Ann. Sci. Math. Québec **34** (2010), no 1, 73–84

CYCLIC COBORDISM OF SURFACES AND THE RELATIVE CLASS NUMBER

ROBERT D. LITTLE

Dedicated to Paulo Ribenboim on the occasion of his 80th birthday.

RÉSUMÉ. Soient p un nombre premier impair, $n \geq 1$ et $O_2(\mathbb{Z}/p^n\mathbb{Z})$ le groupe de cobordisme des applications de période p^n sur une surface lisse, fermée et orientable. Soit $G(p^n)$ l'image de $O_2(\mathbb{Z}/p^n\mathbb{Z})$ sous la signature équivariante. En vertu d'un théorème de Ewing, l'indice de $G(p)$ dans un groupe canonique d'entiers algébriques est $h^-(p)$, où $h^-(p)$ est le nombre de classes relatif de p. Nous généralisons ce résultat et montrons que l'indice de $G(p^n)$ divise $p^{(p^{n-1}-1)/2}h^-(p^n)$, et qu'il y a égalité lorsque $n = 1$.

ABSTRACT. Let p be an odd prime, $n \geq 1$, and $O_2(\mathbb{Z}/p^n\mathbb{Z})$ the cobordism group of maps of period p^n on smooth, closed, orientable surfaces. Let $G(p^n)$ be the image of $O_2(\mathbb{Z}/p^n\mathbb{Z})$ under the equivariant signature. A theorem of Ewing asserts that the index of $G(p)$ in a canonical group of algebraic integers is $h^-(p)$, the relative class number of p. We extend this result and show that the index of $G(p^n)$ divides $p^{(p^{n-1}-1)/2}h^-(p^n)$ with equality in the case $n = 1$.

1. Introduction

Let p be an odd prime, $n \geq 1$, $\lambda = e^{(2\pi i/p^n)}$ and $\alpha_{j/p^n} = (\lambda^j + 1)(\lambda^j - 1)^{-1}$, with $1 \leq j \leq p^n - 1$. If J is a subset of the set $\{1, 2, \ldots, p^n - 1\}$, let $\alpha_J = \{\alpha_{j/p^n} \mid j \in J\}$. We identify two important subsets of J :

$$T(p^n) = \{j \in J \mid 1 \leq j \leq (p^n - 1)/2\} \quad \text{and} \quad S(p^n) = \{j \in T(p^n) \mid (j, p) = 1\}.$$

If $\mathbb{Z}/p^n\mathbb{Z}$ is the cyclic group of order p^n, then the character of the $\mathbb{Z}/p^n\mathbb{Z}$–signature of a $\mathbb{Z}/p^n\mathbb{Z}$ action on a smooth, closed, orientable even dimensional manifold is an element of $\mathbb{Z}[\alpha_{T(p^n)}]$, the polynomial algebra generated by $\alpha_{T(p^n)}$ (see [1, Theorem 2.2]). The cobordism group of maps of period p^n on smooth, closed, orientable surfaces, $O_2(\mathbb{Z}/p^n\mathbb{Z})$, is a free group of rank $(p^n - 1)/2$ (see [3, p. 501]). Let $G(p^n)$ be the image of $O_2(\mathbb{Z}/p^n\mathbb{Z})$ under the character of the $\mathbb{Z}/p^n\mathbb{Z}$–signature mapping. The group $G(p^n)$ is a subgroup of $\mathrm{Span}_{\mathbb{Z}}\, \alpha_{S(p^n)}$, the group of integral linear combinations of elements in $\alpha_{S(p^n)}$ (see [3, p. 500]). A fundamental theorem of Ewing (see [4, Theorem 3.2]) produces a canonical group of algebraic integers $R_2(\mathbb{Z}/p\mathbb{Z})$ which contains $G(p)$ as a subgroup of index $h^-(p)$, the relative class number of p (see [8, Theorem

Reçu le 9 septembre 2008 et, sous forme définitive, le 11 mars 2009.

