ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 31, Number 2, Summer 2001

CYCLOTOMIC SWAN SUBGROUPS AND IRREGULAR INDICES

DANIEL R. REPLOGLE

ABSTRACT. Let p be an odd prime, ζ_p a primitive pth root of unity and $\mathbf{Q}$ the field of rational numbers. For $K = \mathbf{Q}(\zeta_p)$, the ring of algebraic integers is $\mathbf{Z}[\zeta_p]$. Let C_m denote the cyclic group of order m and C_m^n denote the direct sum of n copies of C_m. Under the assumption p satisfies Vandiever's conjecture $T(\mathbf{Z}[\zeta_p]C_p)$, the Swan subgroup of the classgroup $\mathrm{Cl}\,(\mathbf{Z}[\zeta_p]C_p)$, is isomorphic to $C_p^{((p-3)/2)+s}$ where s is the number of irregular indices of p. Hence the group of realizable classes contains a subgroup isomorphic to $C_p^{((p-3)/2)+s}$.

1. Introduction and $T(\mathcal{O}_K[C_p])$. Let $\mathcal{O}_K$ be the ring of integers of an algebraic number field K, and let G be a finite group. The order $\mathcal{O}_K[G]$ in the group algebra $K[G]$ will be denoted Λ, and the locally free class group of Λ will be denoted $\mathrm{Cl}\,(\Lambda)$. There are several interesting subgroups of $\mathrm{Cl}\,(\Lambda)$ one studies in relative Galois module theory. The simplest to describe is the kernel group $D(\Lambda)$; this is the subgroup consisting of those classes in $\mathrm{Cl}\,(\Lambda)$ that become trivial upon extension of scalars to the maximal $\mathcal{O}_K$-order in $K[G]$ containing Λ. In [**14**] Ullom studied a subgroup $T(\Lambda)$, the Swan subgroup of $D(\Lambda)$, consisting of classes of Swan modules. Let n be the order of G and let $\Sigma = \sum_{g\in G} g$. Then for each $s \in \mathcal{O}_K$ so that s and n are relatively prime, define the Swan module $\langle s, \Sigma\rangle$ by $\langle s, \Sigma\rangle = s\Lambda + \Lambda\Sigma$. These Swan modules are rank one locally free Λ-modules and hence determine classes in $\mathrm{Cl}\,(\Lambda)$. Let $\overline{\mathcal{O}_K} = \mathcal{O}_K/n\mathcal{O}_K$ and $\mathrm{Im}\,(\mathcal{O}_K^*)$ denote the image of $\mathcal{O}_K^*$ in $\overline{\mathcal{O}_K}$. Let $\varepsilon : \Lambda \to \mathcal{O}_K$ denote the augmentation map. With this, define $\Gamma = \Lambda/(\Sigma)$ and let $\bar{\varepsilon} : \Gamma \to \overline{\mathcal{O}_K}$ be induced from ε. Last, for any ring S, let S^* be its group of multiplicative units. The major result of [**8**] shows if $K[G]$ satisfies an Eichler condition (see [**1**] or [**8**] and note this holds in particular if G is abelian), there is an exact Mayer-Veitoris sequence:

$$\mathcal{O}_K^* \times \Gamma^* \xrightarrow{h} \overline{\mathcal{O}_K}^* \xrightarrow{\delta} D(\Lambda) \longrightarrow D(\mathcal{O}_K) \oplus D(\Gamma) \longrightarrow 0.$$

Received by the editors on June 9, 1999, and in revised form on March 13, 2000.

