^{n+1}th root of unity. The three first of the four papers in this thesis we work on the problem of finding $\operatorname{Pic}\mathbb{Z}C_{p^n}$ and in the last paper we work on Picard groups of some rings which in some sense fits between $\mathbb{Z}C_{p^n}$ and $\mathbb{Z}[\zeta_n]$. As mentioned, calculating Picard groups for these rings is equivalent to calculating K_0 groups. Calculating $K_0\mathbb{Z}G$ for various groups G was mentioned by R.G. Swan at his talk at the International congress of Mathematicians in Nice 1970 as one of the important problems in algebraic K-theory. Of course, the reasons for this is are applications in topology, like the one above. However, calculating $K_0\mathbb{Z}G$ seems to be pretty hard and even to this date there are no general results. Even when we restrict ourselves to $G = C_{p^n}$ no general explicit formulas are known. Several people have worked on this, though. Kervaire and Murthy presented in [K-M] an approach based on the pullback

$$\begin{array}{ccc} \mathbb{Z}C_{p^{n+1}} & \longrightarrow & \mathbb{Z}[\zeta_n] \\ \downarrow & & \downarrow \\ \mathbb{Z}C_{p^n} & \longrightarrow & \mathbb{F}_p[x]/(x^{p^n}-1) =: R_n \end{array} \tag{2.1}$$

which is a variant of 1.2. The $(*, \operatorname{Pic})$-Mayer-Vietoris exact sequence associated to this pullback reads

$$(\mathbb{Z}C_{p^n})^* \times \mathbb{Z}[\zeta_n]^* \xrightarrow{j} R_n^* \to \operatorname{Pic}\mathbb{Z}C_{p^{n+1}} \to \operatorname{Pic}\mathbb{Z}C_{p^n} \times \operatorname{Pic}\mathbb{Z}[\zeta_n] \to \operatorname{Pic} R_n$$

Following Kervaire and Murthy, we observe that Picard groups of local rings are trivial, that the Picard group of a Dedekind ring equals the class group of the same ring and then define V_n as the co-kernel of the map j in the sequence above. Then we get

$$0 \to V_n \to \operatorname{Pic}\mathbb{Z}C_{p^{n+1}} \to \operatorname{Pic}\mathbb{Z}C_{p^n} \times \operatorname{Cl}\mathbb{Z}[\zeta_n] \to 0. \tag{2.2}$$

Kervaire and Murthy set out to calculate V_n and their approach is based on the fact that all rings involved can be acted upon by the Galois group $G_n := \operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. If $s \in G_n$, let $s(\zeta_n) = \zeta_n^{\kappa(s)}$. If we represent the rings in the pullback as residue class rings of polynomials in the indeterminate X, the action is generated by $s(X) = X^{\kappa(s)}$ for all involved rings. G_n becomes a group of automorphisms of $\mathbb{Z}C_{p^{n+1}}$, $\mathbb{Z}C_{p^n}$ and R_n. The maps in the pullback above commutes with the action of G_n and the exact sequence becomes a sequence of G_n-modules. In particular, complex conjugation, which we denote by c, belongs to G_n and

$c(X) = X^{-1}$. When M is a multiplicative G_n-module, like the group of units of one of the rings in the pullback, we let M^+ denote the subgroup of elements $v \in M$ such that $c(v) = v$ and M^- denote the subgroup of elements such that $c(v) = v^{-1}$. V_n is a finite abelian group of odd order and hence we have that $V_n = V_n^+ \times V_n^-$. The main result in Kervaire and Murthy's article is the following theorem

Theorem 2.1 (Kervaire and Murthy)**.**

$$V_n^- \cong \prod_{\nu=1}^{n-1} (\mathbb{Z}/p^\nu\mathbb{Z})^{\frac{(p-1)^2 p^{n-\nu-1}}{2}}$$

and when p is semi-regular, there exists a canonical injection

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

where $\operatorname{Cl}^{(p)} \mathbb{Q}(\zeta_{n-1})$ is the p primary component of the ideal class group of $\mathbb{Q}(\zeta_{n-1})$.

The calculation of V_n^- is straightforward. Finding the information on V_n^+ turns out to be much harder. Kervaire and Murthy instead proves the result above with V_n^+ replaced by the $+$-part of

$$\mathcal{V}_n := \frac{R_n^*}{j(\mathbb{Z}[z_n]^*)},$$

that is, constructs a canonical injection

$$\operatorname{Char} \mathcal{V}_n^+ \to \operatorname{Cl}^{(p)} \mathbb{Q}(\zeta_{n-1}) \tag{2.3}$$

Then, since V_n^+ is a canonical quotient of $\mathcal{V}_n^+$, 2.3 extends to an injection

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

via the canonical injection

$$\operatorname{Char} V_n^+ \to \operatorname{Char} \mathcal{V}_n^+.$$

The injection 2.3 is actually a composition of the Artin map in class field theory and a canonical injection from Iwasawa theory. The actual proof is mainly based on class field theory.

Kervaire and Murthy conjecture that $\operatorname{Char} V_n^+ = \operatorname{Cl}^{(p)} \mathbb{Q}(\zeta_{n-1}) \cong (\mathbb{Z}/p^n\mathbb{Z})^{r(p)}$, where $r(p)$ is the index of regularity of p, that is the number of Bernoulli numbers $B_2, B_4, \ldots, B_{p-3}$ with numerators (in reduced form) divisible by p. They also conjecture that $\mathcal{V}_n^+ = V_n^+$.

When p is a regular prime it is known that $\operatorname{Cl}^{(p)} \mathbb{Q}(\zeta_{n-1})$ is trivial and hence $V_n = V_n^-$ is determined completely in [K-M].

In [U2], Stephen Ullom uses Iwasawa theory and studies the action of $\operatorname{Aut} C_{p^n}$ on $\operatorname{Pic}\mathbb{Z}C_{p^n}$. He proves in that under a certain extra assumption on p, the first of Kervaire and Murthy's conjectures holds exactly when the Iwasawa invariant λ associated to p equals $r(p)$.. More explicitly the assumption is the following.

Assumption 1. *The Iwasawa invariants λ_{1-i} satisfy $1 \leq \lambda_{1-i} \leq p-1$*

We refer you to [I] for notation. S. Ullom proves that if Assumption 1 holds then, for even i,

$$e_i V_n \cong \frac{\mathbb{Z}}{p^n\mathbb{Z}} \oplus (\frac{\mathbb{Z}}{p^{n-1}\mathbb{Z}})^{\lambda_{1-i}-1}. \tag{2.4}$$

This yields, under the same assumption, that

$$V_n^+ \cong (\frac{\mathbb{Z}}{p^n\mathbb{Z}})^{r(p)} \oplus (\frac{\mathbb{Z}}{p^{n-1}\mathbb{Z}})^{\lambda - r(p)}, \tag{2.5}$$

where

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

Hence, when $\lambda = r$ we get the first of Kervaire and Murthy's conjectures. Note however, that if $\lambda > r$ the conjecture is false.

In the papers that make up this thesis we use a different approach.

Instead of directly studying $\mathbb{Z}C_{p^n}$ we study

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

and use Proposition 1.9 which reads $\operatorname{Pic}\mathbb{Z}C_{p^n} \cong \operatorname{Pic} A_n$ Denote $A_n \bmod p \cong \mathbb{F}_p[x]/(x-1)^{p^n-1}$ by D_n. Then, the with $k=0$ and $l=n$ the pullback 1.4 looks like

$$\begin{array}{ccc} A_{n+1} & \xrightarrow{i_n} & \mathbb{Z}[\zeta_n] \\ \downarrow{\scriptstyle j_n} & \swarrow{\scriptstyle N_n} & \downarrow{\scriptstyle f_{k,l}} \\ A_n & \xrightarrow{g_{k,l}} & D_n \end{array} \tag{2.6}$$

The "norm-map" N_n is constructed so that the lower right triangle of the diagram becomes commutative.

From our pullback we get back the exact sequence 2.2 but a different representation of V_n, namely

$$V_n = \frac{D_n^*}{\mathrm{Im}\{A_n^* \times \mathbb{Z}[\zeta_n]^* \to D_n^*\}} = \frac{D_n^*}{\mathrm{Im}\{A_n^* \to D_n^*\}},$$

where the second equality follows from the existence of N_n. Again using N_n we construct an embedding of $\mathbb{Z}[\zeta_{n-1}]^*$ into A_n^*. We consider this an identification and define

$$\mathcal{V}_n := \frac{D_n^*}{\mathrm{Im}\{\mathbb{Z}[\zeta_{n-1}]^* \to D_n^*\}}.$$

It turns out this definition is equivalent to the one in [K-M].

In paper 1, [H1], in this thesis we re-prove Kervaire and Murthy's result in the case when p is regular. The main part of our proof is based on calculation of the orders of certain groups of units in $\mathbb{Z}[\zeta_{n-1}]^*$. Specifically, let

$$U_{n,k} := \{\text{real } \epsilon \in \mathbb{Z}[\zeta_{n-1}]^* \ : \ \epsilon \equiv 1 \bmod (\zeta_n - 1)^k\}.$$

If p is regular, a famous result by Kummer state that if a unit ϵ in $\mathbb{Z}[\zeta_0]^*$ is congruent to a rational integer modulo $(\zeta_0 - 1)^{p-1}$ (that is modulo p) then ϵ is a p-th power of another unit. We prove a generalization of this (Paper 1, Theorem 3.1) stating that if $\epsilon \in \mathbb{Z}[\zeta_0]^*$ is congruent to 1 modulo $(\zeta_n - 1)^{p^{n+1}-1}$, then $\epsilon = \gamma^p$ where γ is a unit congruent to 1 modulo $(\zeta_n - 1)^{p^n+1}$. If we let U^p denote the group of p-th powers of elements in U and define

$$r_n := \Big|\frac{U_{n,p^{n+1}-1}}{U^p_{n,p^n+1}}\Big|,$$

then our generalization of Kummer's Lemma shows that $r_n = 0$ when p is regular which is something we use in our re-proving of Kervaire and Murthy's result.

In Paper 2, [H-S] we work with three different assumptions on the prime p. The first one is Ulloms Assumption 1 above. We also consider

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

and

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

Under Assumption 1 we prove that Kervaire and Murthy's second conjecture, $\mathcal{V}_n^+ = V_n^+$, holds even when conjecture number one does not. Under Assumption 2 we manage to calculate that the structure of $\mathcal{V}_n^+$ is given by

$$\mathcal{V}_n^+ \cong \Big(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\Big)^{r_0} \oplus \Big(\frac{\mathbb{Z}}{p^{n-1}\mathbb{Z}}\Big)^{r_1-r_0} \oplus \ldots \oplus \Big(\frac{\mathbb{Z}}{p\mathbb{Z}}\Big)^{r_{n-1}-r_{n-2}}. \tag{2.7}$$

This result follows from the existence of a surjection $\pi_n : \mathcal{V}_n^+ \to \mathcal{V}_{n-1}^+$ with $\ker \pi_n \cong (\mathbb{Z}/p\mathbb{Z})^{r_{n-1}}$ and an inductive argument. Under Assumption 3 we first prove that this implies $r_n = r(p)$ for all n and then get that $\mathcal{V}_n^+ \cong (\mathbb{Z}/p^n\mathbb{Z})^{r(p)}$. Then we go on to prove by a direct construction that $\mathcal{V}_n^+ = V_n^+$.

In Paper 3, [H-S2], we construct an injection $\alpha_n : \mathcal{V}_{n-1}^+ \to \mathcal{V}_n^+$ using some results from [K-M] and some class field theory. By using our previous surjection π_n together with α_n we manage to prove that the structure of $\mathcal{V}_n^+$ is given by 2.7 for *all* semi-regular primes. This in turn allows us to prove some structure results on unit groups in $\mathbb{Z}[\zeta_n]^*$. We also get a result on class groups. Let for a multiplicative p-group A, $A(p) = \{x \in A \ : \ x^p = 1\}$. Corollary 4.3 in Paper 3 states:

$$\mathrm{Cl}\,\mathbb{Q}(\zeta_{n-1})(p) \cong \mathrm{Char}(\mathcal{V}_n^+/(\mathcal{V}_n^+)^p) \cong (\mathbb{Z}/p\mathbb{Z})^{r_{n-1}}.$$

This result can be considered as a weak version of Kervaire and Murthys conjecture:

$$\mathrm{Cl}^{(p)}\,\mathbb{Q}(\zeta_{n-1}) \cong \mathrm{Char}\,\mathcal{V}_n^+.$$

It also follows that Assumption 2 actually always holds which means that any unramified extension of $K_n := \mathbb{Q}(\zeta_n)$ of degree p is of the form $K_n(\epsilon^{1/p})$, where $\epsilon \equiv 1 \bmod (\zeta_n - 1)^{p^{n+1}-1}$. For big n we also get a slightly stronger statement, see Corollary 4.5 of [H-S2].

Finally, in the last paper [H2] we generalize some of our results from [H-S] to rings

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

which in some sense fit in between $\mathbb{Z}C_p$ and $\mathbb{Z}[\zeta_n]$. For semi-regular primes satisfying Assumption 3 we give an exact sequence

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

and calculate $V_{k,l}^-$ and $V_{k,l}^+$ explicitly.

References

[A-H] Atiyah M. F. and Hirzebruch F., *Vector Bundles and Homogeneous Spaces.* Proc. of Symp. of Pure Math. Soc. 3 (1961).

[B] Bass, H., *Algebraic K-theory* Benjamin, New York, 1968.

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

[BSG] Borel, A. et Serre J.-P., *Le theoreme de Riemann-Roch (d'apres Grothendieck).* Bull. Soc. Math. France 86 (1958), 94-136.

[H1] O. Helenius, *Kummer's Lemma and Picard Groups of Integer Group Rings*
Theme Issue on Commutative Algebra, Arabian Journal of Science and Engineering Volume 26 (2001), Number 1C, 107-118.

[H2] O. Helenius, *On the Picard Group of some Polynomial Rings*
Preprint 2001:74, Chalmers University of Technology, 2001.

[Hig] Higman, G., *The units of group rings*
Proc. London Math. Soc. 46 (1940), 231-248.

[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 2001:72, 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.

[L] Lang, Serge, *Algebra, Third Edition*
Addison-Wesley, 1993.

[M] Milnor, J., *Introduction to Algebraic K-Theory*
Annals of Math. Studies 72, Princeton University Press 1971.

[R] Rotman, Joseph J., *An Introduction to Homological Algebra*
Academic Press, 1979.

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

[Si] Silvester, John R., *Introduction to Algebraic K-Theory*
Chapman and Hall, 1981.

[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.

[Wa1] Wall, C.T.C., *Finiteness conditions for CW-complexes I*,
Annals of Math. 81 (1965), 56-59.

[Wa2] Wall, C.T.C., *Finiteness conditions for CW-complexes II*,
Proc. Royal Soc. A 295 (1966), 129-139.

[Wh] Whitehead, J.H.C., *Simplicial Spaces, Nuclei and m-groups*
Proc. London Math. Soc. 45 (1939), 243-327

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

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

KUMMER'S LEMMA AND PICARD GROUPS OF INTEGER GROUP RINGS

OLA HELENIUS

ABSTRACT. In this paper we reprove a result by Kervaire and Murthy concerning Picard groups of integer group rings $\mathbb{Z}C$, where C is a cyclic group of prime power order. Our method is more elementary than the one used by Kervaire and Murthy and relies on the construction of certain multiplicative maps by Stolin and on a generalization of Kummer's Lemma on units in cyclotomic fields presented here.

1. INTRODUCTION

For $n = 1, 2, \ldots$, 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. In [K-M], Kervaire and Murthy proved the following theorem.

Theorem 1.1. *Let p be a regular prime and let $n \geq 2$. There is an exact sequence*

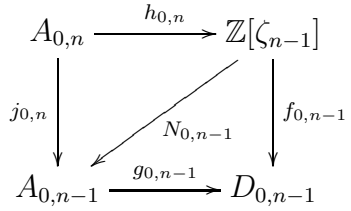
$$0 \to \prod_{j=1}^{n-1} C_{p^j}^{k_j} \to \operatorname{Pic} \mathbb{Z}C_{p^n} \to \operatorname{Cl} \mathbb{Z}[\zeta_{n-1}] \oplus \operatorname{Pic} \mathbb{Z}C_{p^{n-1}} \to 0,$$

where $k_j = \frac{(p-1)^2 p^{n-j-2}}{2}$ for $1 \leq j \leq n-2$ and $k_{n-1} = \frac{p-3}{2}$.

