FINE STRUCTURE OF CLASS GROUPS $\mathrm{Cl}^{(p)}\mathbb{Q}(\zeta_n)$ AND THE KERVAIRE–MURTHY CONJECTURES II

OLA HELENIUS AND ALEXANDER STOLIN

ABSTRACT. There is an Mayer-Vietoris exact sequence

$$0 \to V_n \to \mathrm{Pic}\,\mathbb{Z}C_{p^n} \to \mathrm{Cl}\,\mathbb{Q}(\zeta_{n-1}) \times \mathrm{Pic}\,\mathbb{Z}C_{p^{n-1}} \to 0$$

involving the Picard group of the integer group ring $\mathbb{Z}C_{p^n}$ where C_{p^n} is the cyclic group of order p^n and ζ_{n-1} is a primitive p^n-th root of unity. The group V_n splits as $V_n \cong V_n^+ \oplus V_n^-$ and V_n^- is explicitly known. V_n^+ is a quotient of an in some sense simpler group $\mathcal{V}_n$. In 1977 Kervaire and Murthy conjectured that for semi-regular primes p, $V_n^+ \cong \mathcal{V}_n^+ \cong \mathrm{Cl}^{(p)}(\mathbb{Q}(\zeta_{n-1})) \cong (\mathbb{Z}/p^n\mathbb{Z})^{r(p)}$, where $r(p)$ is the index of regularity of p. Under an extra condition on the prime p, Ullom calculated V_n^+ in 1978 in terms of the Iwasawa invariant λ as $V_n^+ \cong (\mathbb{Z}/p^n\mathbb{Z})^{r(p)} \oplus (\mathbb{Z}/p^{n-1}\mathbb{Z})^{\lambda - r(p)}$.

In the previous paper we proved that for all semi-regular primes, $\mathcal{V}_n^+ \cong \mathrm{Cl}^{(p)}(\mathbb{Q}(\zeta_{n-1}))$ and that these groups are isomorphic to

$$(\mathbb{Z}/p^n\mathbb{Z})^{r_0} \oplus (\mathbb{Z}/p^{n-1}\mathbb{Z})^{r_1 - r_0} \oplus \ldots \oplus (\mathbb{Z}/p\mathbb{Z})^{r_{n-1} - r_{n-2}}$$

for a certain sequence $\{r_k\}$ (where $r_0 = r(p)$). Under Ulloms extra condition it was proved that

$$V_n^+ \cong \mathcal{V}_n^+ \cong \mathrm{Cl}^{(p)}(\mathbb{Q}(\zeta_{n-1})) \cong (\mathbb{Z}/p^n\mathbb{Z})^{r(p)} \oplus (\mathbb{Z}/p^{n-1}\mathbb{Z})^{\lambda - r(p)}.$$

In the present paper we prove that Ullom's extra condition is valid for all semi-regular primes and it is hence shown that the above result holds for all semi-regular primes.

The present paper is a continuation of the paper [H-S] of the authors and we refer you there for a more thorough introduction.

Let p be an odd prime, C_{p^n} denote the cyclic group of order p^n and let ζ_n be a primitive p^{n+1}-th root of unity. In this paper we work on problems related to $\mathrm{Pic}(\mathbb{Z}C_{p^n})$. Our methods also lead to the calculation of the p-part of the ideal class group of $\mathbb{Z}[\zeta_n]$. Recall that calculating Picard groups for a group ring like the one above is equivalent to calculating K_0 groups.

There is a well known exact sequence involving the Picard group of $\mathbb{Z}C_{p^n}$ which was for example presented by Kervaire and Murthy in [K-M]. The sequence,

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

which is based on the $(*, \mathrm{Pic})$-Mayer-Vietoris exact sequence associated to a certain pullback of rings, reads

$$0 \to V_n \to \operatorname{Pic} \mathbb{Z}C_{p^{n+1}} \to \operatorname{Pic} \mathbb{Z}C_{p^n} \times \operatorname{Cl} \mathbb{Q}(\zeta_n) \to 0. \tag{0.1}$$

In [H-S] we observe that $\operatorname{Pic}(\mathbb{Z}C_{p^n}) \cong \operatorname{Pic} A_n$, where