4.10]). We offer an index formula for subgroups of $G(p^n)$ of finite index which contains Ewing's formula as a special case. We are able to explicitly compute the index of an important subgroup of $G(p^n)$ which is equal to $G(p)$ in the special case $n = 1$. If $\varepsilon_{j/p^n} = k_j\alpha_{1/p^n} + \alpha_{j/p^n}$, with $j \in S(p^n)$, $k_j j \equiv -1 \pmod{p^n}$, with $0 < k_j < p^n$, and $E(p^n) = \mathrm{Span}_{\mathbb{Z}}\, \varepsilon_{S(p^n)}$, then $E(p^n)$ is a subgroup of $G(p^n)$ of finite index.

Theorem 1.1. *If H is a subgroup of $G(p^n)$ of finite index, then the index of H in $\mathrm{Span}_{\mathbb{Z}}\, \alpha_{S(p^n)}$ is finite and*

$$[R_2(\mathbb{Z}/p^n\mathbb{Z}) : H] = \left[\mathrm{Span}_{\mathbb{Z}}\, \alpha_{S(p^n)} : H\right] \cdot p^{((p^{n-1}-1)/2)-n} h^-(p^n)\,.$$

In particular, the index of $E(p^n)$ in $R_2(\mathbb{Z}/p^n\mathbb{Z})$ is $p^{(p^{n-1}-1)/2}h^-(p^n)$.

The subgroup $E(p^n)$ has been studied by many authors and $E(p) = G(p)$ (see [1, Theorem 5.2], [4, p. 59], [6, 3.1 Lemma] for instance) and so Ewing's theorem is a corollary of the second assertion in Theorem 1.1.

Corollary 1.2. ([4, Theorem 3.2]) *The index of $G(p)$ in $R_2(\mathbb{Z}/p\mathbb{Z})$ is $h^-(p)$.*

If $n \geq 2$, then $E(p^n)$ is a subgroup of $G(p^n)$ and so Theorem 1.1 provides an upper bound for the index of $G(p^n)$ in $R_2(\mathbb{Z}/p^n\mathbb{Z})$ which we record in our next theorem.

Theorem 1.3. *The index of $G(p^n)$ in $\mathrm{Span}_{\mathbb{Z}}\, \alpha_{S(p^n)}$ divides p^n and the index of $G(p^n)$ in $R_2(\mathbb{Z}/p^n\mathbb{Z})$ divides $p^{(p^{n-1}-1)/2}h^-(p^n)$.*

The index of $G(p^n)$ in $\mathrm{Span}_{\mathbb{Z}}\, \alpha_{S(p^n)}$ is p to a positive power since α_{j/p^n} is not an algebraic integer by [7, Proposition 3.6] and so it follows from Theorem 1.1 that the index of $G(p^n)$ in $R_2(\mathbb{Z}/p^n\mathbb{Z})$ is $h^-(p^n) \cdot p^{(p^{n-1}-1)/2-k}$, where $0 \leq k \leq n-1$. The exponent $(p^{n-1}-1)/2 - k$ is positive if $p \geq 5$ and $n \geq 2$ or $p = 3$ and $n \geq 3$. It is natural to conjecture that these index values are the same as in the case $n = 1$, that is the index of $G(p^n)$ in $\mathrm{Span}_{\mathbb{Z}}\, \alpha_{S(p^n)}$ is p^n and the index of $G(p^n)$ in $R_2(\mathbb{Z}/p^n\mathbb{Z})$ is $p^{(p^{n-1}-1)/2}h^-(p^n)$. It follows from Theorem 1.1 that these two conjectures are equivalent.

Our next two theorems offer another version of the index formula in Theorem 1.1.

Theorem 1.4. *The index of $\mathrm{Span}_{\mathbb{Z}}\, \alpha_{S(p^n)}$ in $\mathrm{Span}_{\mathbb{Z}}\, \alpha_{T(p^n)}$ is $p^{(p^{n-1}-1)/2}$.*

Theorem 1.5. *If H is a subgroup of $G(p^n)$ of finite index, then the index of H in $\mathrm{Span}_{\mathbb{Z}}\, \alpha_{T(p^n)}$ is finite and*

$$[R_2(\mathbb{Z}/p^n\mathbb{Z}) : H] = [\mathrm{Span}_{\mathbb{Z}}\, \alpha_{T(p^n)} : H] \cdot p^{-n} h^-(p^n)\,.$$

This paper is organized as follows. Section 2 contains some useful results about generalized circulant matrices. Section 3 concerns the algebraic numbers α_{j/p^n} and contains the proof of Theorem 1.4 (Theorem 3.6). Section 4 contains the proofs of Theorem 1.1 (Theorems 4.2 and 4.3), Corollary 1.2 (Corollary 4.4), Theorem 1.3 (Corollary 4.5) and Theorem 1.5 (Corollary 4.6).