The sequence is a slight variation of a Mayer-Vietoris sequence associated with a certain cartesian square of rings. The hard part of the proof is finding out the structure of the first non-zero term which is a cokernel of a map between unit groups of rings involved in the cartesian square. Kervaire and Murthy's proof relies on Iwasawa theory and the aim of this paper is to give a more elementary proof. Our proof relies mainly on a construction of certain multiplicative maps (see section 2) and a generalization of Kummer's lemma on units in cyclotomic fields to the prime power case (see section 3).

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

As a starting point for our proof of Theorem 1.1 we will use the following pullback diagram (or Cartesian square)



where

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

and the class of x is denoted by $x_{k,i}$,

$$D_{k,i} := \frac{A_{k,i}}{(p)} \cong \frac{\mathbb{F}_p[x]}{(x-1)^{p^{k+i}-p^k}},$$

$j_{k,i}(x_{k,i}) = x_{k,i-1}$, $h_{k,i}(x_{k,i}) = \zeta_{k+i-1}$, $f_{k,i-1}(\zeta_{k+i-1}) = \bar{x}$ and $g_{k,i-1}$ is the natural surjection. The maps $N_{k,i}$, that are constructed in section 2, are multiplicative and such that the lower triangle of the diagram commutes. The pullback diagram gives us a Mayer-Vietoris sequence

$$\begin{aligned}(1.1)\quad \mathbb{Z}[\zeta_{n-1}]^* \oplus A_{0,n-1}^* \xrightarrow{\beta} D_{0,n-1}^* \to \operatorname{Pic} A_{0,n} \to \\ \to \operatorname{Pic}\mathbb{Z}[\zeta_{n-1}] \oplus \operatorname{Pic} A_{0,n-1} \to \operatorname{Pic} D_{0,n-1}.\end{aligned}$$

This sequence can be used as a starting point for finding the sequence involving $\operatorname{Pic}\mathbb{Z}C_{p^n}$ since, by a generalization of Rim's theorem, $\operatorname{Pic}\mathbb{Z}C_{p^n} \cong \operatorname{Pic} A_{0,n}$ for each $n \geq 1$ (see [R] and [S1]). From the sequence 1.1 we get

$$0 \to \frac{D_{0,n-1}^*}{\beta(\mathbb{Z}[\zeta_{n-1}]^* \oplus A_{0,n-1}^*)} \to \operatorname{Pic} A_{0,n} \to \operatorname{Cl}\mathbb{Z}[\zeta_{n-1}] \oplus \operatorname{Pic} A_{0,n-1} \to 0.$$

The proof of the main theorem thus boils down to finding the structure of $D_{0,n-1}^*/\beta(\mathbb{Z}[\zeta_{n-1}]^* \oplus A_{0,n-1}^*)$. We will indicate how this is done in this introduction and leave the details to section 4.

Step 1: By viewing $D_{0,n-1}$ as the ring consisting of elements $a_0 + a_1(\bar{x}-1) + \ldots + a_{p^{n-1}-2}(\bar{x}-1)^{p^{n-1}-2}$, $a_i \in \mathbb{F}_p$, we see that $|D_{0,n-1}| = p^{p^{n-1}-1}$. Every element with $a_0 = 0$ is nilpotent so we get that every element with $a_0 \neq 0$ is a unit and that $|D_{0,n-1}^*| = (p-1)p^{p^{n-1}-2}$. Clearly, $\mathbb{F}_p^* \subset D_{0,n-1}^*$ and by the structure theorem for abelian groups, $D_{0,n-1}^* = \mathbb{F}_p^* \oplus \tilde{D}_{0,n-1}^*$ where $\tilde{D}_{0,n-1}^*$ is a p-group.

Let c denote the map $\bar{x} \mapsto \bar{x}^{-1}$ in $\tilde{D}_{0,n-1}^*$ and define

$$\tilde{D}_{0,n-1}^{*+} := \{u \in \tilde{D}_{0,n-1}^* \,:\, c(u) = u\}$$

and

$$\tilde{D}^{*-}_{0,n-1} := \{u \in \tilde{D}^{*}_{0,n-1} \,:\, c(u) = u^{-1}\}.$$

Since $\tilde{D}^{*}_{0,n-1}$ is an finite abelian group of odd order and since c has order 2 we get

$$D^{*}_{0,n-1} \cong \mathbb{F}^{*}_{p} \oplus \tilde{D}^{*+}_{0,n-1} \oplus \tilde{D}^{*-}_{0,n-1}.$$

Step 2: In Lemma 4.1 in section 4 we show that $\beta(\mathbb{Z}[\zeta_{n-1}]^{*} \oplus A^{*}_{0,n-1}) = \beta(A^{*}_{0,n-1}) = g_{0,n-1}(A^{*}_{0,n-1})$. Moreover, Lemma 4.2 tells us that

$$g_{0,n-1}(A^{*}_{0,n-1}) \subseteq \mathbb{F}^{*}_{p} \oplus \tilde{D}^{*+}_{0,n-1} \oplus < \bar{x} >, \tag{1.2}$$

where $< \bar{x} > \cong C_{p^{n-1}}$ is the subgroup of $\tilde{D}^{*-}_{0,n-1}$ generated by $\bar{x}$.

Step 3: We want to show that we have equality in Equation 1.2. By elementary direct methods one can show that $g_{0,n-1}(A^{*}_{0,n-1}) \supset \mathbb{F}^{*}_{p} \oplus < \bar{x} >$. Clearly, $g_{0,n-1}(x_{0,n-1}) = \bar{x}$ and a direct calculation shows that if $\bar{k}$ is the class of k in $\mathbb{F}^{*}_{p}$, then $g_{0,n-1}$ maps $(x^{k}_{0,n-1} - 1)/(x_{0,n-1} - 1)$ on $\bar{k}$. The hard part is to show that $\tilde{D}^{*+}_{0,n-1}$ is also contained in $g_{0,n-1}(A^{*}_{0,n-1})$. To do this we show that $\mathbb{Z}[\zeta_{n-2}]$ can be embedded in $A_{0,n-1}$ and that if we consider this as an identification we actually have $g_{0,n-1}(\mathbb{Z}[\zeta_{n-2}]) \supseteq \tilde{D}^{*+}_{0,n-1}$. This is done in Theorem 4.4. In short, it is proved by finding a subgroup of real elements of $\mathbb{Z}[\zeta_{n-2}]$ that maps onto $\tilde{D}^{*+}_{0,n-1}$. We prove this by just counting elements in the image of the subgroup but it turns out that this is fairly tricky and we use both the generalization of Kummer's Lemma exposed in section 3 and some classical number theoretical techniques.

As a result, we get

$$\frac{D^{*}_{0,n-1}}{\beta(\mathbb{Z}[\zeta_{n-1}]^{*} \oplus A^{*}_{0,n-1})} \cong \frac{\tilde{D}^{*-}_{0,n-1}}{< \bar{x} >}$$

Step 4: To finish of the proof of our main theorem we now only need to find the structure of the p-group $\tilde{D}^{*-}_{0,n-1}$. This is done in Proposition 4.3 by an elementary calculation. The result is $\tilde{D}^{*-}_{0,n-1} \cong \prod_{j=1}^{n-1} C^{s_j}_{p^j}$ where $s_j = \frac{(p-1)^2 p^{n-j-2}}{2}$ for $1 \leq j \leq n-2$ and $s_{n-1} = \frac{p-1}{2}$.[1] Since $< \bar{x} > \cong C_{p^{n-1}}$, we get

$$\frac{D^{*}_{0,n-1}}{\beta(\mathbb{Z}[\zeta_{n-1}]^{*} \oplus A^{*}_{0,n-1})} \cong \prod_{j=1}^{n-1} C^{k_j}_{p^j},$$

where k_j are given in Theorem 1.1 and this completes the proof.

[1] If $n = 2$ we get $\tilde{D}^{*-}_{0,1} \cong C_{p}^{\frac{p-1}{2}}$.

2. Norm Maps

In this section, we construct certain multiplicative maps. The maps were first constructed by Stolin, see for example [S3], but since the construction may not be well known we repeat it here.

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

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

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

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

We want to prove the following result.

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

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

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

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

The maps $N_{k,i}$ will be constructed inductively. If $i = 1$ and k is arbitrary, we have $A_{k,1} \cong \mathbb{Z}[\zeta_k]$ and we define $N_{k,1}$ as the usual norm map $\tilde{N}_{k+1,1}$. Since $\tilde{N}_{k+1,1}(\zeta_{k+1}) = \zeta_k$ we only need to prove that our map is additive modulo p, which follows from the lemma below.

Lemma 2.2. *For $k \geq 0$ and $i \geq 1$ we have*

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

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 [S2] and proofs can be found there.

Now suppose $N_{k,j}$ is constructed for all k and all $j \leq i-1$. Let $\varphi = \varphi_{k+1,i} : \mathbb{Z}[\zeta_{k+i}] \to A_{k+1,i}$ be defined by $\varphi(a) = (a, N_{k+1,i-1}(a))$. It is clear that φ is multiplicative. From the lemma above we have a norm map $N : A_{k+1,i} \to A_{k,i}$. Define $N_{k,i} := N \circ \varphi$. It is clear that $N_{k,i}$ is multiplicative. Moreover, $N_{k,i}(\zeta_{k+i}) = N(\zeta_{k+i}, x_{k+1,i-1}) = N(x_{k+1,i}) = x_{k,i}$, where the latter equality follows by a direct computation. To prove that our map makes the diagram in the proposition above commute, we now only need to prove it is additive modulo p. This also follows by a direct calculation once you notice that

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

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

Regarding the other two equalities in proposition 2.1, it is clear that the second one follows from the first. The first statement will follow from the lemma below.

Lemma 2.3. *The diagram*

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

is commutative

Proof. Recall that the maps denoted N (without subscript) are the usual norms defined by the determinant of the multiplication map. An element in $A_{k,i}$ can be represented as a pair $(a,b) \in \mathbb{Z}[\zeta_{k+i-1}] \times A_{k,i-1}$ and an element in $A_{k-1,i}$ can be represented as a pair $(c,d) \in \mathbb{Z}[\zeta_{k+i-2}] \times A_{k-1,i-1}$. If (a,b) represents an element in $A_{k,i}$ one can, directly from the definition, show that $N(a,b) = (N(a), N(b)) \in A_{k-1,i}$.

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

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

and

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

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

3. Kummer's Lemma

Let λ_n be the ideal $(\zeta_n - 1)$ in $\mathbb{Z}[\zeta_n]$. Here we will prove a generalization of the theorem by Kummer that states that if a p is a regular prime and ϵ is a unit in $\mathbb{Z}[\zeta_0]$, congruent to 1 modulo p, then ϵ is a p-th power of a unit.

Theorem 3.1. *Let p be a regular prime. Let $\epsilon \in \mathbb{Z}[\zeta_n]^*$ and suppose $\epsilon \equiv 1 \mod \lambda_n^{p^{n+1}-1}$. Then $\epsilon = \gamma^p$ for some unit $\gamma \in \mathbb{Z}[\zeta_n]^*$.*

The proof can be broken down into four lemmas. Before we state them we need some notation. If R is the ring of integers of a number field K and λ a prime, we let K_λ denote the completion of K at λ and R_λ the valuation ring. By abuse of notation we let λ denote the (unique) maximal ideal of the local ring R_λ.

Lemma 3.2. *Let $\epsilon \in \mathbb{Z}[\zeta_n]^*$ and suppose that $\epsilon \equiv 1 \mod \lambda_n^{p^{n+1}-1}$. Then $\epsilon \equiv 1 \mod \lambda_n^{p^{n+1}}$.*

Lemma 3.3. *Let p be an odd prime. Let $\epsilon \in \mathbb{Z}[\zeta_n]^*$ and suppose that $\epsilon \equiv 1 \mod \lambda_n^{p^{n+1}}$. Then $\epsilon \equiv 1 \mod \lambda_n^{p^{n+1}+1}$.*

Lemma 3.4. *Let ϵ be a unit in $(\mathbb{Z}[\zeta_n])_{\lambda_n}$ with $\epsilon \equiv 1 \mod \lambda_n^{p^{n+1}+1}$, then there exists a unit γ in $(\mathbb{Z}[\zeta_n])_{\lambda_n}$ such that $\epsilon = \gamma^p$. Moreover, $\gamma \equiv 1 \mod \lambda_n^{p^n+1}$.*

Lemma 3.5. *Let p be a regular prime. If $\epsilon \in \mathbb{Z}[\zeta_n]^*$ and $\sqrt[p]{\epsilon} \in (\mathbb{Z}[\zeta_n])_{\lambda_n}$, then $\sqrt[p]{\epsilon} \in \mathbb{Z}[\zeta_n]$.*

It is clear that Theorem 3.1 follows.

The rest of this section is devoted to the proofs of the four lemmas. The last three are simple generalizations of the corresponding results for $n = 0$. Lemma 3.2 is a bit harder and is due to Stolin. His result, which is a bit more general, can be found in [S1]. We give a similar proof here, but in slightly more detail. For this we need to develop some notation and we leave this to the end of the section. We prove the remaining three lemmas first.

Proof of Lemma 3.3. By a well known result by Kummer, $\epsilon = \epsilon_r \zeta_n^k$ for some real unit ϵ_r and some $k \in \mathbb{Z}$. Since $\zeta_n^k = (1 + (\zeta_n - 1))^k \equiv 1 + k(\zeta_n - 1) \mod \lambda_n^2$ and $\epsilon_r \equiv a \mod \lambda_n^2$ for some $a \in \mathbb{Z}$ and since $\epsilon_r \zeta_n^k = \epsilon \equiv 1 \mod \lambda_n^2$, we get that λ_n divides k and hence that p

divides k and $k = pk_1$ for some $k_1 \in \mathbb{Z}$. It is easy to see that $\bar{\epsilon}^{-1} \equiv 1 \mod \lambda_n^{p^{n+1}}$ and this shows that $\zeta_n^{2k} = \epsilon\bar{\epsilon}^{-1} \equiv 1 \mod \lambda_n^{p^{n+1}}$. This in turn means that $p|\zeta_n^{2k}-1 = \zeta_{n-1}^{2k_1}-1$ in $\mathbb{Z}[\zeta_n]$. But then, $(\zeta_{n-1}^{2k_1}-1)/p \in \mathbb{Z}[\zeta_{n-1}]$ and we get that $\lambda_{n-1}^{p^n-p^{n-1}} = p \,|\, \zeta_n^{2k} - 1 = \zeta_{n-1}^{2k_1} - 1$ in $\mathbb{Z}[\zeta_{n-1}]$. Since $p^n - p^{n-1} \geq 2$ this implies $\lambda_{n-1}|(\zeta_{n-1}^{2k_1-1}+\ldots+\zeta_{n-1}+1) \equiv 2k_1 \mod \lambda_{n-1}$ so $\lambda_{n-1}|2k_1$ and hence we get that $p|k_1$ and $p^2|k$. This argument can be repeated in $\mathbb{Z}[\zeta_{n-2}]$ to show that $p^3|k$ and so on until we, from a similar argument in $\mathbb{Z}[\zeta_0]$ get that $p^{n+1}|k$. But this means that $\epsilon = \epsilon_r\zeta^k = \epsilon_r$ so ϵ is real. Since $(\zeta_n - \zeta_n^{-1}) = \lambda_n$ as ideals, $\epsilon \equiv 1 \mod (\zeta_n - \zeta_n^{-1})^{p^{n+1}}$. By representing ϵ in the basis $(\zeta_n - \zeta_n^{-1})^i$, $i = 0, 1, 2, \ldots, p^n(p-1)-1$ and observing that all coefficients with odd index must be zero we get the desired result. □

We leave out the proof of Lemma 3.4 since it is just a simple generalization of the corresponding result for $n = 0$ (see for example the proof of Theorem 5.36, p. 79 [W]).