From [**8**] and [**14**] we have the following. The map h is given by $(u,v) \mapsto \bar{u} \cdot \bar{\varepsilon}(v)^{-1}$, and δ is given by $\delta(u) = [u, \Sigma]$, the class of $\langle u, \Sigma \rangle$. Hence, $T(\Lambda)$ is a subgroup of $D(\Lambda)$ and

$$T(\Lambda) \cong \overline{\mathcal{O}_K}^* / h(\mathcal{O}_K^* \times \Gamma^*). \tag{1}$$

The last subgroup of $\mathrm{Cl}\,(\Lambda)$ we consider is the group of realizable classes. A classical result due to Noether states that L/K is a tame (i.e., at most tamely ramified) Galois extension of number fields with Galois group $\mathrm{Gal}\,(L/K) \cong G$ if and only if $\mathcal{O}_L$ is a locally free Λ-module. Hence, for L/K a tame extension $\mathcal{O}_L$ determines a "Galois module class" $[\mathcal{O}_L]$ in the classgroup $\mathrm{Cl}\,(\Lambda)$. We shall denote the set of tame Galois module classes in $\mathrm{Cl}\,(\Lambda)$ by $R(\Lambda, K)$ to emphasize the dependence on the field K. One refers to the elements of $R(\Lambda, K)$ as realizable classes. McCulloh shows $R(\Lambda, K)$ is a subgroup of $\mathrm{Cl}\,(\Lambda)$ for all finite abelian G, [**7**]. For G p-elementary abelian, p prime, he gives a convenient explicit description of $R(\Lambda, K)$ in [**6**].

Of course from an algebraic number theoretic perspective, it is this last subgroup which is of the most interest. One method of studying $R(\Lambda, K)$ comes from the relationship between $R(\Lambda, K)$, $D(\Lambda)$ and $T(\Lambda)$ from [**2**, Proposition 4], which we state for the case we will consider. Let $T^w(\Lambda)$ denote those classes of $T(\Lambda)$ which are expressible as wth powers.

Theorem (cf. [**2**, Proposition 4]). *For G cyclic of order $p > 2$, p prime, and K an algebraic number field, let $R(\Lambda, K)$, $T(\Lambda)$ and $D(\Lambda)$ be as above. Then $T^{(p-1)/2}(\Lambda) \subseteq R(\Lambda, K) \cap D(\Lambda)$.*

If we restrict ourselves to when K contains the pth roots of unity and G cyclic order p, this is in [**9**] and [**10**] using [**5**]. We see by the theorem of [**2**] computing $T(\Lambda)$, or at least achieving a nontrivial lower bound, allows one to obtain nontrivial lower bounds on $R(\Lambda, K) \cap D(\Lambda)$. Let $\mathbf{Q}$ and $\mathbf{Z}$ denote the field of rational numbers and the ring of (rational) integers, respectively. In this article we explicitly compute $T(\Lambda)$ for $K = \mathbf{Q}(\zeta_p)$ and $G \cong C_p$ when p satisfies Vandiver's conjecture, proving the following result of [**9**].

Theorem 1. *Let p be an odd prime satisfying Vandiver's conjecture. The group $T(\mathbf{Z}[\zeta_p]C_p)$ is isomorphic to $C_p^{((p-3)/2)+s}$ where s is the index of irregularity of the prime p. Hence $R(\Lambda, K) \cap D(\Lambda)$ contains such a subgroup.*

This result has been generalized to an analogous result that holds for all primes p and all $\mathcal{O}_K$, K a real subfield of $\mathbf{Q}(\zeta_p)$, in [**12**]. The proof in [**12**] uses p-adic L-functions much more extensively and does not mention a connection to irregular indices. The results in [**12**] in fact characterize $T(\Lambda)$ as a $\mathbf{Z}_p H$-module for H the character group of G for all real subfields of cyclotomic fields of prime conductor. For other results employing the method of bounding $R(\Lambda, K) \cap D(\Lambda)$ by bounding $T(\Lambda)$, see [**2**] and [**4**]. The results in [**4**] compute $T(\mathbf{Z}[\zeta_p]C_2)$ in several interesting cases using [**3**].

