MATHEMATICS OF COMPUTATION
Volume 71, Number 237, Pages 343–348
S 0025-5718(00)01302-8
Article electronically published on October 18, 2000

COMPUTATION OF SEVERAL CYCLOTOMIC SWAN SUBGROUPS

TIMOTHY KOHL AND DANIEL R. REPLOGLE

ABSTRACT. Let $Cl(\mathcal{O}_K[G])$ denote the locally free class group, that is the group of stable isomorphism classes of locally free $\mathcal{O}_K[G]$-modules, where $\mathcal{O}_K$ is the ring of algebraic integers in the number field K and G is a finite group. We show how to compute the Swan subgroup, $T(\mathcal{O}_K[G])$, of $Cl(\mathcal{O}_K[G])$ when $K = \mathbb{Q}(\zeta_p)$, ζ_p a primitive p-th root of unity, $G = C_2$, where p is an odd (rational) prime so that $h_p^+ = 1$ and 2 is inert in $K/\mathbb{Q}$. We show that, under these hypotheses, this calculation reduces to computing a quotient ring of a polynomial ring; we do the computations obtaining for several primes p a nontrivial divisor of $Cl(\mathbb{Z}[\zeta_p]C_2)$. These calculations give an alternative proof that the fields $\mathbb{Q}(\zeta_p)$ for p=11, 13, 19, 29, 37, 53, 59, and 61 are not Hilbert-Speiser.

1. INTRODUCTION AND BACKGROUND ON SWAN MODULES

For an algebraic number field K we denote by $\mathcal{O}_K$ its ring of algebraic integers. Let $K = \mathbb{Q}(\zeta_p)$ where p is an odd prime and ζ_p is a primitive pth root of unity. It is well known that $\mathcal{O}_K$ is $\mathbb{Z}[\zeta_p]$. Consider the group ring $\mathbb{Z}[\zeta_p]C_2$, where C_2 is the group of order 2. In this paper we indicate how to compute the Swan subgroup, $T(\mathbb{Z}[\zeta_p]C_2)$, of the locally free classgroup $Cl(\mathbb{Z}[\zeta_p]C_2)$ when 2 is inert in K over $\mathbb{Q}$ and $h_p^+ = 1$, (that is, when the class number of the maximal real subfield is one—see the beginning of Section 2 for a definition). We will explicitly compute the Swan subgroup $T(\mathbb{Z}[\zeta_p]C_2)$ for those primes p such that $3 \leq p \leq 66$ satisfying our conditions.

In the rest of this introduction we provide background on Swan subgroups, outline their application to the question of Hilbert-Speiser number fields, and state our main results. The rest of this article is divided into two parts. In Section 2 we reduce the question to one suitable for the computer. In Section 3 we give the result of the computation for several primes p applying this to the question of Hilbert-Speiser number fields. Section 2 is based on parts of the second chapter of the thesis of the second author [5]. The calculations in Section 3 are derived from [3] of the first author.

Let Λ denote the order $\mathcal{O}_K[G]$ in the group algebra $K[G]$ for G a finite group of order n. For each $r \in \mathcal{O}_K$ such that $(r, n) = 1$ we may define the Swan module $\langle r, \Sigma \rangle = r\Lambda + \Lambda\Sigma$ where $\Sigma = \sum_{g \in G} g$. It can be shown (see [1] or [9], for example) that Swan modules are locally free, rank one, Λ-modules and hence determine classes in the locally free classgroup $Cl(\Lambda)$. For the Swan module $\langle r, \Sigma \rangle$ we denote

Received by the editor August 14, 1998 and, in revised form, March 1, 2000.
2000 *Mathematics Subject Classification.* Primary 11R33, 11R18.

its class by $[r, \Sigma] \in Cl(\Lambda)$. The set of Swan classes, $T(\Lambda)$, is a subgroup of $Cl(\Lambda)$ called the Swan subgroup (that $T(\Lambda)$ is a subgroup follows from the exact sequence of Reiner-Ullom discussed below).