Proof of Lemma 3.5. Let ω be a prime in $\mathbb{Q}(\zeta_n)$ that ramifies in $\mathbb{Q}(\zeta_n, \sqrt[p]{\epsilon})$. Since all archimedian primes are complex, they do not ramify so ω is not archimedian. Then ω divides the discriminant $\Delta(S/\mathbb{Z}[\zeta_n])$ where S is the ring of integers in $\mathbb{Q}(\zeta_n, \sqrt[p]{\epsilon})$. Let $N = N_{\mathbb{Q}(\zeta_n, \sqrt[p]{\epsilon})/\mathbb{Q}(\zeta_n)}$ denote the relative norm and let f be the minimal polynomial $x^p - \epsilon$. It is well known that $\Delta(S/\mathbb{Z}[\zeta_n])|N(f'(\sqrt[p]{\epsilon})$ (see for example [J], p. 39). But $N(f'(\sqrt[p]{\epsilon})) = N(p\epsilon^{(p-1)/p}) = up^p = u\lambda^{p^{n+1}(p-1)}$ for some unit u, so $\omega = \lambda_n$. Assume that ϵ is not a p-th power. Then, since $\mathbb{Q}(\zeta_n, \sqrt[p]{\epsilon})$ is the splitting field of $f(x) = x^p - \epsilon$, $\mathbb{Q}(\zeta_n, \sqrt[p]{\epsilon}) \supseteq \mathbb{Q}(\zeta_n)$ is an abelian extension of degree p . By assumption, $(\mathbb{Q}(\zeta_n))_{\lambda_n} = (\mathbb{Q}(\zeta_n))_{\lambda_n}(\sqrt[p]{\epsilon})$ so λ_n trivially does not ramify in $(\mathbb{Q}(\zeta_n))_{\lambda_n}(\sqrt[p]{\epsilon})$ and hence λ_n does not ramify in $\mathbb{Q}(\zeta_n, \sqrt[p]{\epsilon})$ either so $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_n, \sqrt[p]{\epsilon})$ is an unramified abelian extension of degree p. $\mathbb{Q}(\zeta_n, \sqrt[p]{\epsilon})$ is thus a subfield of the Hilbert class field $\mathbb{H}$ of $\mathbb{Q}(\zeta_n)$ and since $[\mathbb{H} : \mathbb{Q}(\zeta_n)] = h_{\mathbb{Q}(\zeta_n)}$ we get that $p|h_{\mathbb{Q}(\zeta_n)}$. But this is a contradiction since p is regular and since $p|h_{\mathbb{Q}(\zeta_n)}$ implies $p|h_{\mathbb{Q}(\zeta_0)}$ by Theorem 10.4 (a), p. 187, [W]. □

The rest of this section is devoted to the norm residue symbol and the proof of Lemma 3.2. Let $K = \mathbb{Q}(\zeta_n)$. If w is a valuation on K and $a \in K^*$, we have a local Artin map

$$\Psi_w : K_w^* \longrightarrow Gal(K_w(\sqrt[p]{a})/K_w).$$

For $a \in K^*$, we will denote the action of $\Psi_w(b)$ on a by $a^{\Psi_w(b)}$. We define the norm residue symbol

$$(\ ,\ )_w : K_w^* \times K_w^* \longrightarrow \mu_p,$$

where μ_p is the group of p-th roots of unity, by $(a, b)_w = (\sqrt[p]{a})^{\Psi_w(b)}(\sqrt[p]{a})^{-1}$.

Lemma 3.6. *Let $a, b \in K_w^*$ and let $N = N_{K_w(\sqrt[p]{a})/K_w}$. Then,*

i) $(a,b)_w = 1$ *if and only if* $b \in N(K_w(\sqrt[p]{a})^*)$
ii) $(a,b)_w = 1$ *if* $a + b \in (K_w)^p$
iii) $\prod_w (a,b)_w = 1$, *where the product is taken over all valuations of* K.

Proof. *i)*: This follows immediately by the well known fact that $\Psi_w(b)$ is the identity map if and only if b is a local norm.

ii): If F is any field that contains the p-th roots of unity, $y \in F^*$ and $x \in F$, then the element $x^p - y$ is a norm from $F(\sqrt[p]{y})$ since if ζ is a fixed primitive p-th root of unity, then

$$x^p - y = \prod_{k=0}^{p-1} (x - \zeta^k \sqrt[p]{y}) = N_{F(\sqrt[p]{a})/F}(x - \sqrt[p]{y}).$$

This fact applied to $F = (\mathbb{Q}(\zeta_n))_{\lambda_n}$, $y = a$ and $x^p = a + b$ shows that b is a local norm and hence, by *i)* that $(a,b)_w = 1$.

iii): It is well known that b is a local norm for almost all valuations. By *i)*, the product can be considered finite, taken over the set S consisting of valuations where b is not a local norm and valuations where the extension $K_w(\sqrt[p]{a})/K_w$ is unramified. Since $\Psi_w(b)$ is the identity if $w \notin S$ and since $\prod_w \Psi_w(b) = 1$ we get that $\prod_{w \in S} \Psi_w(b) = 1$ and the result follows.

□

Now fix n and let $\lambda = \lambda_n$. Let for $i = 1, 2, \ldots$, $\eta_i = 1 - \lambda^i$.

Lemma 3.7. *Let w be a valuation of K. Then,*

i) $(\eta_i, \eta_j)_w = (\eta_i, \eta_{i+j})_w (\eta_{i+j}, \eta_j)_w (\lambda^j, \eta_{i+j})_w$
ii) If $w = \lambda$ *and* $i + j > p^{n+1}$ *then* $(\eta_i, \eta_j)_w = 1$
iii) If $w = \lambda$, $i + j = p^{n+1}$ *and* $1 \le i \le p-1$, *then* $(\eta_i, \eta_j)_w \neq 1$.

Proof. *i)*: Since p is odd, $(a,-1)_w = 1$ and by Lemma 3.6 *ii)*, $(a,-a)_w = 1 = (a, 1-a)_w$ for all $a \in K^*$. It is easy to see that $(\ ,\ )_w$ is (multiplicatively) bilinear so $(a,-b)_w = (a,-1)_w (a,b)_w = (a,b)_w$ for all $a, b \in K^*$. Hence $(a,a)_w = (a,-a)_w = 1$ and by applying the latter equality to $(ab, -ab)_w$ we get that $(a,b)_w (b,a)_w = 1$ Since $\eta_j + \lambda^j \eta_i = \eta_{i+j}$, we get $\frac{\eta_j}{\eta_{i+j}} + \frac{\lambda^j \eta_i}{\eta_{i+j}} = 1$ and hence by Lemma 3.6 *ii)* that

$$1 = \Big(\frac{\eta_j}{\eta_{i+j}}, \frac{\lambda^j \eta_i}{\eta_{i+j}} \Big)_w$$

and *i)* follows by a straightforward calculation, using the above identities.

ii): Suppose $i+j > p^{n+1}$. Then $\eta_{i+j} \equiv 1 \mod \lambda_n^{p^{n+1}+1}$. By Lemma 3.4 any such element is a p-th power and hence a norm in any extension $K_\lambda(\sqrt[p]{\eta_k})/K_\lambda$. By *i*),

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

If on the other hand $i+j = p^{n+1}$ and $1 \leq i \leq p-1$, then $i+j+i > p^{n+1}$ and $i+j+j > p^{n+1}$, so

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

by Lemma 3.6 since λ^i cannot be a norm in the extension $K_\lambda(\sqrt[p]{\eta_{p^{n+1}}})/K_\lambda$. □

Now, put $R = \mathbb{Z}[\zeta_n]$ and for $k = 1, 2, \ldots$, let $U_k = \{u \in R_\lambda^* : u \equiv 1 \mod \lambda^k\}$. Then (the image of) η_k generates the group U_k/U_{k+1} of order p. This means that if $u \in U_k \setminus U_{k+1}$ there exists i such that $(i,p) = 1$ and $u^i\eta_k^{-1} = t \in U_{k+1}$.

Proof of Lemma 3.2. Let ϵ satisfy the conditions of the lemma. Let $v = v_{\lambda_n}$ be the valuation of $K = \mathbb{Q}(\zeta_n)$ with respect to the prime λ_n and let w be a valuation not equal to v. From for example the proof of Lemma 3.5, we know that the extension $K_w(\sqrt[p]{u})/K_w$ is unramified for every unit $u \in \mathbb{Z}[\zeta_n]$, so ϵ is a norm in every such extension. By 3.6 *i*), $(u, \epsilon)_w = 1$ and then, by 3.6 *iii*), $(u, \epsilon)_v = 1$.
Now let $u = \eta_1$. By the assumptions $\epsilon \in U_{p^{n+1}-1}$. Suppose $\epsilon \notin U_{p^{n+1}}$. Choose i such that $(i,p) = 1$ and $\epsilon^i\eta_{p^{n+1}-1}^{-1} = t \in U_{p^{n+1}}$ and in a similar way j such that $t^j\eta_{p^{n+1}}^{-1} = s \in U_{p^{n+1}+1}$. Then by Lemma 3.4 and 3.7 we have $(u, s)_v = (u, \eta_{p^{n+1}})_v = 1$. All this implies

$$(u, \epsilon)_v^{ij} = (u, \eta_{p^{n+1}-1}t)_v^j = (u, \eta_{p^{n+1}-1})_v^j \neq 1.$$

Hence $(u, \epsilon)_v \neq 1$ which is a contradiction by the first part of the proof. Hence $\epsilon \in U_{p^{n+1}}$ and this finishes the proof. □

4. Proof of the Main Theorem

In this section we state and prove the results we needed to prove the main theorem of this paper.

Lemma 4.1. $\beta(\mathbb{Z}[\zeta_{n-1}]^* \oplus A_{0,n-1}^*) = g_{0,n-1}(A_{0,n-1}^*)$.

Proof. Recall that $\beta(a,b) = f_{0,n-1}(a)g_{0,n-1}(b)^{-1}$. By setting $k = 0$ and $i = n-1$ in the commutative diagram from Proposition 2.1 and using the fact that the norm map maps units to units we get

$$f_{0,n-1}(\mathbb{Z}[\zeta_{n-1}]^*) \subseteq g_{0,n-1}(N_{0,n-1}(\mathbb{Z}[\zeta_{n-1}]^*)) \subseteq g_{0,n-1}(A_{0,n-1}^*)$$

□

Lemma 4.2. $g_{0,n-1}(A^*_{0,n-1}) \subseteq \mathbb{F}_p^* \oplus \tilde{D}^{*+}_{0,n-1} \oplus < \bar{x} >$.

Let $c : A^*_{k,i} \to A^*_{k,i}$ be the map defined by $x_{k,i} \mapsto x^{-1}_{k,i}$. In $\mathbb{Z}[\zeta_k]$ we also denote complex conjugation by c. An element invariant under c will be called real. If $\epsilon \in \mathbb{Z}[\zeta_k]$, a famous result by Kummer tells us that there exists $i \in \mathbb{Z}$ and a real unit ϵ_r such that $\epsilon = \zeta_k^i \epsilon_r$. This result can be generalized to the rings $A_{0,i}$, where it can be used to prove the lemma. Since the proof is almost identical to the proof of Lemma 3.2 in [K-M], which is the corresponding result for $\mathbb{Z}C_{p^n}$, we refrain from repeating it here..

Proposition 4.3. $|\tilde{D}^{*+}_{0,n-1}| = p^{\frac{p^{n-1}-3}{2}}$, $|\tilde{D}^{*-}_{0,n-1}| = p^{\frac{p^{n-1}-1}{2}}$ *and*

$$\tilde{D}^{*-}_{0,n-1} \cong \prod_{j=1}^{n-1} C_{p^j}^{s_j}$$

where $s_j = \frac{(p-1)^2 p^{n-j-2}}{2}$ *for* $1 \leq j \leq n-2$ *and* $s_{n-1} = \frac{p-1}{2}$.[2]

Proof. $\tilde{D}^*_{0,n-1}$ can be presented as $\{1 + a_1(x - x^{-1}) + \ldots + a_{p^{n-1}-2}(x - x^{-1})^{p^{n-1}-2}\}$. Since $c((x - x^{-1})^j) = (-1)^j (x - x^{-1})^j$ it is not hard to see that $\tilde{D}^{*-}_{0,n-1}$ can be represented as $\{1 + a_1(x - x^{-1}) + a_3(x - x^{-1})^3 + \ldots + a_{p^{n-1}-2}(x - x^{-1})^{p^{n-1}-2}\}$. Hence $|\tilde{D}^{*-}_{0,n-1}| = p^{\frac{p^{n-1}-1}{2}}$ and since $|\tilde{D}^*_{0,n-1}| = p^{p^{n-1}-2}$ we get $|\tilde{D}^{*+}_{0,n-1}| = p^{\frac{p^{n-1}-3}{2}}$. Since $\tilde{D}^{*-}_{0,n-1}$ is a p-group it is isomorphic to a product of copies of cyclic groups of prime power order. By using the above presentation, taking p^k-th powers and counting the number of elements of different orders we get a system of equations that gives us the s_j in the lemma. □

The rest of this paper is devoted to proving that

$$g_{0,n-1}(A^*_{0,n-1}) \supset \tilde{D}^{*+}_{0,n-1} \tag{4.1}$$

For each $k \geq 0$ and $i \geq 1$ let $\varphi_{k,i} : \mathbb{Z}[\zeta_{k+i-1}]^* \to A^*_{k,i}$ be the injective group homomorphism defined by $\epsilon \mapsto (\epsilon, N_{k,i}(e))$. By Proposition 2.1, $\varphi_{k,i}$ is well defined. In what follows, we identify $\mathbb{Z}[\zeta_{k+i-1}]^*$ with its image in $A^*_{k,i}$.

Let $\mathbb{Z}[\zeta_{n-2}]^{*+}$ be the subgroup of real units of $\mathbb{Z}[\zeta_{n-2}]^*$. To show that Equation 4.1 holds it is obviously enough to prove the following result

Theorem 4.4. *Let p be a regular prime. Then, $g_{0,n-1}(\mathbb{Z}[\zeta_{n-2}]^{*+}) \supset \tilde{D}^{*+}_{0,n-1}$.*

[2] If $n = 2$ we get $\tilde{D}^{*-}_{0,1} \cong C_p^{\frac{p-1}{2}}$.

The proof will rely on the following lemma which is Theorem I.2.7 in [S3].