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

We look at the pullback

$$\begin{array}{ccc} A_{n+1} & \xrightarrow{i_{n+1}} & \mathbb{Z}[\zeta_n] \\ \downarrow{\scriptstyle j_{n+1}} & \swarrow{\scriptstyle N_n} & \downarrow{\scriptstyle f_n} \\ A_n & \xrightarrow{g_n} & \frac{A_n}{pA_n} =: D_n \end{array} \tag{0.2}$$

where the map N_n is constructed so that the lower right triangle of the diagram is commutative. From this we get an exact sequence equivalent to 0.1 where V_n can be represented as

$$V_n = \frac{D_n^*}{g_n(A_n^*)}.$$

Here R^* denotes the group of units in a ring R. Using 0.2 and the map N_n we can construct an embedding of $\mathbb{Z}[\zeta_{n-1}]^*$ into A_n^* which we by abuse of notation consider an identification. This allows us to define

$$\mathcal{V}_n := \frac{D_n^*}{g_n(\mathbb{Z}[\zeta_{n-1}]^*)}.$$

There is an action of $G_n := \operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ on all involved groups so we can use complex conjugation c and for each involved (multiplicative) group G define G^+ and G^- as the subgroups invariant $(c(g) = g)$ respectively anti-invariant $(c(g) = g^{-1})$ under c. Since both V_n and $\mathcal{V}_n$ are p-groups and c is even we get a splitting $V_n = V_n^+ \oplus V_n^-$ and $\mathcal{V}_n = \mathcal{V}_n^+ \oplus \mathcal{V}_n^-$. It turns out that $\mathcal{V}_n^+$ is isomorphic to its counterpart in [K-M] (also denoted by $\mathcal{V}_n^+$).

Recall that a prime p is semi-regular when p does not divide the order of the ideal class group of the maximal real subfield $\mathbb{Q}(\zeta_0 + \zeta_0^{-1})$ of $\mathbb{Q}(\zeta_0)$. A non semi-regular prime has yet to be found and it is an old conjecture by Vandiver that all primes are semi-regular. We also recall that the index of regularity $r(p)$ is defined as the number of Bernoulli numbers $B_2, B_4, \ldots, B_{p-3}$ with numerators (in reduced form) divisible by p. Kervaire and Murthy conjecture in [K-M] that for semi-regular

primes:

$$V_n^+ = \mathcal{V}_n^+ \tag{0.3}$$

$$\operatorname{Char} \mathcal{V}_n^+ = \operatorname{Cl}^{(p)} \mathbb{Q}(\zeta_{n-1}) \tag{0.4}$$

$$\operatorname{Char} V_n^+ \cong \left(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\right)^{r(p)}, \tag{0.5}$$

Results mainly from Iwasawa show that for big enough n,

$$|\operatorname{Cl}^{(p)}(\mathbb{Q}(\zeta_n)| = p^{\lambda n+\nu}$$

and the constants λ and ν are called Iwasawa invariants. Resulting from as splitting of $\operatorname{Cl}^{(p)}(\mathbb{Q}(\zeta_0))$ with respect to idempotents there are also an Iwasawa invariants λ_i for each component e_iS_n of $S_n = \operatorname{Cl}^{(p)}(\mathbb{Q}(\zeta_n)$. In 1978 Ullom showed in [U] that if each λ_{1-i} satisfy $1 \leq \lambda_{1-i} \leq p-1$, then

$$V_n^+ \cong \left(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\right)^{r(p)} \oplus \left(\frac{\mathbb{Z}}{p^{n-1}\mathbb{Z}}\right)^{\lambda - r(p)}. \tag{0.6}$$

In our previous paper [H-S] we prove a number of results regarding the Kervaire–Murthy conjectures. Before presenting them we need a some definitions. For $n \geq 0$ and $k \geq 0$, define

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

where $\lambda_n = (\zeta_n - 1)$ is the prime above (p) in $\mathbb{Z}[\zeta_n]$. Let U^p denote the group of p-th powers of elements of the group U. Note that we in this paper sometimes use the notation R^n for n copies of the ring (or group) R. The context will make it clear which one of these two things we mean. Similarly the context should make it clear wether an indexed λ means an Iwasawa invariant or a prime ideal.

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

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

It turns out that $r_0 = r(p)$ (see for example [B-S]). Our main results from [H-S] are:

Theorem 0.1. *For semi regular primes,*

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

If Ulloms assumption holds, then $r_k = \lambda$ for all $k \geq 1$, $\nu = r(p) = r(0)$ and

$$\operatorname{Char} V_n^+ \cong \operatorname{Char} \mathcal{V}_n^+ \cong \operatorname{Cl}^{(p)} \mathbb{Q}(\zeta_{n-1}) \cong \left(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\right)^{r(p)} \oplus \left(\frac{\mathbb{Z}}{p^{n-1}\mathbb{Z}}\right)^{\lambda - r(p)}. \tag{0.7}$$

Moreover, $\lambda = r(p)$ is equivalent to that all three Kervaire–Murthy conjectures hold and if λ equals r(p), then ν equals $r(p)$.