Let $D(\Lambda)$ denote the kernel group which is the subgroup of $Cl(\Lambda)$ determined by those classes that become trivial upon extension of scalars to the maximal order of $K[G]$ containing $\mathcal{O}_K[G]$. Let ϵ and $\overline{\epsilon}$ denote the augmentation and induced augmentation maps, respectively, and let ϕ and $\overline{\phi}$ denote the canonical quotient maps. With this, consider the fiber product:

$$\begin{array}{ccc} \mathcal{O}_K G & \stackrel{\overline{\phi}}{\to} & \Gamma = \mathcal{O}_K[G]/\mathcal{O}_K\Sigma \\ \epsilon \downarrow & & \overline{\epsilon} \downarrow \\ \mathcal{O}_K & \stackrel{\phi}{\to} & \overline{\mathcal{O}_K} = \mathcal{O}_K/n\mathcal{O}_K. \end{array}$$

The result in [4], applied to the case when G is abelian of order n, is that there is an exact Mayer-Vietoris sequence

$$\mathcal{O}_K^* \times \Gamma^* \stackrel{h}{\to} \overline{\mathcal{O}_K}^* \stackrel{\delta}{\to} D(\Lambda) \to D(\Gamma) \oplus D(\mathcal{O}_K) \to 0,$$

where for any ring S we denote its group of multiplicative units by S^*. We define the two maps h and δ. If $(u, v) \in {\mathcal{O}_K}^* \times \Gamma^*$, then $h[(u, v)] = \overline{u} \cdot \overline{v}^{-1} = \phi(u)\overline{\epsilon}(v)^{-1}$. For $s \in \overline{\mathcal{O}_K}^*$ it is shown in [9], for instance, that $\delta(s)$ is the Swan class $[s, \Sigma]$. This gives that $T(\Lambda) \subseteq D(\Lambda)$ and that $T(\Lambda) \cong \overline{\mathcal{O}_K}^*/Im(\mathcal{O}_K^* \times \Gamma^*)$, where Im denotes the image under the map h.

This description of the Swan subgroup is both powerful and limited at the same time. It is powerful because it does describe the Swan subgroup in terms of ring theoretic information. However, it is limited as $\overline{\mathcal{O}_K}$, ${\mathcal{O}_K}^*$, and Γ^* are rarely computable. More precisely, the computation of these objects is in itself a separate algebraic number theoretic question. For the group of order two, the following result from [8], which we state as a lemma, removes the Γ^* term. This result follows from the fact that, for the group of order two, $\Gamma^* \cong {\mathcal{O}_K}^*$.

Lemma (cf [8, Proposition 2]). *For $|G| = 2$ one has $T(\Lambda) \cong \overline{\mathcal{O}_K}^*/Im({\mathcal{O}_K}^*)$.*

For 2 prime in $\mathbb{Z}[\zeta_p]$, one has that $\overline{\mathbb{Z}[\zeta_p]} = \mathbb{Z}[\zeta_p]/2\mathbb{Z}[\zeta_p]$ is isomorphic to a quotient ring of a polynomial ring. Restricting to when $h_p^+ = 1$ allows one to work with a computationally convenient set of units. We see precisely under these restrictions the Swan subgroup $T(\mathbb{Z}[\zeta_p]C_2)$ is readily computable by computer analysis. Specifically, letting $\mathbb{F}_2$ denote the field of two elements, we state our first main result.

Theorem 1. *For 2 prime in $\mathbb{Z}[\zeta_p]$ and $h_p^+ = 1$,*

$$T(\mathbb{Z}[\zeta_p]C_2) \cong (\mathbb{F}_2[z]/\langle \Phi_p(z) \rangle)^*/\langle \overline{z+1} \rangle \langle \overline{z} \rangle$$

is cyclic, where $\Phi_p(z)$ is the pth cyclotomic polynomial and $\langle z+1 \rangle$ and $\langle z \rangle$ are the ideals generated by the polynomials $z+1$ and z in $\mathbb{F}_2[z]/\langle \Phi_p(z) \rangle$.

We note (see Lemma 5) that we will show that the restrictions 2 being prime in $\mathbb{Z}[\zeta_p]$, and $h_p^+ = 1$ are satisfied by the primes in the following list.

List 2. $p = 3, 5, 11, 13, 19, 29, 37, 53, 59,$ *and* 61.