Lemma 4.5. $\ker(g_{k,i}|_{\mathbb{Z}[\zeta_{k+i-1}]^*}) = \{\epsilon \in Z[\zeta_{k+i-1}]^* : \epsilon \equiv 1 \mod \lambda_{k+i-1}^{p^{k+i}-p^k}\}$

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

If for example $i = 2$, we get after just one step $a \equiv 1 \mod p$ in $\mathbb{Z}[\zeta_{k+1}]$, $N(a) \equiv 1 \mod p$ and $N(\frac{a-1}{p}) \equiv \frac{N(a)-1}{p} \mod p$ in $A_{k,1} \cong \mathbb{Z}[\zeta_k]$, where N is the usual norm. By viewing N as a product of automorphisms, recalling that N is additive modulo p and that the usual trace of any element of $\mathbb{Z}[\zeta_{k+1}]$ is divisible by p one gets that $N(a) \equiv 1 \mod p^2$ and hence that $N(\frac{a-1}{p}) \equiv 0 \mod p$. By analysing how the norm acts one can show that this means that $a \equiv 1 \mod \lambda_k^{p^{k+2}-p^k}$

Proof of Theorem 4.4. For $m = 1, 2, \ldots$, define

$$U_m := \{\epsilon \in \mathbb{Z}[\zeta_{n-2}]^* : \epsilon \equiv 1 \mod \lambda_{n-2}^m\}.$$

It is clear that $U_1 \supseteq U_2 \supseteq \ldots$ and that $U_1 = \mathbb{Z}[\zeta_{n-2}]^*$. Let U_1^+ be the subgroup of real units in U_1. Since $g_{0,n-1}$ commutes with complex conjugation we have $g_{0,n-1}(U_1^+) \subseteq \tilde{D}_{0,n-1}^{*+}$ and to prove the theorem it is obviously enough to show that this is actually an equality. We will prove this by induction on n. First, by Lemma 4.5, we have for any $n \geq 2$

$$g_{0,n-1}(U_1^+) \cong \frac{U_1^+}{U_{p^{n-1}-1}^+}.$$

Since $g_{0,n-1}(U_1^+) \subseteq g_{0,n-1}(\mathbb{Z}[\zeta_{n-2}]^{*+}) \subseteq \tilde{D}_{0,n-1}^{*+}$ the group $\frac{U_1^+}{U_{p^{n-1}-1}^+}$ is finite. Similarly $\frac{\mathbb{Z}[\zeta_{n-2}]^{*+}}{U_{p^{n-1}-1}^+}$ is finite. This shows that $\big|\frac{\mathbb{Z}[\zeta_{n-2}]^{*+}}{U_1^+}\big|$ is finite since

$$\big|\frac{\mathbb{Z}[\zeta_{n-2}]^{*+}}{U_1^+}\big|\big|\frac{U_1^+}{U_{p^{n-1}-1}^+}\big| = \big|\frac{\mathbb{Z}[\zeta_{n-2}]^{*+}}{U_{p^{n-1}-1}^+}\big|.$$

If $n = 2$, this and Dirichlet's theorem on units tells us that both U_1^+ and $U^+_{p^{n-1}-1} = U^+_{p-1}$ are isomorphic to $\mathbb{Z}^{\frac{p-3}{2}}$. By the classical version of Kummer's lemma we get $U^+_{p-1} = (U_1^+)^p$. Hence

$$\frac{U_1^+}{U^+_{p-1}} \cong \frac{\mathbb{Z}^{\frac{p-3}{2}}}{(p\mathbb{Z})^{\frac{p-3}{2}}} \cong C_p^{\frac{p-3}{2}}.$$

This shows that

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

so we have proved our statement for $n = 2$.

Now fix $n > 2$ and assume the statement of the theorem holds with n replaced by $n - 1$. We can write

$$\Big|\frac{U_1^+}{U^+_{p^{n-1}-1}}\Big| = \Big|\frac{U_1^+}{U^+_{p^{n-2}-1}}\Big|\Big|\frac{U^+_{p^{n-2}-1}}{U^+_{p^{n-2}+1}}\Big|\Big|\frac{U^+_{p^{n-2}+1}}{U^+_{p^{n-1}-1}}\Big| \tag{4.2}$$

By Dirichlet's theorem on units we have $(\mathbb{Z}[\zeta_{n-2}]^*)^+ \cong \mathbb{Z}^{\frac{p^{n-1}-p^{n-2}}{2}-1}$ Since all quotient groups involved are finite we get that U_1^+, $U^+_{p^{n-1}-1}$, $U^+_{p^{n-2}-1}$ and $U^+_{p^{n-2}+1}$ are all isomorphic to $\mathbb{Z}^{\frac{p^{n-1}-p^{n-2}}{2}-1}$. The rest of the proof is devoted to the analysis of the three right hand factors of 4.2.

By Theorem 3.1, Kummer's Lemma in the prime power case, we have $U^+_{p^{n-1}-1} = (U^+_{p^{n-2}+1})^p$ so

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

This shows that

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

We now turn to the second factor of the right hand side of Equation 4.2. We will show that this number is p by finding a unit $\epsilon \notin U^+_{p^{n-2}+1}$ such that

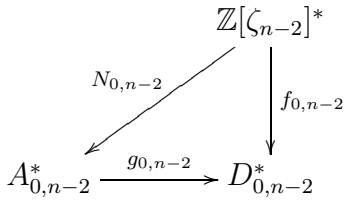
$$< \epsilon >= \frac{U^+_{p^{n-2}-1}}{U^+_{p^{n-2}+1}}.$$

Since we know that the p-th power of any unit in $U^+_{p^{n-2}-1}$ belongs to $U^+_{p^{n-2}+1}$ this is enough. Let $\zeta = \zeta_{n-2}$ and $\eta := \zeta^{\frac{p^{n-1}+1}{2}}$. Then $\eta^2 = \zeta$ and $c(\eta) = \eta^{-1}$. Let $\epsilon := \frac{\eta^{p^{n-2}+1} - \eta^{-(p^{n-2}+1)}}{\eta - \eta^{-1}}$. Then $c(\epsilon) = \epsilon$ and one can by direct calculations show that ϵ is the unit we are looking for.

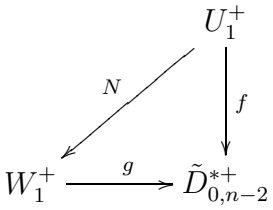
We now turn to

$$|\frac{U_1^+}{U_{p^{n-2}-1}^+}|.$$

Consider the commutative diagram



Let $W_m := \{\epsilon \in \mathbb{Z}[\zeta_{n-3}] \,:\, \epsilon \equiv 1 \mod \lambda_{n-3}^m\}$. It is clear that $f_{0,n-2}(U_1^+) \subseteq \tilde{D}^{*+}_{0,n-2}$ and that $g_{0,n-2}(W_1^+) \subseteq \tilde{D}^{*+}_{0,n-2}$. Recall that $A^*_{0,n-2} \cong \mathbb{Z}[\zeta_{n-3}]^* \oplus B$ and that the norm map $N_{0,n-2}$ acts like the usual norm map $N = \tilde{N}_{n-2,1} : \mathbb{Z}[\zeta_{n-2}]^* \to \mathbb{Z}[\zeta_{n-3}]^*$. It is well known that $N(\zeta_{n-2}) = \zeta_{n-3}$. By finding the constant term of the minimal polynomial $(x-1)^p - \zeta_{n-3}$ of λ_{n-2} we see that $N(\lambda_{n-2}) = \lambda_{n-3}$ and by a similar argument that $N(\zeta_{n-2}^k - 1) = \zeta_{n-3}^k - 1$ when $(k,p) = 1$. Since N is additive modulo p we get that $N_{0,n-2}(U_1^+) \subseteq W_1^+$. Hence we have a commutative diagram



We want to show that N is surjective. In $\mathbb{Z}[\zeta_j]$, let $w_j := -\zeta_j^{\frac{p^{j+1}+1}{2}}$ and consider

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

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

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

and hence real. Moreover,

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

so when $(l,p) = 1$ the $\gamma_{j,l}$ are units. Let J_j be the group of positive real units in $\mathbb{Z}[\zeta_j]$ and let $J_{0,j}$ be the subgroup generated by $\gamma_{j,l}$, $l \in \{2, 3, \ldots, (p^{j+1}-1)/2,\ (l,p) = 1\}$. This is a well known construction and the details can be found in the proof of Lemma 8.1, p. 149 in [W]. Since $\gamma_{j,l}$ is real, it is congruent to a rational integer $a \mod (\lambda_j^2)$. Of course, $a \not\equiv 0 \mod (p)$. Hence $a^{p-1} \equiv 1 \mod (p)$ and this shows that

$\gamma_{j,l}^{p-1} \equiv 1 \mod \lambda_j$. With $j = n-2$ this shows that $\gamma_{n-2,l}^{p-1} \in U_1^+$ and with $j = n-3$ that $\gamma_{n-3,l}^{p-1} \in W_1^+$. Now, a straightforward calculation shows that $N(\gamma_{n-2,l}^{p-1}) = \gamma_{n-3,l}^{p-1}$ so $J_{0,n-2}^{p-1} \subset N(U_1^+)$. Let h^+ be the class number of $\mathbb{Q}(\zeta_{n-3})^+$. It is well known that $h^+ | h_{\mathbb{Q}(\zeta_{n-3})}$. Since p is regular we get that $(p, h^+) = 1$. By Theorem 8.2 on p. 145 of [W] we have

$$\left|\frac{J_{n-3}}{J_{0,n-3}}\right| = h^+.$$

Now take arbitrary $\epsilon \in W_1^+$. Then ϵ^2 is positive and hence an element of J_{n-3}. By the fact above there exists $s \in \mathbb{Z}$ such that $(s,p) = 1$ and $e^{2s} \in J_{0,n-3}$. This means that $e^{2s(p-1)} \in N(U_1^+)$. Since $(2s(p-1), p) = 1$ we can find $u, v \in \mathbb{Z}$ such that $2s(p-1)u + pv = 1$ so $\epsilon = \epsilon^{2s(p-1)u+pv} = (\epsilon^{2s(p-1)})^u (\epsilon^p)^v \in N(U_1^+)$. This shows that N is surjective.

We will now use our inductive hypothesis. This means that $g(W_1^+) = \tilde{D}_{0,n-2}^{*+}$, that is, the map g is surjective. But since the diagram above is commutative this implies that f is also surjective. It is easy to see that $\ker(f) = U_{p^{n-2}-1}^+$ so

$$\frac{U_1^+}{U_{p^{n-2}-1}^+} \cong \tilde{D}_{0,n-2}^{*+}$$

and

$$\left|\frac{U_1^+}{U_{p^{n-2}-1}^+}\right| = |\tilde{D}_{0,n-2}^{*+}| = p^{\frac{p^{n-2}-3}{2}}$$

by proposition 4.3 This finally gives

$$\left|\frac{U_1^+}{U_{p^{n-1}-1}^+}\right| = p^{\frac{p^{n-2}-3}{2}} \cdot p \cdot p^{\frac{p^{n-1}-p^{n-2}}{2}-1} = p^{\frac{p^{n-1}-3}{2}}.$$

Hence $|g_{0,n-1}(U_1^+)| = |\tilde{D}_{0,n-1}^{*+}|$ and this proves the theorem. □

References

[J] Janusz, Gerald J, *Algebraic Number Fields, Second Edition* American Mathematics Society, 1996.

[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.

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

[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.* Proc. of the 2nd Int. Conf in Comm. Alg. 1997, 443-455.

[S3] Stolin, Alexander. *On the Picard Group of the Integer Group Ring of the Cyclic p-Group and Certain Galois Groups.* Journal of Number Theory 72, 1998, 28-66.

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

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

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

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

OLA HELENIUS AND ALEXANDER STOLIN

ABSTRACT. In 1977 Kervaire and Murthy presented two conjectures regarding $K_0\mathbb{Z}C_{p^n}$, where C_{p^n} is the cyclic group of order p^n and p an odd semi-regular prime. There is a group V_n that injects into $\tilde{K}_0\mathbb{Z}C_{p^n} \cong \operatorname{Pic}\mathbb{Z}C_{p^n}$. V_n is a canonical quotient of an in some sense simpler group $\mathcal{V}_n$. Both groups split in a "positive" and "negative" part. While V_n^- is well understood there is still no complete information on V_n^+. Kervaire and Murthy conjectured that $V_n^+ \cong (\mathbb{Z}/p^n\mathbb{Z})^{r(p)}$, where $r(p)$ is the index of irregularity of the prime p and that $\mathcal{V}_n^+ \cong V_n^+$. Under an extra assumption on the prime p, Ullom proved in 1978 that $V_n^+ \cong (\mathbb{Z}/p^n\mathbb{Z})^{r(p)} \oplus (\mathbb{Z}/p^{n-1}\mathbb{Z})^{\lambda - r(p)}$, where λ is one of the Iwasawa invariants. Hence Kervaire and Murthys first conjecture holds only when $\lambda = r(p)$. In the present paper we prove that under the same condition Ullom used, conjecture two always holds. We also discuss a different assumption on p regarding the p-rank of certain class groups in relation to the order of certain groups of units. Under this assumtion, which is implied by Ulloms assumption, we give a complete characteristation of $\mathcal{V}_n^+$. Finally, in the case $\lambda = r(p)$ we reprove Ulloms result by first proving that $\mathcal{V}_n^+ \cong (\mathbb{Z}/p^n\mathbb{Z})^{r(p)}$. Then we construct a special basis for a ring closely related to $\mathbb{Z}C_{p^n}$, consisting of units from a number field. This basis is used to prove that $\mathcal{V}_n^+ \cong V_n^+$.

1. INTRODUCTION

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

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

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

prove that there is an exact sequence

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

where

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

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

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

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

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

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

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

Kervaire and Murthy also formulate the following conjectures.

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

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

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

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

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

Assumption 1. *The Iwasawa invariants* λ_{1-i} *satisfy* $1 \leq \lambda_{1-i} \leq p-1$

We refer you to [I] for notation. S. Ullom proves that if Assumption 1 holds then, for even i,

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

This yields, under the same assumption, that

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

where

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

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

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

2. Preliminaries

We start this section by defining some rings that in some sense are close to $\mathbb{Z}C_{p^n}$. We discuss why we can and want to work with these rings instead of $\mathbb{Z}C_{p^n}$ and go on get an exact Mayer-Vietoris sequence from a certain pullback of these rings.

Let for $k \geq 0$ and $l \geq 1$

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

and

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

We denote the class of x in $A_{k,l}$ by $x_{k,l}$ and in $D_{k,l}$ by $\bar{x}_{k,l}$. Sometimes we will, by abuse of notation, just denote classes by x. Note that $A_{n,1} \cong \mathbb{Z}[\zeta_n]$ and that

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

By a generalization of Rim's theorem (see for example [ST1]) $\operatorname{Pic} \mathbb{Z}C_{p^n} \cong \operatorname{Pic} A_{0,n}$ for all $n \geq 1$ so for our purposes we can just as well work with $A_{0,n}$ instead of directly with $\mathbb{Z}C_{p^n}$. It is easy to see that there exists a pullback diagram

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

where $i_{k,l+1}(x_{k,l+1}) = \zeta_{k+l}$, $j_{k,l+1}(x_{k,l+1}) = x_{k,l}$, $f_{k,l}(\zeta_{k+l}) = \bar{x}_{k,l}$ and $g_{k,l}$ is just taking classes modulo p. The norm-maps $N_{k,l}$ will be constructed later in this paper. These maps are really the key to our methods.

The pullback 2.1 induces a Mayer-Vietoris exact sequence

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

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

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

we get an exact sequence

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

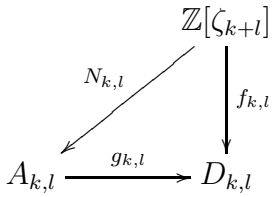
Note that definition of V_n is slightly different from the one from [K-M] but the two groups are isomorphic. By abuse of notation, let c denote the automorphisms on $A_{k,l}^*$, $\mathbb{Z}[\zeta_n]^*$ and $D_{k,l}^*$ induced by $c(t) = t^{-1}$ for $t = x_{k,l}$, $t = \zeta_n$ and $t = \bar{x}_{k,l}$ respectively. We also denote the maps induced on $\mathcal{V}_n$ and V_n by c.

Before moving on we need to introduce the map $N_{k,l}$. An element $a \in A_{k,l+1}$ can be uniquely represented as a pair $(a_l, b_l) \in \mathbb{Z}[\zeta_{k+l}] \times A_{k,l}$. Using a similar argument on b_l, and then repeating this, we find that a can also be uniquely represented as an $(l+1)$-tuple $(a_l, \ldots, a_m, \ldots, a_0)$ where $a_m \in \mathbb{Z}[\zeta_{k+m}]$. In the rest of this

paper we will identify an element of $A_{k,l+1}$ with both its representations as a pair or an $(l+1)$-tuple.

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

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



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

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

The construction of $N_{k,l}$ can be found in [ST2]. Since it may not be well known we will for completeness repeat it here. Before this we notice an immediate consequence of the commutativity of the diagram in Proposition 2.1.

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

Proof. The maps $N_{k,l}$ will be constructed inductively. If $i = 1$ and k is arbitrary, we have $A_{k,1} \cong \mathbb{Z}[\zeta_k]$ and we define $N_{k,1}$ as the usual norm map $\tilde{N}_{k+1,1}$. Since $\tilde{N}_{k+1,1}(\zeta_{k+1}) = \zeta_k$ we only need to prove that our map is additive modulo p, which follows from the lemma below.

Lemma 2.3. *For $k \geq 0$ and $l \geq 1$ we have*

i) $A_{k+1,l}$ is a free $A_{k,l}$-module under $x_{k,l} \mapsto x^p_{k+1,l}$.
ii) The norm map $N : A_{k+1,l} \to A_{k,l}$, defined by taking the determinant of the multiplication operator, is additive modulo p.