Our first proposition describes $T(\Lambda)$ in terms of ring theoretic information for the case we are considering. We note this result may be generalized to all algebraic number fields to give a lower bound on $T(\Lambda)$ for G p-elementary abelian ([**2**, Theorem 5]) and an upper bound on $T(\Lambda)$ for G cyclic ([**11**, Lemma 3.4]). However, even in the case G is cyclic of prime order these bounds may not be equal. In that regard especially see [**11**, Theorem 4.2] where it is shown for $K = \mathbf{Q}(\sqrt{-d})$, $d > 3$, and the rational prime p, in fact prime in $\mathcal{O}_K$, that the lower bound on $T(\mathcal{O}_K[C_p])$ is $C_{(p+1)/2}$ and the upper bound is C_{p+1}.

Proposition 2 (cf. [**12**]). *Let $K = \mathbf{Q}(\zeta_p)$, ζ_p a primitive pth root of unity, and let G be a cyclic of order p. Then*

$$T(\Lambda) \cong (\mathcal{O}_K/p\mathcal{O}_K)^*/\mathrm{Im}\,((\mathbf{Z}/p\mathbf{Z})^*)\mathrm{Im}\,(\mathcal{O}_K^*).$$

Proof. By (1) and the definition of the map h, we have

$$T(\Lambda) \cong \overline{\mathcal{O}_K}^*/h(\mathcal{O}_K^* \times \Gamma^*) \cong (\overline{\mathcal{O}_K}^*/\mathrm{Im}\,(\mathcal{O}_K^*))/(\bar{\varepsilon}(\Gamma^*)/\mathrm{Im}\,(\mathcal{O}_K^*).$$

By [**2**, Lemma 6] one has for all $\gamma \in \Gamma^*$ that $\bar{\varepsilon}(\gamma)^{p-1} \in \mathrm{Im}\,(\mathcal{O}_K^*)$. From this it follows that

$$\mathrm{im}\,(h) \subseteq \{s \in \mathcal{O}_K^* : s^{p-1} \in \mathrm{Im}\,(\mathcal{O}_K^*)\}.$$

Since p totally ramifies in $K/\mathbf{Q}$ and the index of $K/\mathbf{Q}$ is $p-1$, it follows that $\overline{\mathcal{O}_K}^*$ is an abelian group of exponent $p(p-1)$. As $\mathrm{Im}\,((\mathbf{Z}/p\mathbf{Z})^*)$ is the $p-1$-torsion subgroup of $\overline{\mathcal{O}_K}^*$ we in fact have

$$\mathrm{im}\,(h) \subseteq \mathrm{Im}\,((\mathbf{Z}/p\mathbf{Z})^*)\mathrm{Im}\,(\mathcal{O}_K^*).$$

It is well known that for G cyclic $T(\mathbf{Z}[G])$ is trivial (see [**14**, 2.10] for example). Thus by extending scalars from $\mathbf{Z}$ to $\mathcal{O}_K$, we conclude the Swan class $[s, \Sigma]$ is trivial whenever $s \in \mathbf{Z}$. Thus we have

$$\mathrm{im}\,(h) = \ker(\delta) \supseteq \mathrm{Im}\,((\mathbf{Z}/p\mathbf{Z})^*)\mathrm{Im}\,(\mathcal{O}_K^*).$$

This proves the proposition. $\square$

We have the following corollary of Proposition 2 and the theorem of [**2**].