2. Circulant matrices

Let $(\mathbb{Z}/p^n\mathbb{Z})^*$ denote the group of units in $\mathbb{Z}/p^n\mathbb{Z}$ expressed in the canonical way, that is $(\mathbb{Z}/p^n\mathbb{Z})^* = \{j \mid 1 \leq j < p^n, (j,p) = 1\}$. If f is a complex valued function defined on $(\mathbb{Z}/p^n\mathbb{Z})^*$ and ϕ is Euler's totient, then the $\phi(p^n) \times \phi(p^n)$ matrix $[f(kj^{-1})]$, where j is the row counter and k the column counter, is called the *generalized circulant matrix associated with* f (see [2, p. 421]). We will be interested in the function defined by the equation

$$f_{p^n}(\omega) = (2\omega - p^n)p^{-n},$$

with $\omega \in (\mathbb{Z}/p^n\mathbb{Z})^*$. The upper left hand $(\phi(p^n)/2) \times (\phi(p^n)/2)$ corner of $[f_{p^n}(kj^{-1})]$ is denoted by $B(p^n)$.

Theorem 2.1. *Let p be an odd prime, $n \geq 1$ and $\mu = (p-1)/2$. Then*

$$h^-(p^n) = (-1)^\mu p^n 2^{-(\phi(p^n)/2)+1} \det B(p^n)\,. \tag{1}$$

Proof. If $B_{1,\chi}$ is the generalized Bernoulli number at level 1 associated with the Dirichlet character χ (see [8, p. 30]), then the class number formula (see [8, Theorem 4.17]) asserts that for any m we have

$$h^-(m) = (-1)^{\phi(m)/2} Qam 2^{-\phi(m)/2} \prod_{\chi \,\mathrm{odd}} B_{1,\chi} \tag{2}$$

where

$$Q = \begin{cases} 1 & \text{if } m \text{ is a prime power,} \\ 2 & \text{otherwise,} \end{cases} \qquad \text{and} \qquad a = \begin{cases} 2 & \text{if } m \text{ is odd,} \\ 1 & \text{if } m \text{ is even.} \end{cases}$$

The Bernoulli number $B_{1,\chi}$ is equal to the first moment of χ by [8, p. 37]. It follows from this fact and viewing circulant matrices in terms of a basis of translation functions (see [2, p. 421]) that the determinant of $B(p^n)$ satisfies the equation

$$\det B(p^n) = \prod_{\chi \,\mathrm{odd}} B_{1,\chi}\,. \tag{3}$$

Formula (1) follows from (2) in the case $m = p^n$ and (3). □

Note that $\det B(p^n) \neq 0$ since $B_{1,\chi} \neq 0$ if χ is odd (see [8, p. 37]). It is clear from (1) that $B(p^n)$ will play a role in our index formulas. Another invertible $\phi(p^n)/2$ by $\phi(p^n)/2$ matrix will play a role and we will relate its determinant to $\det B(p^n)$. We begin with a lemma followed by an immediate corollary.

Lemma 2.2. *If $n \geq 2$ and $\omega_0 \in (\mathbb{Z}/p^{n-1}\mathbb{Z})^*$, then*

$$\sum_{\omega \equiv \omega_0 (\mathrm{mod}\, p^{n-1})} f_{p^n}(\omega) = f_{p^{n-1}}(\omega_0)\,. \tag{4}$$

Proof. Since $\omega_0 \in (\mathbb{Z}/p^{n-1}\mathbb{Z})^*$, we have

$$\sum_{\omega \equiv \omega_0 (\mathrm{mod}\, p^{n-1})} f_{p^n}(\omega) = (2\omega_0 - p^n)p^{-n} + \sum_{\ell=1}^{p-1} \left(2\left(\omega_0 + \ell p^{n-1}\right) - p^n\right) p^{-n}\,. \tag{5}$$