This is Lemma 2.1 and Lemma 2.2 in [ST2] and proofs can be found there.

Now suppose $N_{k,j}$ is constructed for all k and all $j \leq l-1$. Let $\varphi = \varphi_{k+1,l} : \mathbb{Z}[\zeta_{k+l}] \to A_{k+1,l}$ be defined by $\varphi(a) = (a, N_{k+1,l-1}(a))$. It is clear that φ is multiplicative. From the lemma above we have a norm map $N : A_{k+1,l} \to A_{k,l}$. Define $N_{k,l} := N \circ \varphi$. It is clear that $N_{k,l}$ is multiplicative. Moreover, $N_{k,l}(\zeta_{k+l}) = N(\zeta_{k+l}, x_{k+1,l-1}) = N(x_{k+1,l}) = x_{k,l}$, where the latter equality follows by a direct computation. To prove that our map makes the diagram in the proposition above

commute, we now only need to prove it is additive modulo p. This also follows by a direct calculation once you notice that

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

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

Regarding the other two equalities in Proposition 2.1, it is clear that the second one follows from the first. The first statement will follow from the lemma below.

Lemma 2.4. *The diagram*

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

is commutative

Proof. Recall that the maps denoted N (without subscript) are the usual norms defined by the determinant of the multiplication map. An element in $A_{k,l}$ can be represented as a pair $(a,b) \in \mathbb{Z}[\zeta_{k+l-1}] \times A_{k,l-1}$ and an element in $A_{k-1,l}$ can be represented as a pair $(c,d) \in \mathbb{Z}[\zeta_{k+l-2}] \times A_{k-1,l-1}$. If (a,b) represents an element in $A_{k,l}$ one can, directly from the definition, show that $N(a,b) = (N(a), N(b)) \in A_{k-1,l}$. We now use induction on l. If $l = 1$ the statement is well known. Suppose the diagram corresponding to the one above, but with i replaced by $i-1$, is commutative for all k. If $a \in \mathbb{Z}[\zeta_{k+l}]$ we have

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

and

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

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

With the proof of this Lemma the proof of Proposition 2.1 is complete. □

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

Lemma 2.5. *Let $B_{k,l}$ be the subgroup of $A^*_{k,l}$ consisting of elements $(1,b)$, $b \in A^*_{k,l-1}$. Then $A^*_{k,l} \cong \mathbb{Z}[\zeta_{k+l-1}]^* \times B_{k,l}$*

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

Before we move on we will state a technical lemma which is Theorem I.2.7 in [ST3].

Lemma 2.6. $\ker(g_{k,l}|_{\mathbb{Z}[\zeta_{k+l-1}]^*}) = \{\epsilon \in \mathbb{Z}[\zeta_{k+l-1}]^* : \epsilon \equiv 1 \mod \lambda_{k+l-1}^{p^{k+l}-p^k}\}$

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

If for example $l = 2$, we get after just one step $a \equiv 1 \mod p$ in $\mathbb{Z}[\zeta_{k+1}]$, $N(a) \equiv 1 \mod p$ and $N(\frac{a-1}{p}) \equiv \frac{N(a)-1}{p} \mod p$ in $A_{k,1} \cong \mathbb{Z}[\zeta_k]$, where N is the usual norm. By viewing N as a product of automorphisms, recalling that N is additive modulo p and that the usual trace of any element of $\mathbb{Z}[\zeta_{k+1}]$ is divisible by p, we get that $N(a) \equiv 1 \mod p^2$ and hence that $N(\frac{a-1}{p}) \equiv 0 \mod p$. By analyzing how the norm acts one can show that this means that $a \equiv 1 \mod \lambda_{k+1}^{p^{k+2}-p^k}$

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

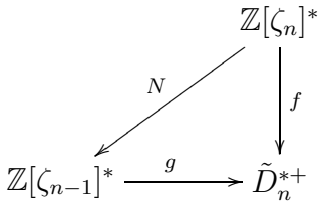
Now define $\mathcal{V}_n$ as

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

where $\tilde{\mathbb{Z}}[\zeta_{n-1}]^*$ are the group of all units ϵ such that $\epsilon \equiv 1 \bmod \lambda_{n-1}$, where λ_n denotes the ideal $(\zeta_n - 1)$, and $\tilde{D}^*_n$ are the units that are congruent to 1 modulo the class of $(\bar{x} - 1)$ in D^*_n. This definition is equivalent to the definition in [K-M] by the following Proposition.

Proposition 2.7. *The two definitions of $\mathcal{V}_n$ coincide.*

Proof. The kernel of the surjection $(\mathbb{F}_p[x]/(x-1)^{p^n})^* \to (\mathbb{F}_p[x]/(x-1)^{p^n-1})^* = D_n^*$ consists 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 $\epsilon := \frac{\eta^{p^n+1}-\eta^{-(p^n+1)}}{\eta-\eta^{-1}}$. One can by a direct calculation show that $\epsilon = 1+(\zeta_n-1)^{p^n-1}+t(\zeta_n-1)^{p^n}$ 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



is commutative and N (which is the restriction of the usual norm-map) surjective when p is semi-regular (Lemma 3.3) the proposition follows. □

3. On Conjecture 2

Let $\mathcal{V}_n^+ := \{v \in \mathcal{V}_n \ : \ c(v) = v\}$. What we want to do is to find the structure of $\mathcal{V}_n^+$. For $n \geq 0$ and $k \geq 0$, define

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

One of our main results is the following proposition.

Proposition 3.1. *If p is semi-regular, $|\mathcal{V}_n^+| = |\mathcal{V}_{n-1}^+| \cdot |U_{n-1,p^n-1}/(U_{n-1,p^{n-1}+1})^{(p)}|$.*

Here $U^{(p)}$ denotes the group of p-th powers of elements of the group U.

For $k = 0, 1, \ldots$, define r_k by

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

By Lemma 2 in [ST1] we get that $U_{k,p^{k+1}-1} = U_{k,p^{k+1}}$ and since the the λ_n-adic valuation of $\epsilon - 1$, where ϵ is a real unit, is even, $U_{k,p^{k+1}} = U_{k,p^{k+1}+1}$. We hence have

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

One can prove that $r_0 = r(p)$, the index of irregularity, since if the λ_0-adic valuation of $\epsilon \in \mathbb{Z}[\zeta_0]^{*+}$ is less than $p-1$, then local considerations show that the

extension $\mathbb{Q}(\zeta_0) \subseteq \mathbb{Q}(\zeta_0, \sqrt[p]{\epsilon})$ is ramified. The result then follows from the fact that

$$\frac{U_{0,p-1}}{(U_{0,2})^p} \cong \frac{S_0}{pS_0}$$

where S_0 is the p-class group of $\mathbb{Q}(\zeta_0)$.

Before the proof of Proposition 3.1 we will state and a lemma, which is well-known.

Lemma 3.3. *If p is semi-regular $N_{n-1} : \mathbb{Z}[\zeta_{n-1}] \to A_{n-1}$ maps $U_{n-1,1}$ surjectively onto $U_{n-2,1}$.*

Proof of Proposition 3.1. In a similar way as the ideal $\lambda_n := (\zeta_n - 1)$ equal the ideal $(\zeta_n - \zeta_n^{-1})$ in $\mathbb{Z}[\zeta_n]$ one can show that that $(\bar{x} - 1) = (\bar{x} - \bar{x}^{-1})$ in D_n. It is easy to show that $\tilde{D}_n^{*+}$ can be represented by elements $1 + a_2(\bar{x} - \bar{x}^{-1})^2 + a_4(\bar{x} - \bar{x}^{-1})^4 + \ldots + a_{p^n-3}(x - x^{-1})^{p^n-3}$, $a_i \in \mathbb{F}_p$. Hence $|\tilde{D}_n^{*+}| = p^{(p^n-3)/2}$. We want to evaluate

$$|\tilde{D}_n^{*+}|/|g_n(U_{n-1,1})|.$$

By Lemma 2.6 we have

$$g_n(U_{n-1,1}) \cong \frac{U_{n-1,1}}{U_{n-1,p^n-1}}.$$

Since $g_n(U_{n-1,1}) \subseteq g_n(\mathbb{Z}[\zeta_{n-1}]^{*+}) \subseteq \tilde{D}_n^{*+}$ the group $U_{n-1,1}/U_{n-1,p^n-1}$ is finite. Similarly $\mathbb{Z}[\zeta_{n-1}]^{*+}/U_{n-1,p^n-1}$ is finite. This shows that $\mathbb{Z}[\zeta_{n-1}]^{*+}/U_{n-1,1}$ is finite since

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

We can write

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

By Dirichlet's theorem on units we have $(\mathbb{Z}[\zeta_{n-1}]^*)^+ \cong \mathbb{Z}^{\frac{p^n-p^{n-1}}{2}-1}$ Since all quotient groups involved are finite we get that $U_{n-1,1}$, U_{n-1,p^n-1}, $U_{n-1,p^{n-1}-1}$ and $U_{n-1,p^{n-1}+1}$ are all isomorphic to $\mathbb{Z}^{\frac{p^n-p^{n-1}}{2}-1}$. The rest of the proof is devoted to the analysis of the four right hand factors of 3.1.

Obviously,

$$\frac{U_{n-1,p^{n-1}+1}}{(U_{n-1,p^{n-1}+1})^p} \cong \frac{\mathbb{Z}^{\frac{p^n-p^{n-1}}{2}-1}}{(p\mathbb{Z})^{\frac{p^n-p^{n-1}}{2}-1}} \cong C_p^{\frac{p^n-p^{n-1}}{2}-1}.$$

This shows that

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

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

$$< \epsilon >= \frac{U_{n-1,p^{n-1}-1}}{U_{n-1,p^{n-1}+1}}.$$

Since the p-th power of any unit in $U_{n-1,p^{n-1}-1}$ belongs to $U_{n-1,p^{n-1}+1}$ this is enough. Let $\zeta = \zeta_{n-1}$ and $\eta := \zeta^{\frac{p^n+1}{2}}$. Then $\eta^2 = \zeta$ and $c(\eta) = \eta^{-1}$. Let $\epsilon := \frac{\eta^{p^{n-1}+1}-\eta^{-(p^{n-1}+1)}}{\eta-\eta^{-1}}$. Then $c(\epsilon) = \epsilon$ and one can by direct calculations show that ϵ is the unit we are looking for.

We now want to calculate

$$|\frac{U_{n-1,1}}{U_{n-1,p^{n-1}-1}}|.$$

Consider the commutative diagram

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

It is clear that $f_{n-1}(U_{n-1,1}) \subseteq \tilde{D}^{*+}_{n-1}$ and that $g_{n-2}(U_{n-2,1}) \subseteq \tilde{D}^{*+}_{n-1}$. By Lemma 3.3 we have a commutative diagram

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

where N is surjective. Clearly, $f(U_{n-1,1}) = g(U_{n-2,1})$.

It is easy to see that $\ker(f) = U_{n-1,p^{n-1}-1}$ so by above

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

Now recall that by definition $\mathcal{V}_{n-1}^+ = \tilde{D}_{n-1}^{*+}/g(U_{n-2,1})$. Hence

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

This finally gives

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

which is what we wanted to show.

□

Recall that $\lambda_k\mathbb{Z}[\zeta_{k+1}] = \lambda_{k+1}^p$ as ideals in $\mathbb{Z}[\zeta_{k+1}]$. By Lemma 3.2, the inclusion of $\mathbb{Z}[\zeta_k]$ in $\mathbb{Z}[\zeta_{k+1}]$ induces an inclusion of $U_{k,p^{k+1}-1} = U_{k,p^{k+1}+1}$ into $U_{k+1,p^{k+2}+p} \subseteq U_{k+1,p^{k+2}-1}$. Since a p-th power in $\mathbb{Z}[\zeta_k]$ obviously is a p-th power in $\mathbb{Z}[\zeta_{k+1}]$ we get an homomorphism of

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

If $\epsilon \in U_{k,p^{k+1}-1}$ is a not p-th power in $\mathbb{Z}[\zeta_k]$ then one can show that $\mathbb{Q}(\zeta_k) \subseteq \mathbb{Q}(\zeta_k, \epsilon)$ is an unramified extension of degree p. If ϵ would be a p-th power in $\mathbb{Z}[\zeta_{k+1}]$ we would get $\mathbb{Q}(\zeta_{k+1}) = \mathbb{Q}(\zeta_k, \epsilon)$ which is impossible since $\mathbb{Q}(\zeta_k) \subseteq Q(\zeta_{k+1})$ is ramified. Hence the homomorphism 3.2 is injective. This shows that the sequence $\{r_k\}$ non-decreasing.

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

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

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

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

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

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

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

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

Since V_n^+ is a quotient of $\mathcal{V}_n^+$ applying this to $n = n_0 + 1$ yields

$$r_0 + \lambda n_0 \leq r_0 + r_1 + \ldots + r_{n_0} \leq r_0 + n_0 r_{n_0} \leq r_0 + n_0 \lambda.$$

This obviously implies that $r_k = \lambda$ for all $k = 1, 2, \ldots$.

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

The following theorem is now immediate.

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

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

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

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

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

Theorem 3.9. *If Assumption 2 holds*

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

Before the proof we need some results.

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

Proof of Lemma 3.10. The canonical surjection $j_n : A_n \to A_{n-1}$ can be considered mod (p) and hence yields a surjection $\bar{j}_n : D_n \to D_{n-1}$. Suppose that $\bar{u} \in D_{n-1}^{*+}$, $\bar{v} \in D_n^{*+}$, $\bar{j}_n(\bar{v}) = \bar{u}$ and that $\bar{v} = g_n(v)$, where $v = (\epsilon, N_{n-1}(\epsilon))$, $\epsilon \in \mathbb{Z}[\zeta_{n-1}]$. Then $j_n(v) = N_{n-1}(\epsilon)$, and $\bar{u} = \bar{j}_n(\bar{v}) = \bar{j}_n g_n N_{n-1}(\epsilon)$. But $N_{n-1}(\epsilon) = (\tilde{N}_{n-1,1}(\epsilon), N_{n-2}\tilde{N}_{n-1,1}(\epsilon))$ by Proposition 2.1. In other words, if $\bar{v}$ represents 1 in $\mathcal{V}_n$, then $\bar{j}_n(\bar{v})$ represents 1 in $\mathcal{V}_{n-1}$ so the map $\bar{j}_n$ induces a well defined surjection $\mathcal{V}_n^+ \to \mathcal{V}_{n-1}^+$. □

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

Proof. Proposition 3.1 and the definition of r_n clearly implies that $|\ker \pi_n| = p^{r_{n-1}}$. We need to prove that any element in $\ker \pi_n$ has order at most p. Suppose that in the surjection $D_n^{*+} \to D_{n-1}^{*+}$, the element $u \in D_{n-1}^{*+}$ is the image of $v \in D_n^{*+}$ and suppose $u = g_{n-1}((\epsilon, N_{n-2}(\epsilon)))$ for some $\epsilon \in U_{n-2,1} \subset \mathbb{Z}[z_{n-2}]$. For some $a \in A_n$, $v = g_n(a)$ and $(\epsilon, N_{n-2}(\epsilon)) = j_n(a)$. Since p is semi-regular we know from Lemma 3.3 that the norm map N_{n-1} resticted to $U_{n-1,1}$ is surjective onto $U_{n-2,1}$ and acts as the usual norm $\tilde{N}_{n-1,1}$. Hence there exists $\epsilon' \in U_{n-1,1}$ such that $N_{n-1}(\epsilon') = (\epsilon, N_{n-2}(\epsilon))$. This means that $(\epsilon', N_{n-1}(\epsilon')) \in A_n^{*+}$ maps to $(\epsilon, N_{n-2}(\epsilon))$ under j_n. Since $f_{n-1}(\epsilon') = g_{n-1}N_{n-1}(\epsilon') = u$ and all the maps come from a pullback we get that $a = (\epsilon', N_{n-1}(\epsilon'))$, that is, v is the image of a unit in $U_{n-1,1}$. Now define $\tilde{D}_{n,(k)}^{*+} := \{a \in \tilde{D}_n^{*+} : a \equiv 1 \bmod (x-1)^k\}$. Then