Corollary 3. *For $K = \mathbf{Q}(\zeta_p)$ we have $T(\mathbf{Z}[\zeta_p]C_p)$ contains a subgroup isomorphic to C_p^{p-2-k} for some k such that $1 \leq k \leq (p-1)/2$. Therefore, $R(\Lambda, K) \cap D(\Lambda)$ contains such a subgroup.*

Proof. We show $T(\Lambda)$ contains such a subgroup using Proposition 2; the result then follows from the theorem of [**2**]. As p totally ramifies $\overline{\mathbf{Z}[\zeta_p]}^* \cong C_{p-1} \times C_p^{p-2}$ and by Dirichlet's unit theorem $\mathbf{Z}[\zeta_p]^* \cong \langle -\zeta \rangle \times \langle \nu_1 \rangle \times \cdots \langle \nu_{(p-3)/2} \rangle$ where the ν are a system of fundamental units and ζ is any primitive pth root of unity. Since ζ is not congruent to 1 mod p, $T(\Lambda) \cong C_p^{p-2-k}$ where $1 \leq k \leq (p-1)/2$. $\square$

Notes. (1) Corollary 3 is essentially [**10**, Proposition 15]. (2) In [**10**] this was used to establish that $R(\Lambda, K) \cap D(\Lambda)$ is nontrivial for $p \geq 5$ for $K = \mathbf{Q}(\zeta_p)$, $G \cong C_p$.

2. Computing $T(\mathbf{Z}[\zeta_p]C_p)$ assuming Vandiver's conjecture. To complete the proof of Theorem 1 it suffices to find the exact value of the constant k in Corollary 3 above. We will show that when p satisfies Vandiver's conjecture there is a way of doing this that relates this constant k to the number of irregular indices of the prime $p > 2$.

Specifically, from Proposition 4 below, it immediately follows that $k = ((p-1)/2) - s$ where s is the number of irregular indices when $p > 2$ satisfies Vandiver's conjecture. This with the theorem of [**2**] proves Theorem 1.

Proposition 4. *If $p \nmid h_p^+$, then $T(\mathbf{Z}[\zeta_p]C_p) \cong C_p^{((p-3)/2)+s}$ where s is the number of irregular indices of the prime p.*

We begin with reviewing relative class numbers and Vandiver's conjecture and setting some more notation. If K is a CM-field (an imaginary quadratic extension of a totally real field) one denotes by K^+ its maximal real subfield. One usually denotes by $h(K)$ the class number of K and by $h^+(K)$ the class number of K^+. Vandiver's conjecture is that $p \nmid h^+(\mathbf{Q}(\zeta_p))$ for all primes p. Vandiver's conjecture has been verified for all primes p such that $p < 4{,}000{,}000$ [**15**]. To simplify notation, we denote $h^+(\mathbf{Q}(\zeta_p))$ by h_p^+. Let $\lambda = \zeta_p - 1$, and let $E = \mathbf{Z}[\zeta_p]^*$. For $j > 0$, let U_j denote the group of local units congruent to 1 mod $\lambda^j\mathbf{Z}[\zeta_p]$. Denote by $\mathbf{Z}_p$ the p-adic integers. Let $\Delta = \mathrm{Gal}\,(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ and $\omega : \Delta \to \mathbf{Z}_p$ be the Teichmuller character [**15**, p. 81]. Then ε_i is the idempotent in $\mathbf{Z}_p\Delta$ associated to ω^i, that is, $\varepsilon_i = (1/(p-1)) \sum_{s=1}^{p-1} \omega^i(s)\sigma_s^{-1}$ where σ is a fixed generator of Δ and $\sigma_s = \sigma^s$.

The proof of Proposition 4 follows in two steps. We first use Proposition 2 to write $T(\mathbf{Z}[\zeta_p]C_p)$ as a direct sum of $p-1$ indexed quotient groups (Lemma 5). Lemma 6 shows these quotient groups are isomorphic with C_p when the index i, $1 \le i \le p-2$, is odd or an irregular index and trivial otherwise. Upon counting the result follows. The method of proof given here comes in part from suggestions from the referee which greatly improved the presentation.