A number field K will be said to be Hilbert-Speiser if each finite tame abelian extension N/K has a trivial Galois module structure. That is, K is Hilbert-Speiser if $\mathcal{O}_N$ is a free Λ-module whenever N/K is a finite tame abelian Galois extension of number fields with Galois group $Gal(N/K) \cong G$. The classical Hilbert-Speiser theorem asserts that $\mathbb{Q}$, the rationals, is such a field. In [2] Swan modules and tame elementary abelian extensions are considered to derive conditions a Hilbert-Speiser field must satisfy. Let $S = \mathcal{O}_K$ and for each prime l let $\overline{S} = S/lS$ and $V_l = \overline{S}^*/Im(S^*)$.

Theorem ([2, Theorem 1]). *Let K be a Hilbert-Speiser number field. Then:*

(i) *The class number of K is 1;*
(ii) *For each odd prime l the exponent of the group V_l divides $(l-1)^2/2$;*
(iii) *The group $T(\mathcal{O}_K[C_2]) \cong V_2$ is trivial.*

This theorem is used to show that if K is any algebraic number field other than $\mathbb{Q}$, then K is not Hilbert-Speiser [2, Theorem 2]. This is proved by a Galois theoretic argument showing for each algebraic number field other than $\mathbb{Q}$ that there is an odd prime l such that condition (ii) is violated. Our interest in this fact is that upon performing the computation for the primes in List 2 we will obtain a proof of the following corollary, our second main result, by violating condition (iii).

Corollary 3. *For $p = 11, 13, 19, 29, 37, 53, 59,$ and 61, $\mathbb{Q}(\zeta_p)$ is not Hilbert-Speiser.*

2. Reduction to computation

If K is a CM-field, then one usually denotes by K^+ its maximal real subfield. Of course, cyclotomic fields $K = \mathbb{Q}(\zeta_n)$ for any positive integer $n > 2$ are CM and $K^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$. Denote the class number of K^+ by h_n^+. Here and throughout rest of the text, let ϕ be the usual Euler ϕ function. It is known that $h_n^+ = 1$ when n is a prime power and $\phi(n) \leq 66$ or if n is not a prime power and both $n \leq 200$ and $\phi(n) < 162$. Stronger statements are possible if one assumes the Generalized Riemann Hypothesis. For other results see for example the appendix of [10] from which these remarks were taken. We note that in general to compute cyclotomic Swan subgroups, it is natural to put restrictions on h_p or use p-adic L-functions. See [6] and [7] for example.

Proposition 4. $\mathbb{Z}[\zeta_p]/2\mathbb{Z}[\zeta_p] \cong \mathbb{F}_{2^{p-1}} \cong \mathbb{F}_2[z]/\langle \Phi_p(z) \rangle$, *where $\Phi_p(z)$ is the pth cyclotomic polynomial, whenever 2 is inert in $\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}$.*

Proof. Since we have assumed 2 is inert, $\mathbb{Z}[\zeta_p]/2\mathbb{Z}[\zeta_p]$ is a field as $2\mathbb{Z}[\zeta_p]$ is a maximal ideal. Furthermore, since $\mathbb{Z}[\zeta_p]/2\mathbb{Z}[\zeta_p]$ is a field extension of $\mathbb{Z}/2\mathbb{Z}$ of degree $p-1$, we have $\mathbb{Z}[\zeta_p]/2\mathbb{Z}[\zeta_p] \cong \mathbb{F}_{2^{p-1}}$. However, $\mathbb{F}_{2^{p-1}} \cong \mathbb{F}_2[\mu]$, where μ is the root of a polynomial of degree $p-1$ which is irreducible over $\mathbb{F}_2[z]$, as $\Phi_p(z)$ is irreducible of degree $p-1$, the result follows. □

By the remarks in Section 1 we know we wish to focus on when $h_p^+ = 1$ and 2 is prime in $\mathbb{Z}[\zeta_p]$. We now show why the primes in List 2 satisfy this.