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

Now note that if $b \in \tilde{D}_{n,(p^{n-1})}^{*+}$, then $b^p = 1$ so such a unit clearly has order p. We will show that any unit $a \in \tilde{D}_{n,(p^{n-1}-1)}^{*+}$ can be written as $a = bg_n(\epsilon)^k$ for some $b \in \tilde{D}_{n,(p^{n-1})}^{*+}$, natural number k and $\epsilon \in U_{n-1,p^{n-1}-1}$. Then $a^p = b^p g_n(\epsilon)^{kp}$ is clearly trivial in $\ker \pi_n \subseteq \mathcal{V}_n^+$. Let $\eta := \zeta_{n-1}^{\frac{p^n+1}{2}}$. Then $\eta^2 = \zeta_{n-1}$ and $c(\eta) = \eta^{-1}$. Let $\epsilon := \frac{\eta^{p^{n-1}+1} - \eta^{-(p^{n-1}+1)}}{\eta - \eta^{-1}}$. One can by a direct calculation show that $\epsilon \in U_{n-1,p^{n-1}-1} \setminus U_{n-1,p^{n-1}+1}$. In fact, $\epsilon = 1 + e_{p^{n-1}-1}(\zeta_{n-1} - \zeta_{n-1}^{-1})^{p^{n-1}-1} + t(\zeta_{n-1} - \zeta_{n-1}^{-1})^{p^{n-1}+1}$ for some non-zero $e_{p^{n-1}-1} \in \mathbb{Z}[z_{n-2}]$, not divisible by λ_{n-1}, and some $t \in \mathbb{Z}$. Suppose $a = 1 + a_{p^{n-1}-1}(x_{n-1} - x_{n-1}^{-1})^{p^{n-1}-1} + \ldots \in \tilde{D}_{n,(p^{n-1}-1)}^{*+}$, $a_{p^{n-1}-1} \in \mathbb{F}_p^*$. Since $e_{p^{n-1}-1}$ is not divisible by λ_{n-1}, $g_n(\epsilon) \in \mathbb{F}_p^*$ Hence we can choose k such that $kg_n(e_{p^{n-1}-1}) \equiv a_{p^{n-1}-1} \mod p$. Then it is just a matter of calculations to show that $a = bg_n(\epsilon)^k$, where $b \in \tilde{D}_{n,(p^{n-1})}^{*+}$, which concludes the proof □

Proof of Theorem 3.9. Induction with respect to n. If $n = 1$ the result is known from for example [K-M]. Suppose the result holds with the index equal to $n-1$. There are no elements in D_n^* with order greater than p^n and hence there

are no elements in $\mathcal{V}_n^+$ with order greater than p^n. Since $\mathcal{V}_n^+$ is a p-group,

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

By Proposition 3.11 and the assumtion we have an exact sequence

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

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

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

□

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

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

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

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

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

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

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

Proof of Proposition 4.1. By Lemma 3.2 we need to calculate the number $|U_{n,p^{n+1}+1}/(U_{n,p^n+1})^p|$. Denote the field $\mathbb{Q}(\zeta_n)$ by K_n and let L_n be the maximal unramified extension of K_n of period p. Clearly, $G_n := \operatorname{Gal}(L_n/K_n) = \operatorname{Cl}^{(p)}(K_n)/p\operatorname{Cl}^{(p)}(K_n)$. By the assumption $|G_n| = p^r$. It is known by Iwasawa theory that $G_n = G_n^-$. If $\epsilon \in U_{n,p^{n+1}+1}$ it follows from local considerations that

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

Now recall that for $n = 1$ it is proved in [K-M] that $\mathcal{V}_1^+ \cong (\mathbb{Z}/p\mathbb{Z})^r$. Suppose the result holds for all $k \leq n$. Then $\mathcal{V}_{n-1}^+ \cong (\mathbb{Z}/p^{n-1}\mathbb{Z})^r$ and the surjection $\pi_n : \mathcal{V}_n^+ \to \mathcal{V}_{n-1}^+$ from Lemma 3.10 means that $\mathcal{V}_n^+$ has at least r generators. By our assumtion $\mathrm{Cl}^{(p)}\,\mathbb{Q}(\zeta_{n-1})$ has r generators and by using the injection $\mathrm{Char}\,\mathcal{V}_n^+ \to \mathrm{Cl}^{(p)}\,\mathbb{Q}(\zeta_{n-1})$ we get that $\mathcal{V}_n^+$ has at most, and hence by above exactly r generators. By Theorem 4.2 $|\mathcal{V}_n^+| = p^{rn}$. Since no elements in D_n^{*+} and hence no elements in $\mathcal{V}_n^+$ have order greater than p^n we now get the following theorem by induction.

Theorem 4.3. *If p is a semi-regular prime and r the index of irregularity and Assumption 3 holds, then $\mathcal{V}_n^+ \cong (\mathbb{Z}/p^n\mathbb{Z})^r$.*

We now proceed to show how we can directly show that $\mathcal{V}_n^+ = V_n^+$ when $\mathcal{V}_n^+ \cong (\mathbb{Z}/p^n\mathbb{Z})^r$. The proof of this relies of constructing a certain basis for D_{n-1}^+ consisting of norms of elements from $\mathbb{Z}[\zeta_{n-1}]^*$ considered $\mod p$.

Let $\Phi : U_{n-1,p^n-p^{n-1}} \to D_{n-1}^+$ be defined by

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

Since N_{n-1} is additive $\mod p$ one can show with some simple calculations that Φ is a group homomorphism. See Lemmas 4.8 and 4.14 for details.

Explicitly, what we want to prove is the following.

Theorem 4.4. *If $\mathcal{V}_n^+ \cong (\mathbb{Z}/p^n\mathbb{Z})^r$, then Φ is a surjective group homomorphism.*

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

Corollary 4.5. *If $\mathcal{V}_n^+ \cong (\mathbb{Z}/p^n\mathbb{Z})^r$, then $V_n^+ = \mathcal{V}_n^+$*

Proof of the Corollary. We want to show that for any $(1,\gamma) \in A_n^*$ there exists $(\epsilon, N_{n-1}(\epsilon)) \in A_n^*$ such that $(1,\gamma) \equiv (\epsilon, N_{n-1}(\epsilon)) \mod p$, or more explicitly that for all $\gamma \in A_{n-1}^{*+}$, $\gamma \equiv 1 \mod p$ there exists $\epsilon \in \mathbb{Z}[\zeta_{n-1}]^*$ such that $(\epsilon, N(\epsilon)) \equiv (1,\gamma) \mod p$ in A_n. This is really equivalent to the following three statements in $\mathbb{Z}[\zeta_{n-1}]$, A_{n-1} and D_{n-1} respectively

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

Note that $(1,\gamma) \in A_n$ implies $g_{n-1}(\gamma) = f_{n-1}(1)$ in D_{n-1}, or in other words, that $\gamma \equiv 1 \mod p$. Hence we only need to show that for any $\gamma \in A_{n-1}^{*+}$ there exists $\epsilon \in U_{n-1,p^n-p^{n-1}}$ such that

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

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

We now proceed to start proving Theorem 4.4. Recall that $r = r(p)$ are the number of indexes $i_1, i_2 \dots i_r$ among $1, 2 \dots (p-3)/2$ such that the nominator of the Bernoulli number B_{i_k} (in reduced form) is divisible by p.

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

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

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

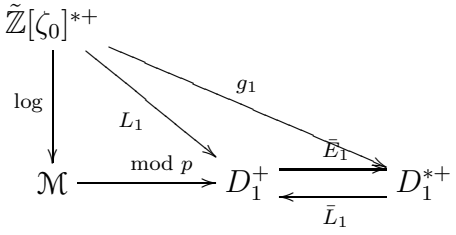
$$\bar{L_n}(1+y) = y - \frac{y^2}{2} + \dots - \frac{y^{p-1}}{(p-1)}.$$

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

We denote the cyclytomic units of $\mathbb{Z}[\zeta_0]^{*+}$ by C_0^+. Let $\mathcal{M}$ be the group of real λ_0-adic integers with zero trace. Any $a \in \mathcal{M}$ can be uniquely presented as $a = \sum_{i=1}^{m-1} b_i \lambda_0^{2i}$, $m = (p-1)/2$. Consider the homomorphism $\Psi : \mathbb{Z}[\zeta_0]^* \to \mathcal{M}$ defined

by $\epsilon \mapsto \log(\epsilon^{p-1})$. Following [B-S], page 370-375, we see that there are exactly r elements λ_0^{2i}, namely $\lambda_0^{2i_k}$, such that $\lambda_0^{2i} \notin \Psi(C_0^+)$. This implies that for exactly the r indexes $i_1, i_2 \dots i_r$ we have $(\bar{x}_1 - \bar{x}_1^{-1})^{2i_k} \neq g_1(log(\epsilon^{p-1}))$ for any $\epsilon \in C_0^+$.

Suppose $(x - x^{-1})^{2i_s} = g_1(\log \epsilon)$ for some $\epsilon \in \mathbb{Z}[\zeta_0]^{*+}$. It is well known that the index of C_0^+ in $\mathbb{Z}[\zeta_0]^{*+}$ equals the classnumber h_+ of $\mathbb{Q}(\zeta_0)^+$. Since p is semi-regular there exists s with $(s,p) = 1$ such that $\epsilon^s \in C_0^+$ and by co-primality of $s(p-1)$ and p we can find u, v such that $1 = s(p-1)u + pv$. Then $\epsilon = \epsilon^{s(p-1)u+pv} = (\epsilon^s)^{p-1}\epsilon^{pv}$ so $\log((\epsilon^{su})^{(p-1)u}) = \log \epsilon - pv \log \epsilon \equiv \log \epsilon \equiv (x - x^{-1})^{2i_s}$, which is a contradiction. Hence $(x - x^{-1})^{2i_s} \notin g_1(\log \mathbb{Z}[\zeta_0]^{*+})$. Since formally, $\exp(\log(1+y)) = 1 + y$ it is not hard to see that $E_1(L_1(1+y)) \equiv 1 + y \mod p$ and that we have a commutative diagram



Recall that $D_{n,(s)}^{*+} := \{y \in D_n^{*+} : y \equiv 1 \mod (x - x^{-1})^s\}$ and that we know that $\mathcal{V}_1^+ := D_1^{*+}/g_1(\mathbb{Z}[\zeta_0]^{*+})$ has $r := r(p)$ generators. If we now apply the map E_1 and do some simple calculations we now get the following proposition.

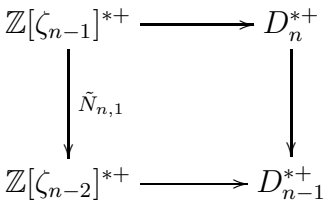
Proposition 4.6. *The r elements $\bar{E}_1((x_1 - x_1^{-1})^{2i_k})$ generate $D_1^{*+}/g_1(\mathbb{Z}[\zeta_0]^{*+})$ and belong to $D_{1,(2)}^{*+}$ but do not belong to $D_{1,(p-2)}^{*+}$.*

We now want to lift this result to D_n^{*+}. From now on (exepting Lemma 4.11) we will denote the generator $x \in D_n$ by x_n.

Proposition 4.7. *If Assumption 3 holds, then the r elements $\bar{E}_n((x_n - x_n^{-1})^{2i_k})$ generate the group $\mathcal{V}_n^+ := D_n^{*+}/g_n(\mathbb{Z}[\zeta_{n-1}]^{*+})$. The elements $\bar{E}_n((x_n - x_n^{-1})^{2i_k})^{p^{n-1}}$ are non-trivial in $\mathcal{V}_n^+$, belong to $D_{n,(p^{n-1})}^{*+}$ but do not belong to $D_{n,(p^n - 2p^{n-1})}^{*+}$*

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

(4.1)



is commutative. Hence, if $z_n \in D_n^*$ is mapped to $z_{n-1} \in D_{n-1}^*$ and $z_{n-1} \notin \operatorname{Im}\mathbb{Z}[\zeta_{n-2}]^*$, then $z_n \notin \operatorname{Im}\mathbb{Z}[\zeta_{n-1}]^*$. Moreover, $z_n^p \notin \operatorname{Im}\mathbb{Z}[\zeta_{n-1}]^*$ in this case. This follows from the fact that $\mathcal{V}_m^+ \cong (\mathbb{Z}/p^m\mathbb{Z})^r$ for all m. Hence, if an element $z \in \mathcal{V}_n^+$ has order p, then the surjection $\mathcal{V}_n^+ \to \mathcal{V}_{n-1}^+$ maps z to the neutral element in $\mathcal{V}_{n-1}^+$. Now, the elements $\bar{E}_n((x_n - x_n^{-1})^{2i_k})^{p^{n-1}}$ are not in the image of $\mathbb{Z}[\zeta_{n-1}]^*$ by Theorem 4.3 and since $\bar{E}_n((x_n - x_n^{-1})^{2i_k})^{p^{n-2}}$ clearly map onto $\bar{E}_{n-1}((x_{n-1} - x_{n-1}^{-1})^{2i_k})^{p^{n-2}} \notin g_{n-1}(\mathbb{Z}[\zeta_{n-2}]^{*+})$ by induction. Finally, since $1 \leq 2i_k \leq p-1$ we get $p^{n-1} \leq 2p^{n-1}i_k \leq p^n - 2p^{n-1}$ and this means that all the elements

$$\begin{aligned}\bar{E}_n((x_n - x_n^{-1})^{2i_k})^{p^{n-1}} &= (1 + (x_n - x_n^{-1})^{2i_k} + \ldots)^{p^{n-1}} = \\ &= 1 + (x_n - x_n^{-1})^{2p^{n-1}i_k} + \ldots\end{aligned}$$

fulfil our requirements. □

Recall that $c : D_n \to D_n$ is the map induced by $\bar{x} \mapsto \bar{x}^{-1}$ and that $D_n^+ := \{a \in D_n : c(a) = a\}$ Define $\varphi : U_{n-1,p^n-p^{n-1}}^+ \to D_{n-1}^+$ by $\varphi(\gamma) = N_{n-1}\big(\frac{\gamma-1}{p}\big) \mod p$.

Lemma 4.8. *φ is a homomorphism from the multiplicative group $U_{n-1,p^n-p^{n-1}}^+$ to the additive group D_{n-1}^+ and the kernel is $U_{n-1,p^n-1}^+ = U_{n-1,p^n+1}^+$.*

Proof. Let ϵ and γ belong to $\in U_{n-1,p^n-p^{n-1}}^+$. Then, since N_{n-1} is additive mod p and $N_{n-1}(\epsilon) \equiv 1 \mod p$,

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

so φ is a homomorphism. Suppose $N_{n-1}((\gamma-1)/p) \equiv 0 \mod p$. Then, by Proposition 2.1, $f_{n-1}((\gamma-1)/p) = 0$ which means $\gamma \in U_{n-1,p^n-1}^+ = U_{n-1,p^n+1}^+$ (the latter equality is due to Lemma 3.2). □

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

Proposition 4.9. *If Assumption 3 holds, then the map*

$$\tilde{\varphi} : (U_{n-1,p^n-p^{n-1}})/(U_{n-1,p^n+1}) \to D_{n-1}^+$$

induced by φ is an isomorphism.