Formula (4) follows from (5). □

Corollary 2.3. *Let $n \geq 2$, $k \in S(p^n)$, $k_0 \in S(p^{n-1})$ and $k \equiv k_0 \pmod{p^{n-1}}$. Then, for $j_0 \in S(p^{n-1})$, we have*

$$\sum_{j \equiv j_0 (\mathrm{mod}\, p^{n-1})} f_{p^n}\left(kj^{-1}\right) = f_{p^{n-1}}\left(k_0 j_0^{-1}\right). \tag{6}$$

The next step is to record the effect of (6) on certain column sums of $B(p^n)$. This will help us relate $\det B(p^n)$ to $\det B(p^{n-1})$ if $n \geq 2$. Recall that $B(p^n)$ is the upper left $\phi(p^n)/2 \times \phi(p^n)/2$ corner of $[f_{p^n}(kj^{-1})]$. We will denote the entry of $B(p^n)$ with row counter j and column counter k by $b_{jk}(p^n)$, for j, $k \in S(p^n)$ where $S(p^n)$ is the set of integers between 1 and $(p^n - 1)/2$, inclusive, which are prime to p. We will continue the convention started in Corollary 2.3 of distinguishing counters in $S(p^{n-1})$ by a subscript of zero. It will help with bookkeeping to recall that $S(p^n)$ is the union of $S(p^{n-1})$ with the union of the sets $\{j = \ell p^{n-1} \pm j_0 \mid 1 \leq \ell \leq \mu\}$ as j_0 varies over $S(p^{n-1})$. Our next lemma shows that if the entries in a column of $B(p^n)$ with row counters congruent to $\pm j_0$ modulo p^{n-1} are summed in a certain way, the result is an entry of $B(p^{n-1})$ up to sign.

Lemma 2.4. *Let $n \geq 2$, $k \in S(p^n)$, $k_0 \in S(p^{n-1})$ and $k \equiv \pm k_0 \pmod{p^{n-1}}$. Then, for $j_0 \in S(p^{n-1})$, we have*

$$b_{j_0 k}(p^n) + \sum_{\ell=1}^{\mu} \left(b_{\ell p^{n-1} + j_0 k}(p^n) - b_{\ell p^{n-1} - j_0 k}(p^n)\right) = \pm b_{j_0 k_0}(p^{n-1}). \tag{7}$$

Proof. This follows from (6) and the fact that $f_{p^n}(kj^{-1})$ is odd when restricted to a fixed column or row, since f_{p^n} is an odd function. □

We will now use (7) to transform $B(p^n)$ using elementary row/column operations. Recall that a Type I row/column operation is a switch of two rows/columns, a Type II is multiplication of a row/column by a constant, and a Type III row/column operation replaces a row/column by itself plus a multiple of another row/column. We will transform $B(p^n)$ using only Type III operations and so the determinant is unchanged. First, we use Type III row operations and (7) to transform $B(p^n)$ into a new matrix $B'(p^n)$ which is the same as $B(p^n)$ save in the first $\phi(p^{n-1})/2$ rows. In these rows, $B'(p^n)$ can be described, looking left to right, as $B(p^{n-1})$, followed by $-B(p^{n-1})$ with the order of the columns reversed, with this pattern repeated, finishing with $B(p^{n-1})$. We continue our convention of distinguishing counters in $S(p^{n-1})$ with a zero subscript in our next lemma.