In the present paper we prove that Ulloms assumption on the Iwasawa invariants λ_{1-i} above is true for all semi-regular primes. Before we can explain exactly what we prove we need some more notation. We remind the reader that S_n denotes the p-part of the ideal class group of $\mathbb{Q}(\zeta_n)$. One can find a set of mutually orthagonal idempotents, ϵ_i, such that $S_n = \bigoplus \epsilon_i S_n$. In [W] it was proved that

$$\epsilon_i S_n \cong \frac{\mathbb{Z}_p[[T]]}{((1+T)^{p^n}-1, f_i(T))},$$

where $f_i(T) = a_0 + a_1 T + a_2 T^2 + \ldots$ is a power series satisfying $f_i((1+p)^s - 1) = L_p(s, \omega^{1-i})$. Here $L_p(s,\chi)$ is the p-adic L-function with a Dirichlet character χ defined for instance in [W] and $\omega(a)$ is a p-adic Dirichlet character of conductor $p-1$.

For the constant term we have $a_0 = -B_{1,\omega^{-i}} = L_p(0, \omega^{1-i})$, where B_{1,ω^i} is a generalized Bernoulli number (again, see [W]).

The Iwasawa invariants λ_i turn out to be the first exponent such that $p \not| a_{\lambda_i}$. Let $\mathcal{O}$ be a finite extension of $\mathbb{Z}_p$ and $\mathcal{M}$ its maximal ideal. A polynomial $h \in \mathcal{O}[T]$ is called distinguished if it has leading coefficient 1 and all other coefficients belong to $\mathcal{M}$. It is known (see for instance Proposition 7.2 in [W]) that for a distinguished polynomial h,

$$\frac{\mathcal{O}[[T]]}{(h(T))} \cong \frac{\mathcal{O}[T]}{(h(T))}.$$

In our case, using Weierstrass preparation theorem one can find a distinguished polynomial

$$g_i(T) = a_0' + a_1' T + \ldots + a_{\lambda_{i-1}}' T^{\lambda_{i-1}} + T^{\lambda_i}$$

and an invertible series $u_i(T)$ such that $f_i(T) = g_i(T) u_i(T)$. This representation is unique. Using this we get

$$\epsilon_i S_n \cong \frac{\mathbb{Z}_p[[T]]}{((1+T)^{p^n}-1, g_i(T))} \cong \frac{\mathbb{Z}_p[T]}{((1+T)^{p^n}-1, g_i(T))}.$$

Recall that we are interested in evaluating λ_i. First, for $n = 0$ we get that

$$\epsilon_i S_0 \cong \frac{\mathbb{Z}_p[T]}{(T, g_i(T))} \cong \frac{\mathbb{Z}_p}{(a_0)} \cong \frac{\mathbb{Z}_p}{(a_0')}.$$

From our previous results on S_n we know that $\epsilon_i S_n \cong \mathbb{Z}/p\mathbb{Z}$, so $a_0' = pu$ for some unit $u \in \mathbb{Z}_p$. Hence g_i is an Eisenstein polynomial and hence irreducible. Now consider the case $n = 1$. We get

$$\epsilon_i S_1 \cong \frac{\mathbb{Z}_p[T]}{((1+T)^{p}-1, g_i(T))}.$$

Choose β_i such that $g_i(\beta_i) = 0$. Then,

$$\epsilon_i S_1 \cong \frac{\mathbb{Z}_p[\beta_i]}{((1+\beta_i)^p - 1)}.$$

Suppose $\lambda_i \geq p$. The field $\mathbb{Q}_p(\beta_i)$ completely remifies over $\mathbb{Q}_p$ and has degree λ_i. Therefore $(\beta_i)^{\lambda_i} = (p)$ and we see that $(1+\beta_i)^p - 1 = u\beta_i^p$ for some unit $u \in \mathbb{Z}_p[\beta_i]$. Then we get that

$$\frac{\mathbb{Z}_p[\beta_i]}{((1+\beta_i)^p - 1)} = \frac{\mathbb{Z}_p[\beta_i]}{(\beta_i^p)}$$

and multiplication by p annihilates this factor-ring. Therefore for some k we have:

$$\frac{\mathbb{Z}_p[\beta_i]}{((1+\beta_i)^p - 1)} \cong (\mathbb{Z}/p\mathbb{Z})^k.$$

So, if we deduce from our previous results that there are elements of order p^2 in $\epsilon_i S_1$, it will contradict to the assumption that $\lambda_i \geq p$. We will hence prove the following two theorems.