Lemma 5. *$T(\mathbf{Z}[\zeta_p]C_p) = \oplus_{i=0}^{p-2}\varepsilon_i(U_1/U_{p-1})/\beta(\varepsilon_i(E/E^p))$ where β is induced from the natural map $E \to (\mathbf{Z}[\zeta_p]/p\mathbf{Z}[\zeta_p])^*$ and from the isomorphism $U_1/U_{p-1} \to (\mathbf{Z}[\zeta_p]/p\mathbf{Z}[\zeta_p])^*/((\mathbf{Z}/p\mathbf{Z})^*)$.*

Proof. The prime p is totally ramified in $\mathbf{Q}(\zeta_p)$ of ramification degree $p-1$ and hence the ideal (p) in $\mathbf{Z}[\zeta_p]$ factors $(\lambda)^{p-1} = (p)$. Therefore we have the isomorphism $\mathbf{Z}[\zeta_p]/p\mathbf{Z}[\zeta_p] \cong \mathbf{Z}_p[\zeta_p]/(\lambda)^{p-1}$ coming from the natural map $\mathbf{Z}[\zeta_p] \to \mathbf{Z}_p[\zeta_p]$. Hence we have the isomorphisms

$$(2) \qquad \begin{aligned} U_1/U_{p-1} &\cong (\mathbf{Z}_p[\zeta_p]/p\mathbf{Z}[\zeta_p])^*/(\mathbf{Z}/p\mathbf{Z})^* \\ &\cong (\mathbf{Z}[\zeta_p]/p\mathbf{Z}[\zeta_p])^*/(\mathbf{Z}/p\mathbf{Z})^*, \end{aligned}$$

where U_1/U_{p-1} has exponent p. In view of Proposition 2, we have an exact sequence

$$(3) \qquad E/E^p \xrightarrow{\beta} U_1/U_{p-1} \longrightarrow T(\mathbf{Z}[\zeta_p]C_p) \longrightarrow 0,$$

where β is induced from (2) and the natural map $E \to (\mathbf{Z}[\zeta_p]/p\mathbf{Z}[\zeta_p])^*$. The group Δ is cyclic of order $p-1$ and ω generates the character group of Δ. Since U_1/U_{p-1} and $E_p = E/E^p$ are p-groups, we have from (2) and (3):

$$(4) \qquad \begin{aligned} T(\mathbf{Z}[\zeta_p]C_p) &\cong \bigoplus_{i=0}^{p-2} \varepsilon_i(T(\mathbf{Z}[\zeta_p]C_p)) \\ &\cong \bigoplus_{i=0}^{p-2} \frac{\varepsilon_i(U_1/U_{p-1})}{\beta(\varepsilon_i(E_p))}. \end{aligned}$$

This proves the lemma. □

Lemma 6. *The summands in* (4) *are nontrivial precisely when i is odd in the range $1 < i \le p-2$, or i is even and irregular in the range $1 < i \le p-2$.*

Proof. For all $i > 0$, the map $\mathbf{Z}/p\mathbf{Z} \to U_i/U_{i+1}$ defined by $a \bmod p \mapsto 1 + a\lambda^i \bmod U_{i+1}$ is an isomorphism of additive groups. It follows for all $i > 0$, U_i/U_{i+1} is a vector space of dimension 1 over $\mathbf{Z}/p\mathbf{Z}$ on which Δ acts via the character ω^i. Now as $\mathbf{Z}_p\Delta$ is semi-simple and U_1/U_{p-1} has a composition series with factors $\{U_i/U_{i+1}\}_{i=1}^{p-2}$, we see $\varepsilon_0(U_1/U_{p-1}) = 0$ and

$$(5) \qquad \#\varepsilon_i(U_1/U_{p-1}) = \#\varepsilon_i(U_i/U_{i+1}) = p \quad \text{if } 1 \le i \le p-2.$$

Because $\zeta_p = 1 + \lambda$ generates $U_1/U_2 = \varepsilon_1(U_1/U_2)$, we also have

$$(6) \qquad \varepsilon_1(U_1/U_{p-1}) = \varepsilon_1(\langle \zeta_p \rangle) = \beta(\varepsilon_1(E_p)).$$

From [**15**, Proposition 8.10] one has $\varepsilon_i(E_p) = 0$ if $1 < i \leq p-2$ and i is odd.