Since $\tilde{\varphi}$ is obviously injective it is enough to prove the following proposition

Proposition 4.10. *Suppose Assumption 3 holds. Then*

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

Proof. Recall that $|D^+_{n-1}| = p^{\frac{p^{n-1}-1}{2}}$ so we need to prove that

$$|(U_{n-1,p^n-p^{n-1}})/(U_{n-1,p^n-1})| = p^{\frac{p^{n-1}-1}{2}}.$$

An element of $\mathcal{V}^+_n$ of the form $b = 1+(x_n-x_n^{-1})^{2s_1}$, where $p^{n-1} < 2s \leq 2s_1 < p^n-1$, correspond to a non-trivial element of

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

which is a canonical subgroup of $\mathcal{V}^+_n$. If t_{2s} is the number of independent such elements b, then

$$\frac{D^{*+}_{n,(2s)}}{g_n(\mathbb{Z}[\zeta_{n-1}]^{*+}) \cap D^{*+}_{n,(2s)}} \cong (\mathbb{Z}/p\mathbb{Z})^{t_{2s}}$$

By Proposition 4.7, $t_{2s} = 0$ if $2s > p^n - 2p^{n-1}$. On the other hand

$$g_n(\mathbb{Z}[\zeta_{n-1}]^{*+}) \cap D^{*+}_{n,(2s)} \cong U_{n-1,2s}/U_{n-1,p^n-1}$$

since $U_{n-1,p^n-1} = \ker(g_n)$, and hence $U_{n-1,2s}/U_{n-1,p^n-1} \cong D^{*+}_{n,(2s)}$ if $2s > p^n - 2p^{n-1}$. The number of elements in $D^{*+}_{n,(2s)}$ is $p^{\frac{p^n-1-2s}{2}}$. Setting $2s = p^n - p^{n-1}$ completes the proof. □

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

Lemma 4.11. *Let $2 \leq n$ and $1 \leq k < n$. If $\epsilon \in \mathbb{Z}[\zeta_{n-1}]$ and If $\epsilon \equiv 1 \mod p^{s+1}\lambda_{n-1}^{p^{n-1}-p^k}$, then $(N_{n-1}(\epsilon)-1)/p$ can be represented by a polynomial $f(x) = p^s f_1(x)$ in A_{n-1}, where $f_1(x) \equiv 0 \mod (x-1)^{p^{n-1}-p^{k-1}}$ in D_{n-1}.*

Before the proof, recall that the usual norm $\tilde{N}_{n,1}$, $1 \leq n, 1 \leq k < n$, can be viewed as a product of automorphisms of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}(\zeta_{n-1})$. If $t_n \in \mathbb{Z}[\zeta_n]$ and $t_{n-1} \in \mathbb{Z}[\zeta_{n-1}]$ we immediately get $\tilde{N}_{n,1}(1+t_{n-1}t_n) = 1 + \mathrm{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_{n-1})}(t_n)t_{n-1}t'$ for some $t' \in \mathbb{Z}[\zeta_{n-1}]$. Recall that the trace is always divisible by p. In the proof below we will for convenience denote any generic element whose value is not interesting for us by the letter t.

Proof. Induction on n. If $n = 2$ (which implies $k = 1$), $N_{n-1} = \tilde{N}_{1,1} : \mathbb{Z}[\zeta_1] \to A_1 \cong \mathbb{Z}[\zeta_0]$. Let $\epsilon := 1 + tp^{s+1}$ Then $\epsilon = 1 + tp^s\lambda_1^{p^2-p} = 1 + tp^s\lambda_0^{p-1}$. By the note above,

$$\frac{\tilde{N}_{1,1}(\epsilon) - 1}{p} = tp^s\lambda_0^{p-1}$$

which is represented by some $f(x) = p^s(x-1)^{p-1}f_1(x)$ in A_1 Suppose the statement of the Lemma holds with the index equal to $n-2$. Let $\epsilon := 1 + tp^{s+1}\lambda_{n-1}^{p^{n-1}-p^k}$. Note that $\epsilon = 1+tp^{s+1}\lambda_{n-2}^{p^{n-2}-p^{k-1}}$ and by the note before this proof, $\tilde{N}_{n-1,1}(\epsilon) = 1 + tp^{s+2}\lambda_{n-2}^{p^{n-2}-p^{k-1}}$. Let $(N_{n-1}(\epsilon) - 1)/p$ be represented by a pair $(a, b) \in \mathbb{Z}[\zeta_{n-2}] \times A_{n-2}$. Then $a = (\tilde{N}_{n-1,1}(\epsilon) - 1)/p = tp^{s+1}\lambda_{n-2}^{p^{n-2}-p^{k-1}}$. In $A_{n-2,1}$ a hence can be represented by a polynomial $a(x) = p^{s+1}(x-1)^{p^{n-2}-p^{k-1}}a_1(x)$ for some $a_1(x)$. By the expression for $\tilde{N}_{n-1,1}(\epsilon)$ and by the assumption, we get

$$b = \frac{N_{n-2}(\tilde{N}_{n-1,1}(\epsilon)) - 1}{p} = \frac{N_{n-2}(1 + tp^{s+2}\lambda_{n-2}^{p^{n-2}-p^{k-1}}) - 1}{p} = p^{s+1}b_1(x)$$

where $b_1(x) \equiv (x-1)^{p^{n-2}-p^{k-2}}b_2(x) \mod p$ for some $b_2(x)$. Define $b(x) := p^{s+1}b_1(x)$. We want to find a polynomial $f(x) \in A_{n-1}$ that represents (a, b), that is, maps to $a(x)$ and $b(x)$ in $A_{n-2,1}$ and A_{n-2} respectively. Note that

$$p = \frac{x^{p^{n-1}} - 1}{x^{p^{n-2}} - 1} + t(x)\frac{x^{p^{n-2}} - 1}{x - 1}$$

for some polynomial $t(x) \in \mathbb{Z}[x]$. Hence

$$a(x) - b(x) = \Big(\frac{x^{p^{n-1}} - 1}{x^{p^{n-2}} - 1} + t(x)\frac{x^{p^{n-2}} - 1}{x - 1}\Big)p^s((x-1)^{p^{n-2}-p^{k-1}}a_1(x) - b_1(x))$$

Then we can define a polynomial $f(x)$ by

$$\begin{aligned} f(x) : &= a(x) + p^s((x-1)^{p^{n-2}-p^{k-1}}a_1(x) - b_1(x))\frac{x^{p^{n-1}} - 1}{x^{p^{n-2}} - 1} = \\ &= b(x) + p^s((x-1)^{p^{n-2}-p^{k-1}}a_1(x) - b_1(x))t(x)\frac{x^{p^{n-2}} - 1}{x - 1}. \end{aligned}$$

Clearly, f maps to $a(x)$ and $b(x)$ respectively. We now finish the proof by observing that

$$\begin{aligned} f(x)/p^s &= p(x-1)^{p^{n-2}-p^{k-1}}a_1(x) + ((x-1)^{p^{n-2}-p^{k-1}}a_1(x) - b_1(x))\frac{x^{p^{n-1}} - 1}{x^{p^{n-2}} - 1} \equiv \\ &\equiv ((x-1)^{p^{n-2}-p^{k-1}}a_1(x) - (x-1)^{p^{n-2}-p^{k-2}}b_2(x))(x-1)^{p^{n-1}-p^{n-2}} = \\ &= (a_1(x) - (x-1)^{p^{k-1}-p^{k-2}}b_2(x))(x-1)^{p^{n-1}-p^{k-1}} \mod p. \end{aligned}$$

□

By setting $s = 0$ we in the lemma above we immediately get the following theorem.

Theorem 4.12. *Let $2 \leq n$ and $1 \leq k < n$. Suppose $\epsilon \in U_{n-1,p^n-p^k}$. Then $g_{n-1}((N_{n-1}(\epsilon)-1)/p) \equiv 0 \mod (x-1)^{p^{n-1}-p^{k-1}}$ in D_{n-1}*

The following proposition is immediate by using that $g_{n-1}N_{n-1} = f_{n-1}$.

Proposition 4.13. *Let $2 \leq n$, $1 \leq k < n$ and let $\epsilon \in U_{n-1,p^n-p^k} \setminus U_{n-1,p^n-p^{k-1}}$. Then $g_{n-1}((N_{n-1}((\epsilon-1)/p))) \equiv 0 \mod (x-1)^{p^{n-1}-p^k}$ but $g_{n-1}((N_{n-1}((\epsilon-1)/p))) \not\equiv 0 \mod (x-1)^{p^{n-1}-p^{k-1}}$ in D_{n-1}.*

Let $\omega : U_{n-1,p^n-p^{n-1}} \to D^+_{n-1}$ be defined by $\omega(\gamma) := g_{n-1}((N_{n-1}(\gamma)-1)/p)$.

Lemma 4.14. *ω is a homomorphism*

Proof. Suppose ϵ and γ belong to $U_{n-1,p^n-p^{n-1}}$. Then $N_{n-1}(\gamma) \equiv 1 \mod p$ in A_{n-1} because

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

and $\tilde{N}_{n-1,k}(\gamma) \equiv 1 \mod p^2$ for all $k = 1, 2, \ldots, n-1$. Hence

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

□

Note that if $\epsilon \in U_{n-1,p^n-1}$ then $\omega(\epsilon) = 0$. This can be shown using similar, but simpler, methods as we did in the proof of Lemma 4.11. We can hence define

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

Now, if $a \in D^+_{n-1}$, let $\mathcal{O}(a)$ be the maximal power of $(x - x^{-1})$ that devides a. In this language we can combine Thereom 4.12 and Proposition 4.13 to the following lemma.

Lemma 4.15. *Let $2 \leq n$, $1 \leq k < n$ and let $\epsilon \in U_{n-1,p^n-p^k} \setminus U_{n-1,p^n-p^{k-1}}$. Then $p^{n-1} - p^k \leq \mathcal{O}(\tilde{\varphi}(\epsilon)) < p^{n-1} - p^{k-1} \leq \mathcal{O}(\tilde{\omega}(\epsilon))$.*

Proposition 4.16. *The map $\tilde{\Phi} := \tilde{\varphi} - \tilde{\omega}$ is an isomorphism.*

Proof. By Proposition 4.9 φ is an isomorphism. Hence there exists (classes of) units $\epsilon_i, i = 1, 2, \ldots, (p^{n-1}-1)/2$ such that the set $\varphi(\epsilon_i)$ forms a basis for D^+_{n-1}. If $a \in D^+_{n-1}$ there exist unique a_i such that $a = \sum_{i=1}^{(p^{n-1}-1)/2} a_i\varphi(\epsilon_i)$. To prove the Proposition it is enough to show that the map

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

is invertible. Consider the matrix M for this map in the basis $\{(x - x^{-1})^{2j}\}$. Obviously this matrix can be written $I - M'$, where I is the identity matrix and M' is induced by $\varphi(\epsilon_i) \mapsto \omega(\epsilon_i)$. By Lemma 4.15 the matrix M' is a lower diagonal matrix with zeros on the diagonal. This means M is lower triangular with ones on the diagonal and hence invertible. □

Proof of Theorem 4.4. The map $\tilde{\Phi}$ is obviously induced by Φ which hence must be surjective by prop 4.16. □

5. Final remarks

We end this paper with some further discussion about how one can find a basis for the groups D^+_n. In the proof of Theorem 4.4 the main idea was that one could find a basis for D^+_n consisting of the image of certain elements from $\mathbb{Z}[\zeta_{n-2}]$ under a certain mapping. To be a bit more specific we can formulate this as a corollary to Proposition 4.9.

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

Recall that this was proved under the assumption $r_k = r(p)$ for all k. Now suppose that Assumption 1 holds instead. Then, by Lemma 3.7, $r_k = \lambda$ for $k = 1, 2, \ldots$ and $r_0 = r(p)$. From Theorem 3.7 and Ullom's result we conclude $\mathcal{V}^+_k$ has λ generators for all $k \geq 2$ and all of these generators have exponent at least p^{k-1}. In particular, $\mathcal{V}^+_k(p) \cong (\mathbb{Z}/p\mathbb{Z})^\lambda$ and hence coincides with $ker\,\pi_k$ by Proposition 3.10 and Lemma 3.6. Here for any abelian p-group A we denote by $A(p^k)$ the subgroup generated by all elements of A of exponent p^k.

It follows from the proof of Proposition 3.10 that there exist λ elements $a_i = 1 + (x_2 - x_2^{-1})^{p+s_i} \in \tilde{D}^{*+}_{2,(p+1)}$, $p^2 - p - 3 \geq s_i \geq 1$, which generate $\mathcal{V}^+_2(p)$ (see the proof of Proposition 3.10 for the definition of $\tilde{D}^{*+}_{k,(t)}$).

The natural projection $\tilde{D}^{*+}_{3,(p+1)} \to \tilde{D}^{*+}_{2,(p+1)}$. induces the following exact sequence $0 \to ker\,\pi_3 \to \mathcal{V}^+_3(p^2) \to \mathcal{V}^+_2(p) \to 0$ which reads as $0 \to (\mathbb{Z}/p\mathbb{Z})^\lambda \to (\mathbb{Z}/p^2\mathbb{Z})^\lambda \to$

$(\mathbb{Z}/p\mathbb{Z})^\lambda \to 0$. Let us consider elements $b_i = 1 + (x_3 - x_3^{-1})^{p+s_i} \in \tilde{D}^{*+}_{3,(p+1)}$. The commutativity of the diagram 4.1 implies that images of b_i are nontrivial in $\mathcal{V}_3^+$. Moreover, Proposition 3.10 implies again that b_i are not in $ker\,\pi_3$ and therefore all b_i have exponent p^2 and generate $\mathcal{V}_3^+(p^2)$. Thus, we can conclude that $b_i^p = 1 + (x_3 - x_3^{-1})^{p^2+ps_i}$ are not in the image of $\mathbb{Z}[\zeta_2]^*$.

On the other hand $p^3 - 3p \geq p^2 + ps_i \geq p^2 + p$ and b_i^p generate $\mathcal{V}_3^+(p) = ker\,\pi_3$.

It follows that

$$\left|\frac{U_{2,p^3-3p+2}}{U_{2,p^3-1}}\right| = p^{\frac{3p-3}{2}}$$

Proceeding in the same way we obtain the following

Lemma 5.2. *Let $n \geq 3$. If $a \in D^{*+}_{n,(p^n-3p^{n-2}+2)}$, then $a \in g_n(\mathbb{Z}[\zeta_{n-1}]^*)$.*

From this lemma, just as in the proof of Proposition 4.10, we get the following proposition.

Proposition 5.3. *Suppose Assumption 1 holds. Then*

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

Now define $\varphi_2 : U_{n,p^{n+1}-p^{n-1}} \to D^+_{n-1}$ by $\varphi_2(\gamma) = g_{n-1}(N_{n-1}(\frac{1}{p}\tilde{N}_{n-1,1}(\frac{\gamma-1}{p})))$. We remind the reader that $\tilde{N}_{n-1,1}$ is the usual norm $\mathbb{Z}[\zeta_n] \to \mathbb{Z}[\zeta_{n-1}]$ and $N_{n-1} : \mathbb{Z}[\zeta_{n-1}] \to A_{n-1}$ is our "standard" multiplicative map. One can easily check that φ_2 is a group homorphism. A straightforward calculation gives us that $\ker\varphi_2 = U_{n,p^{n+1}-1}$. We hence get an induced injective map

$$\tilde{\varphi}_2 : \frac{U_{n,p^{n+1}-p^{n-1}}}{U_{n,p^{n+1}-1}} \to D^+_{n-1}.$$

Since

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

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

Proposition 5.4. *Suppose Assumption 1 holds. Then $\varphi_2 : U_{n,p^{n+1}-p^{n-1}} \to D^+_{n-1}$ is an isomorphism and there exists a basis for D^+_{n-1} consisting of elements $\varphi_2(\gamma)$ where $\gamma \in U_{n,p^{n+1}-p^{n-1}}$.*

If we analyse the proof above we see that we really only require that $r_1 = r_2 = rank\,(\mathcal{V}_n^+)$, $n \geq 1$ ($rank\,(\mathcal{V}_n^+)$ is the number of generators of $\mathcal{V}_n^+$) for Proposition 5.4 to hold. We know from Proposition 3.6 that $r_N = r_{N+k}$ for some N and

if Assumption 2 is true, then $r_N = r_{N+k} = rank\,(\mathcal{V}^+_{N+k})$, $k \geq 0$. In this case it follows that we have the following exact sequence

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

and the following two statements are now straightforward.

Lemma 5.5. *Suppose Assumption 2 holds. Then* $\tilde{D}^{*+}_{n,(p^n-3p^{n-N}+2)} \subset g_n(\mathbb{Z}[\zeta_{n-1}]^*)$ *for* $n \geq N+1$.

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

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

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

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

Since

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

this map is surjective and we get the following proposition.

Proposition 5.6. *Suppose Assumption 2 holds. Let* N *be as in Proposition 3.6 and let* $n \geq N+1$. *Then there exists a basis for* D^+_{n-N} *consisting of elements* $\varphi_N(\gamma)$ *where* $\gamma \in U_{n,p^{n+1}-p^{n-N}}$.