Theorem 0.2. *Let p be a semi-regular prime and let g_i be the distinguished polynomial defined above, with a_0' being the constant coefficient. Then we have*

(1) $p^2 \not| a_0'$
(2) $g_i(T)$ *is an Eisenstein polynomial of degree strictly less than p.*

Theorem 0.3. *For semi-regular primes,*

(1) λ_{1-i} *satisfy* $1 \leq \lambda_{1-i} \leq p-1$.
(2) $r_k = \lambda$ *for all* $k = 1, 2, 3 \ldots$.
(3) $V_n^+ \cong \mathcal{V}_n^+ \cong \text{Char } S_{n-1} \cong \left(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\right)^{r(p)} \oplus \left(\frac{\mathbb{Z}}{p^{n-1}\mathbb{Z}}\right)^{\lambda - r(p)}$

Remark. The above yields for semi-regular p that $\nu = r(p)$.

Let us recall that

$$S_1 \cong (\mathbb{Z}/p^2\mathbb{Z})^{r(p)} \oplus (\mathbb{Z}/p\mathbb{Z})^{r_1 - r(p)}$$

The usual norm map induces an epimorphism $N : S_1 \to S_0$.

Proposition 0.4.

$$\ker N \cong (\mathbb{Z}/p\mathbb{Z})^{r_1}$$

Proof. Let A be any finite abelian group and let us denote by $\text{Char } A$ or $A^\times$ the group of its characters. Clearly any homomorphism $f : A \to B$ induces a dual homomorphism $f^* : B^\times \to A^\times$.

In the proof of Theorem 2.14 in [H-S] we constructed an embedding $\alpha_1 : \mathcal{V}_0^+ \cong S_0^\times \to S_1^\times \cong \mathcal{V}_1^+$. The map α_1 is induced by the canonical embedding $\mathbb{Q}(\zeta_0) \to \mathbb{Q}(\zeta_1)$ and then clearly $N^* = \alpha_1$. Then we get that

$$\ker N \cong \mathrm{Char}\, \frac{\mathcal{V}_1^+}{\mathrm{Im}(\alpha_1)}$$

Therefore we have to prove that

$$\frac{\mathcal{V}_1^+}{\mathrm{Im}(\alpha_1)} \cong (\mathbb{Z}/p\mathbb{Z})^{r_1}$$

For this we recall that we also have a surjection $\pi_1 : \mathcal{V}_1^+ \to \mathcal{V}_0^+$ [Proposition 2.12, H-S]. Moreover, it was proved in the proof of Theorem 2.14 in [H-S] that $\alpha_1(\pi_1(a)) = a^p$ for any $a \in \mathcal{V}_1^+$. The latter implies that

$$\frac{\mathcal{V}_1^+}{\mathrm{Im}(\alpha_1)} = \frac{\mathcal{V}_1^+}{(\mathcal{V}_1^+)^p} \cong (\mathbb{Z}/p\mathbb{Z})^{r_1}$$

□

Corollary 0.5. *$\epsilon_i S_1$ contains elements of order p^2.*

Proof. It is known that N maps $\epsilon_i S_1$ onto $\epsilon_i S_0$ (see for instance [W]). Since S_1 has r_1 generators and $\ker N \cong (\mathbb{Z}/p\mathbb{Z})^{r_1}$ it follows that any preimage of non-zero $a \in S_0$ has order p^2 and hence, $\epsilon_i S_1$ contains an element of order p^2. This completes the proofs of Corrolary 0.5 and Theorems 0.2, 0.3. □

Final Remark. The following result was proved in [W].

Theorem 0.6. *Suppose p is semi-regular. Let an even index i be such that $2 \le i \le p-3$ and $p|B_i$ (B_i is the corresponding ordinary Bernoulli number). If*

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

and

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

then for all $n \ge 0$

$$S_n \cong (\mathbb{Z}/p^{n+1}\mathbb{Z})^{r(p)}$$

For semi-regular p the above yields

$$\lambda = \nu = r(p)$$

It was written in a remark after the result that the above incongruences hold for all $p < 4000000$ but there does not seem to be any reason to believe this in general.

Our results show that the first incongruence is valid for all semi-regular primes as well as $\nu = r(p)$. So we may hope that the second incongruence above obtained numerically also is valid in some generality.

References

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

[C-F] Cassels, J. W. S. and Fröhlich, A., *Algebraic Number Theory,*
Academic Press, London and New York, 1967.

[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-S1] O. Helenius and A. Stolin, *On the Kervaire–Murthy Conjectures*
Preprint, Chalmers University of Technology, 2000 (to be published in Rocky Mountain J. Math).

[H-S] O. Helenius and A. Stolin, *Fine Structure of Class Groups* $\mathrm{Cl}^{(p)}\,\mathbb{Q}(\zeta_n)$ *and the Kervaire–Murthy Conjectures* Preprint, Chalmers University of Technology, 2002, math.NT/0207286.

[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. 1971.

[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. *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

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