Lemma 5. *The primes in List 2 satisfy our conditions.*

Proof. From the appendix in [10] one knows for p prime and $2 \leq p \leq 66$ that $h_p^+ = 1$. Hence we show that those primes in this interval for which 2 is inert are those precisely in List 2. Let $K = \mathbb{Q}(\zeta_m)$, ζ_m be a primitive mth root of unity, and

$q \in \mathbb{N}$ be prime. Then we have from [10, Theorem 2.13] that if q does not divide m, then q factors in $\mathcal{O}_K$ into the product of r distinct prime ideals of degree f, where $rf = \phi(m)$ and f is the least integer such that $q^f \equiv 1 \bmod m$. Thus if $q^f \equiv 1 \bmod p$ is satisfied only by $f = p - 1$, then q is inert. Determining that the minimal f which solves congruence $2^f \equiv 1 \bmod p$ is $p - 1$ is exactly the same as determining which primes (in the interval $3 \leq p \leq 66$) have 2 as their least primitive roots. The ones for which this holds are those in List 2. □

Our next proposition gives the units we will work with and their images.

Proposition 6. *If $h_p^+ = 1$ and 2 is inert in $\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}$, then the image of the units of $\mathbb{Z}[\zeta_p]$ in $(\mathbb{Z}[\zeta_p]/2\mathbb{Z}[\zeta_p])^*$ is generated by the images of $\zeta_p + 1$ and ζ_p. The image of $1 + \zeta_p$ in $\mathbb{Z}[\zeta_p]/2\mathbb{Z}[\zeta_p]$ is the same as the image of $1 + z$ in $\mathbb{F}_2[z]/\langle \Phi_p(z) \rangle$, where Φ_p is the pth cyclotomic polynomial. Similarly, the image of ζ_p is given by z.*

Proof. Combining several facts about the units of $\mathbb{Z}[\zeta_p]$ that may be found in of [10, Chapter 8], we have that for p a prime such that $h_p^+ = 1$, the units of $\mathbb{Z}[\zeta_p]$ are generated by $\pm\zeta$, where ζ is any primitive pth root of unity, and units of the form $\xi_a = \zeta_p^{(1-a)/2}[(1 - \zeta_p^a)/(1 - \zeta_p)]$. From this it follows that the image of the units of $\mathbb{Z}[\zeta_p]$ is generated by the images of ζ_p and $[(1 - \zeta_p^a)/(1 - \zeta_p)]$, $1 < a < p/2$. The quotient mod 2 is congruent to $1+\zeta_p$ as 2 is primitive root mod p (2 is inert), we have that $a \equiv 2^r \bmod p$. We have $\mathbb{Z}[\zeta_p]/2\mathbb{Z}[\zeta_p] \cong \mathbb{F}_{2^{(p-1)}} \cong \mathbb{F}_2[z]/\langle \Phi_p(z) \rangle$ by Proposition 4. Therefore, the result follows and the isomorphism is given by $\zeta_p \to z$. □

We now can complete the proof of the theorem.

Proof Theorem 1. Let $\Lambda = \mathbb{Z}[\zeta_p][C_2]$. We have $T(\Lambda) \cong \overline{\mathcal{O}_K}^*/Im\ (\mathcal{O}_K{}^*)$. By the lemmas above, the image of $\mathcal{O}_K{}^*$ in $\overline{\mathcal{O}_K}^*$ is isomorphic with the image of the subgroup generated by $z + 1$ and $z \in \mathbb{F}_2(z)/\langle \Phi_p(z) \rangle$ under the map $\zeta_p \to z$. $T(\Lambda)$ is cyclic, as it is a quotient of the cyclic group $(\mathbb{Z}[\zeta_p]/2\mathbb{Z}[\zeta_p])^*$, (the group of multiplicative units of a field). □

What all the above imply when taken together is that to compute $T(\mathbb{Z}[\zeta_p]C_2)$ when 2 is inert and $h_p^+ = 1$, it is equivalent to compute $(\mathbb{F}_2[z]/\langle \Phi_p(z) \rangle)^*/\langle \overline{z+1} \rangle \langle \overline{z} \rangle$. This is only effectively computable for small values of p, even using a computer. The computation is easier if $p \nmid |(\mathbb{F}_2[z]/\langle \Phi_p(z) \rangle)^*/\langle \overline{z+1} \rangle|$ as then the image of ζ_p does not have to be considered. (That is, since $Im(\langle z \rangle)$ must either be trivial or of order p, if $p \nmid |(\mathbb{F}_2[z]/\langle \Phi_p(z) \rangle)^*/\langle \overline{z+1} \rangle|$, then the image must be trivial.)