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

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

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

References

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

[H-S] O. Helenius and A. Stolin, *On the Kervaire-Murthy Conjectures* Preprint, Chalmers University of Technology, 2000.

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

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

[ST1] Stolin, Alexander. *An Explicit Formula for the Picard Group of the Cyclic Group of Order p^2.*
Proceedings of the American Mathematical Society, Vol. 121 (1994), 375-383.

[ST2] Stolin, Alexander. *On the Picard Group of the Integer Group Ring of the Cyclic p-Group and Rings Close to It.*
Proc. of the 2nd Int. Conf in Comm. Alg. 1997, 443-455.

[ST3] Stolin, Alexander. *On the Picard Group of the Integer Group Ring of the Cyclic p-Group and Certain Galois Groups.*
Journal of Number Theory 72, 1998, 48-66.

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

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

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

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

E-mail address: olahe@math.chalmers.se, astolin@math.chalmers.se

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 assumptions 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 $\operatorname{Cl}^{(p)}\mathbb{Q}(\zeta_{n-1})$ 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 ζ_n be a primitive p^{n+1}-th root of unity. Kervaire and Murthy prove in [K-M] that there is an exact sequence

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

where

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

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

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

The numbers r_k are defined as $\log_p$ 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 λ_n^k where $\lambda_n = (\zeta_n - 1)$. We proved in [H-S] that r_n is non-decreasing sequence bounded by λ, where λ is one of the Iwasawa invariants for p.

Our main theorem is, as mentioned, the following.

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

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

Before we can prove this we need to recall some notation from [H-S]. Let for $k \geq 0$ and $l \geq 1$

$$A_{k,l} := \frac{\mathbb{Z}[x]}{\big(\frac{x^{p^{k+l}}-1}{x^{p^k}-1}\big)}$$

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

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

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

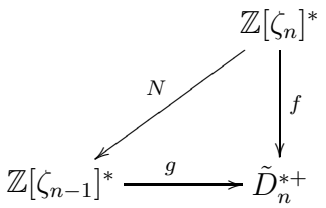
$$\mathcal{V}_n' := \frac{(\mathbb{F}_p[x]/(x^{p^n}-1))^*}{\operatorname{Im}\{\mathbb{Z}[\zeta_n]^* \to (\mathbb{F}_p[x]/(x^{p^n}-1))^*\}} \tag{2.3}$$

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



is commutative and N (which is the restriction of the usual norm-map) 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 λ_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 ι map λ_{n-1} to λ_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 α 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 α_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 λ_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]:

$$1)\ Gal^+(M_n/K_n) \cong Gal^+(M_n/L_n) \cong \mathcal{V}_n^+$$

$$2)\ M_{n-1} \cap K_n = K_{n-1}\,(\text{lemma } 4.4).$$

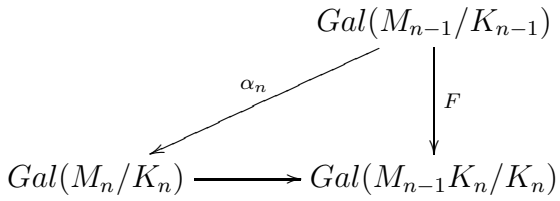
Obviously the field extension K_n/K_{n-1} induces a natural homomorphism

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

which we denote with some abuse of notations by α_n. Therefore it is sufficient to prove that the latter α_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 Φ'_{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:



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

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

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

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 φ_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 $U_{n,k,(p)} := \{real\,\epsilon \in \mathbb{Z}_p[\zeta_n]^* : \epsilon \equiv 1 \bmod \lambda_n^k\}$ and let us define φ'_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 γ 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 hence 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 $\mathcal{V}_{n+1}^+$. Recall that $\mathbb{Z}[\zeta_{n-1}]^*$ is identified with its image in A_n. We will now prove that the map $g_n : \mathbb{Z}[\zeta_{n-1}]^* \to D_n^*$ respects the filtrations λ_{n-1}^k and $(x-1)^k$.

Proposition 3.1. *Let $1 \le s \le p^n - 1$ and $\epsilon \in \mathbb{Z}[\zeta_{n-1}]^*$. Then $\epsilon \in U_{n-1,s}$ if and only if $g_n(\epsilon) \in D_{n,(s)}^*$.*

Using this Proposition we see that an element of $D^{*+}_{n+1,(2s)}$ which is non-trivial in $\mathcal{V}^+_{n+1}$ corresponds to a missed place $2s$ at level n.

Proof. To show that $g_n(\epsilon) \in D^*_{n,(s)}$ implies $\epsilon \in U_{n-1,s}$ we can use the same technique as in the proof of Theorem I.2.7 in [S3] (also see Lemma 2.6 [H-S]). For the other direction, first note that is $s \leq p^n - p^{n-1}$ the statement follows directly from the commutativity of the diagram

$$\begin{array}{ccc} A^*_n & \longrightarrow & \mathbb{Z}[\zeta_{n-1}]^{*+} \\ \Big\downarrow \text{mod } p & & \Big\downarrow \text{mod } p \\ D^*_n \cong \big(\frac{\mathbb{F}_p[x]}{(x-1)^{p^n-1}}\big)^* & \longrightarrow & \big(\frac{\mathbb{F}_p[x]}{(x-1)^{p^n-p^{n-1}}}\big)^* \end{array} \tag{3.1}$$

What is left to prove is that $\epsilon \in U_{n-1,s}$ implies $g_n(\epsilon) \in D^*_{n,(s)}$ also for $p^n - p^{n-1} \leq s \leq p^n - 1$. For technical reason we will prove that if $\epsilon \in U_{n-1,p^n-p^k+r}$ for some $1 \leq k \leq n-1$ and $0 \leq r \leq p^k - p^{k-1}$ then $g_n(\epsilon) \in D^*_{n,(p^n-p^k+r)}$. Note that $\epsilon \in U_{n-1,p^n-1}$ is equivalent to $g_n(\epsilon) = 1 \in D^*_n$ by Lemma 2.6 of [H-S]. Suppose $\epsilon = 1 + t\lambda_{n-1}^{p^n-p^k+r}$ for some $t \in \mathbb{Z}[\zeta_{n-1}]$. By Lemma 4.11 of [H-S] we get $N_{n-1}(\epsilon) = 1 + t'p(x-1)^{p^{n-1}-p^{k-1}}$ for some $t' \in A_{n-1}$. In A_n,

$$p = \frac{x^{p^n}-1}{x^{p^{n-1}}-1} + t(x)\frac{x^{p^{n-1}}-1}{x-1}$$

for some polynomial $t(x)$. In A_n consider the element

$$p(t(x-1)^{p^{n-1}-p^k+r} - t'(x-1)^{p^{n-1}-p^{k-1}}) =$$
$$= \big(\frac{x^{p^n}-1}{x^{p^{n-1}}-1} + t(x)\frac{x^{p^{n-1}}-1}{x-1}\big)(t(x-1)^{p^{n-1}-p^k+r} - t'(x-1)^{p^{n-1}-p^{k-1}}).$$

By computing the right hand side and re-arrange the terms we get

$$f := tp(x-1)^{p^{n-1}-p^k+r} - \big(t(x-1)^{p^{n-1}-p^k+r} - t'(x-1)^{p^{n-1}-p^{k-1}}\big)\frac{x^{p^n}-1}{x^{p^{n-1}}-1} =$$
$$= t'(x-1)^{p^{n-1}-p^{k-1}} - b(x)\frac{x^{p^{n-1}}-1}{x-1}.$$

Using the two representations of f we see that $i_n(1+f) = \epsilon$ and $j_n(1+f) = N_{n-1}(\epsilon)$ so $1+f$ represents $(\epsilon, N_{n-1}(\epsilon))$ (which represents ϵ under our usual identification) in A_n. Since $\leq p^k - p^{k-1}$ we now get $g_n(1+f) \equiv 1 \bmod (x-1)^{p^{n-1}-p^k+r}$ in D_n as asserted. □

Theorem 2.1 and its proof now give us specific information about the missed places which we will formulate in a Theorem below. We start with a simple lemma.

Lemma 3.2. *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, ϵ is real and since

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

ϵ 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 3.3. *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 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. As in Proposition 4.7 of [H-S] an induction argument using the map π_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 and that a missed place k at level $n-1$ lift to missed places k and pk at level n. What is left to prove is that the "new" missed places we get when we go from level $n-1$ to n all end up in the n-strip and that no "new" missed places are divisible by p. 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 $a_l = 1 + t(x_{n+1} - 1)^s$, $t \neq 0$, $s < p^n - 1$, is a "new" generator. Then $\pi_{n+1}(a_l) = 1 + t(x_n - 1)^s$ is neccesarily trivial in $\mathcal{V}_n^+$ but not in D_n^{*+}. Hence $\pi_{n+1}(a_l) = g_n(\epsilon)$ for some $\epsilon \in \mathbb{Z}[\zeta_{n-1}]^*$.

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 $b \in \ker\{\tilde{D}^{*+}_{n+1} \to \tilde{D}^{*+}_n\} = \tilde{D}^{*+}_{n+1}(p^n - 1)$. 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 no "new" missed places are divisible by p we need to show 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 $k \notin \{i_1, \ldots, i_{r_{n-1}}\}$ 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 α_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* $\mathrm{Cl}\,\mathbb{Q}(\zeta_{n-1})(p) \to Char(\mathcal{V}^+_n)$.

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)
$$\begin{array}{ccc} A_{n,(p)} & \xrightarrow{i_n} & \mathbb{Z}_p[\zeta_{n-1}] \\ \downarrow{\scriptstyle j_n} & \swarrow{\scriptstyle N_{n-1}} & \downarrow{\scriptstyle f_{n-1}} \\ A_{n-1,(p)} & \xrightarrow{g_{n-1}} & D_{n-1} \end{array}$$

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 ω 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

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

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 α be an ideal in $\mathbb{Z}[\zeta_{n-1}]$ co-prime to λ_{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 α in $\mathrm{Cl}\,\mathbb{Q}(\zeta_{n-1})(p)$ because if we use $r\alpha$ instead of α 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 α^p, which is 1 modulo λ_{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 γ is either real or $\gamma = \zeta_{n-1}^{pk}\gamma_1$ with a real unit γ_1. Hence we must consider $\tau_{\gamma q}(v)$ for real γ. 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 γ are real, while ζ_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 γ 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 remify in the λ_{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 λ_{n-1}.

Let us 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 γ. Kummer's theory says that $q = \gamma r^p$ and then obviously $\alpha = (r)$, i.e. α is a principal ideal. So, it remains to prove that the case $k = p^n - 1$ is impossible. For this consider ζ_{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 ζ_{n-1} is a unit and the extension $K_{n-1}(q^{1/p})/K_{n-1}$ is unramified in ω. 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 α and all the q_i which generate all α^{ps} for non-trivial α^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 σ 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 α^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 η_{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* ϵ *is a unit satisfying* $\epsilon = 1 + \lambda_{n-1}^{p^n+1}t$.

Corollary 4.5. *There exists an integer* N *such that* $r_k = \lambda$ *for* $k > N$ *(here* λ *is the Iwasawa invariant for* p*). Moreover, any unramified extension of* $\mathbb{Q}(\zeta_k) = K_k$

of degree p is of the form $K_k(\epsilon^{1/p})/K_k$, where $\epsilon \in \mathbb{Z}[\zeta_N]^*$ is a unit satisfying $\epsilon = 1 + \lambda_N^{p^{N+1}+1}t$.

Finally we obtain Kummer's Lemma for semiregular primes

Corollary 4.6. *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 γ, γ_1 and $\gamma_1 \equiv 1 \, mod \, \lambda_{n-1}^{p^n+1}$.*

Proof. If $\epsilon \equiv r^p \bmod \lambda_{n-1}^{p^n-1}$ then $r^{-p}\epsilon \equiv 1 \bmod \lambda_{n-1}^{p^n-1}$ and it follows from the proof of the theorem that in fact $r^{-p}\epsilon \equiv 1 \bmod \lambda_{n-1}^{p^n}$. Then the extension $K_{n-1}(\epsilon^{1/p})/K_{n-1}$ is unramified and therefore $\epsilon = \gamma^p\gamma_1$, where $\gamma_1 \equiv 1 \bmod \lambda_{n-1}^{p^n+1}$. Clearly, then γ is a unit. □

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.

[S3] Stolin, Alexander. *On the Picard Group of the Integer Group Ring of the Cyclic p-Group and Certain Galois Groups.*
Journal of Number Theory 72, 1998, 48-66.

[U] Ullom, S. *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

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

$$V_n^- \cong C_{p^n}^{\frac{p-3}{2}} \times \prod_{j=1}^{n-1} C_{p^j}^{\frac{(p-1)^2 p^{n-1-j}}{2}}. \tag{1.2}$$

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

$$V_n^+ \cong (\frac{\mathbb{Z}}{p^n\mathbb{Z}})^{r(p)} \oplus (\frac{\mathbb{Z}}{p^{n-1}\mathbb{Z}})^{\lambda - r(p)}, \tag{1.3}$$

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

(1.4)
$$\begin{array}{ccc} A_{k,l+1} & \xrightarrow{i_{k,l+1}} & \mathbb{Z}[\zeta_{k+l}] \\ \downarrow{\scriptstyle j_{k,l+1}} & \swarrow{\scriptstyle N_{k,l}} & \downarrow{\scriptstyle f_{k,l}} \\ A_{k,l} & \xrightarrow{g_{k,l}} & D_{k,l} \end{array}$$

where $i_{k,l+1}(x_{k,l+1}) = \zeta_{k+l}$, $j_{k,l+1}(x_{k,l+1}) = x_{k,l}$, $f_{k,l}(\zeta_{k+l}) = \bar{x}_{k,l}$ and $g_{k,l}$ is just taking classes modulo p. The 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 1.4 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

$$0 \to V_{k,l} \to \operatorname{Pic} A_{k,l+1} \to \operatorname{Cl} \mathbb{Z}[\zeta_{k+l}] \times \operatorname{Pic} A_{k,l} \to 0. \tag{1.5}$$

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 1.4, 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

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

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 1.4 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

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

□

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 do 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 $(\bar{x}_{k,l} - \bar{x}_{k,l}^{-1})^s$.

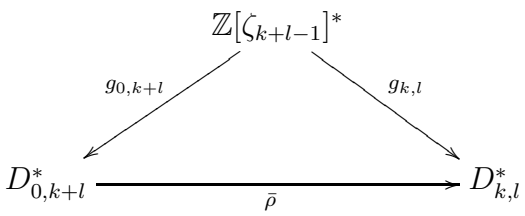
Proof. By using the identifications

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

and

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

we get a commutative diagram



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 the proof of Proposition 4.10 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

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

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

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

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

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

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

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

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

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

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

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

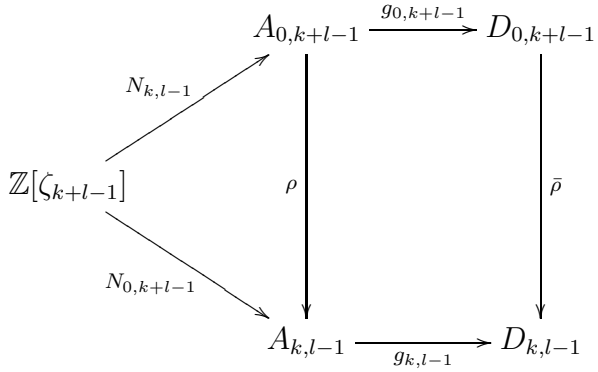
As before one can show that $\omega_{0,n-1}$ is a group homomorphism and that we get an induced map $\tilde{\omega}_{0,n-1} : (U_{0,p^n-p^{n-1}})/(U_{0,p^n+1}) \to D_{0,n-1}^+$ Since $\tilde{\varphi}_{0,n-1}$ is an isomorphism we can find units $\{\epsilon_i\} \subset U_{0,p^n-p^{n-1}}$ such that $\{\tilde{\varphi}_{0,n-1}(\epsilon_i)\}$ 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)



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 1.5. 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