We now claim that if $2 \leq i \leq p-2$ and $2|i$, then $\varepsilon_i(U_i/U_{p-1}) = \beta(\varepsilon_i(E_p))$ if and only if $p \nmid B_i$ where B_i is the ith Bernoulli number. To show this, note that it is shown in the proof of [**15**, Theorem 8.16] that if $2 \leq i \leq p-2$ and i is even, then

$$L_p(1, \omega^i) \equiv -B_i/i \bmod p, \tag{7}$$

where $L_p(s, \omega^i)$ is the p-adic L-function of ω^i. Now, as we've assumed $p \nmid h_p^+$, the claim follows from (5)–(7) together with Proposition 8.10, Theorem 8.2 and Theorem 8.25 of [**15**]. The integer i is an irregular index when precisely $2 \leq i \leq p-2$, $2|i$, and $p|B_i$. The number of irregular indices is called the index of irregularity and is denoted s. This proves the lemma, Proposition 4 and Theorem 1. $\square$

Acknowledgments. This article is partly based on Chapter 4 of the author's thesis [**9**]. The author wishes to thank A. Srivastav for his assistance in obtaining these results. The author also wishes to thank the referee for suggestions improving the presentation.

REFERENCES

1. C.W. Curtis and I. Reiner, *Methods of representation theory*, Volume II, Wiley-Interscience, New York, 1987.

2. C. Greither, D.R. Replogle, K. Rubin and A. Srivastav, *Swan modules and Hilbert-Speiser number fields*, J. Number Theory **79** (1999), 164–173.

3. T. Kohl, *Group rings and Hopf Galois theory in Maple*, in *Maple* V: *Mathematics and its application, Proc. Maple Summer Workshop and Sympos.*, Birkhauser, Boston, 1994.

4. T. Kohl and D.R. Replogle, *Computation of several cyclotomic swan subgroups*, submitted to Math. Comp., posted October 18, 2000 (to appear in print).

5. L. McCulloh, *A Stickleberger condition on Galois module structure for Kummer extensions of prime degree*, in *Algebraic number fields, Proc. Durham Sympos. 1975*, Academic Press, London, 1977, 525–538.

6. ———, *Galois module structure elementary abelian extensions*, J. Algebra **82** (1983), 102–134.

7. ———, *Galois module structure of abelian extensions*, J. Reine Angew. Math. **375/376** (1987), 259–306.

8. I. Reiner and S. Ullom, *A Mayer-Vietoris sequence for classgroups*, J. Algebra **31** (1974), 305–342.

9. D.R. Replogle, *Swan classes and realisable classes for integral grouprings over groups of odd prime order*, Thesis, SUNY, Albany, 1997.

10. ———, *Swan modules and realisable classes for Kummer extensions of prime degree*, J. Algebra **212** (1999), 482–494.

11. ———, *Kernel groups and nontrivial Galois module structure of imaginary quadratic fields and their compositums*, submitted to Rocky Mountain J. of Math.

12. A. Srivastav, *On Galois module structure of tame p-extensions of $\mathbf{Q}(\mu_p)^+$ and p-adic L-functions*, submitted.

13. A. Srivastav and S. Venkataraman, *Relative Galois module structure of quadratic extensions*, Indian J. Pure Appl. Math. **25** (1994), 473–488.

14. S.V. Ullom, *Nontrivial lower bounds for class groups of integral group rings*, Illinois J. Math. **20** (1976), 361–371.

15. L. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Math. **83**, Springer, New York, 1980.

Department of Mathematics and Computer Science, College of Saint Elizabeth, 2 Convent Road, Morristown, NJ 07960
E-mail address: `dreplogl@liza.st-elizabeth.edu`