3. Computations

As mentioned above, the computation of $T(\mathbb{Z}[\zeta_p]C_2)$ using these methods involves determining the order of $z + 1$ inside $(\mathbb{F}_2[z]/\langle \Phi_p(z) \rangle)^*$ for each prime p in List 2. Each of the corresponding unit groups is cyclic of order $N = 2^{p-1} - 1$. Since each of the elements in the group are equivalence classes of polynomials, the whole problem is suited to being done in a CAS such as Maple since Maple treats all its basic expressions as polynomials. Moreover, the first author recognized that the package described in [3], a set of tools to do computations within the group algebras $\mathbb{Q}(\zeta_{p^n})C_{p^n}$, could be modified to tackle this problem.

The final results of the order calculations are given in Table 1.

TABLE 1

p	N	$\lvert z+1\rvert$	$\lvert T\rvert$
3	3	3	1
5	15	15	1
11	1023	341	3
13	4095	819	5
19	262143	9709	27
29	268435455	475107	565
37	68719476735	3233097	21255
53	4503599627370495	3556769739	1266205
59	288230376151711743	31675383749	9099507
61	1152921504606846975	65498251203	17602325

Observe now that $p \nmid |\frac{N}{|z+1|}|$ is indeed the case for each prime p and so,

$$\begin{aligned} T(\mathbb{Z}[\zeta_p]C_2) &\cong (\mathbb{F}_2[z]/\Phi_p(z))^*/(\langle\overline{z+1}\rangle\langle z\rangle) \\ &= (\mathbb{F}_2[z]/\Phi_p(z))^*/\langle\overline{z+1}\rangle. \end{aligned}$$

Now observing that for p=11, 13, 19, 29, 37, 53, 59, and 61 we have that $V_2 \cong T(\mathbb{Z}[\zeta_p]C_2)$ is nontrivial, we have proved Corollary 3.

We note that the proof of this corollary in this manner is in the spirit of [8]. That is, the corollary of [8, Theorem 1] gives V_2 is nontrivial for all imaginary quadratic fields of class number 1 except $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$, and $\mathbb{Q}(\sqrt{-7})$. Thus they obtained, in effect, that these three fields were the only possible Hilbert-Speiser imaginary quadratic fields.

ACKNOWLEDGMENTS

The second author would like to thank A. Srivastav and L. Childs for conversations regarding Section 2. Both authors would like to thank the referee for several suggestions for improving the presentation.

REFERENCES

[1] C. W. Curtis and I. Reiner, *Methods of Representation Theory*, Wiley-Interscience, New York, 1987. MR **88f:**20002

[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. CMP 2000:04

[3] T. Kohl, *Group rings and Hopf Galois Theory in Maple, in Maple V: Mathematics and Its Application, Proceedings of the Maple Summer Workshop and Symposium*, Birkhauser, Boston, 1994.

[4] I. Reiner and S. V. Ullom, *A Mayer-Vietoris sequence for class groups*, J. Algebra **31** (1974), 305-342. MR **50:**2321

[5] D. R. Replogle, *Swan Classes and Realisable Classes for Integral Group Rings over Groups of Prime Order*, Thesis, SUNY Albany, 1997.

[6] D. R. Replogle, *Cyclotomic Swan Subgroups and Irregular Indices*, Rocky Mountain J. Math. (to appear).

[7] A. Srivastav, *Galois Module Structure Subfileds of tame p-extensions of* $\mathbb{Q}(\zeta_p)^+$ *and p-adic L-functions*, submitted for publication.

[8] A. Srivastav and S. Venkataraman, *Relative Galois module structure of quadratic extensions*, Indian J. Pure. Appl. Math., **25 No. 5** (1994), 473-488. MR **95c:**11133

[9] S. V. Ullom, *Nontrivial lower bounds for class groups of integral group rings*, Illinois Journal Mathematics **20** (1976), 361-371. MR **52:**14024

[10] L. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics 83, Springer-Verlag, New York, 1982. MR **85g:**11001

Office of Information Technology, Boston University, Boston, Massachusetts
E-mail address: tkohl@math.bu.edu

Department of Mathematics and Computer Science, College of Saint Elizabeth, Morristown, New Jersey
E-mail address: dreplogle@liza.st-elizabeth.edu