Lemma 2.5. *If $n \geq 2$, then $B(p^n)$ is Type III row equivalent to $B'(p^n) = [b'_{jk}(p^n)]$ where*

$$b'_{jk}(p^n) = \begin{cases} \pm b_{j_0 k_0}(p^{n-1}) & \text{if } j = j_0 \text{ and } k \equiv \pm k_0 \pmod{p^{n-1}}, \\ b_{jk}(p^n) & \text{otherwise.} \end{cases} \tag{8}$$

Proof. For $j_0 \in S(p^{n-1})$, replace $\mathrm{Row}_{j_0} B(p^n)$ by

$$\mathrm{Row}_{j_0} B(p^n) + \sum_{\ell=1}^{\mu} \left(\mathrm{Row}_{\ell p^{n-1} + j_0} B(p^n) - \mathrm{Row}_{\ell p^{n-1} - j_0} B(p^n)\right) \tag{9}$$

in a series of Type III row operations. Formula (8) follows from (7). □

It is clear from (8) that we can use Type III column operations to transform the first $\phi(p^{n-1})/2$ rows of $B'(p^n)$ into a copy of $B(p^{n-1})$ in the upper left hand corner and then all zeros. This will not change the first $\phi(p^{n-1})/2$ columns of the remaining rows, but it will produce a square matrix in the lower right hand corner which will be useful later because of the specific Type III column operations used in the transformation.

Lemma 2.6. *If $n \geq 2$, then $B'(p^n)$ is Type III column equivalent to another matrix $B''(p^n) = [b''_{jk}(p^n)]$ such that there is a $(\phi(p^n) - \phi(p^{n-1}))/2$ by $(\phi(p^n) - \phi(p^{n-1}))/2$ matrix $A(p^n) = [a_{jk}(p^n)]$ with*

$$b''_{jk}(p^n) = \begin{cases} b_{jk}(p^{n-1}) & \text{if } j,k \in S(p^{n-1}), \\ 0 & \text{if } j \in S(p^{n-1}) \text{ and } k \in S(p^n) \setminus S(p^{n-1}), \\ b_{jk}(p^n) & \text{if } j \in S(p^n) \setminus S(p^{n-1}) \text{and } k \in S(p^{n-1}), \\ a_{jk}(p^n) & \text{if } j,k \in S(p^n) \setminus S(p^{n-1}). \end{cases} \tag{10}$$

Proof. If $k = \ell p^{n-1} \pm k_0$, with $k_0 \in S(p^{n-1})$ and $1 \leq \ell \leq \mu$, then Type III column operations are performed on $\mathrm{Col}_k\, B'(p^n)$ as follows: $\mathrm{Col}_{\ell p^{n-1} \pm k_0}\, B'(p^n)$ is replaced by $\mathrm{Col}_{\ell p^{n-1} \pm k_0}\, B'(p^n) \mp \mathrm{Col}_{k_0}\, B'(p^n)$. Formula (10) follows from (8). □

Corollary 2.7. *If $n \geq 2$, then*

$$\det B(p^n) = \det B(p^{n-1}) \det A(p^n)\,. \tag{11}$$

Proof. Type III operations do not change the determinant and so

$$\det B(p^n) = \det B'(p^n) = \det B''(p^n).$$

Formula (11) follows since (10) implies that $\det B''(p^n) = \det B(p^{n-1}) \det A(p^n)$. □

3. The algebraic numbers α_{j/p^n}

In this section, we study the numbers $\alpha_{j/p^n} = (\lambda^j + 1)(\lambda^j - 1)^{-1}$. They are algebraic numbers with minimal polynomial equal to a transform of the cyclotomic polynomial $\Phi_{p^n}(x)$ but they are not algebraic integers (see [7, Propositions 3.3 and 3.6]). We will prove Theorem 1.4 in this section. We begin with a result which relates the algebraic numbers α_{j/p^n} to $B(p^n)$ and the algebraic integers $v_{j/p^n} = \lambda^j - \lambda^{-j}$.

Proposition 3.1. *If p is an odd prime and $n \geq 1$, then*

$$[\alpha_{j/p^n} \mid j \in S(p^n)]^T = B(p^n)[v_{j/p^n} \mid j \in S(p^n)]^T + [\alpha_{j/p^{n-1}} \mid j \in S(p^n)]^T\,. \tag{12}$$

Proof. A formula in the literature (see [1, Lemma 4.4]) and a bit of computation yield

$$\alpha_{j/p^n} = p^{-n} \sum_{k \in S(p^n)} (2k - p^n) v_{kj/p^n} + \alpha_{j/p^{n-1}}\,. \tag{13}$$

Formula (12) is just (13) written using column vectors. □

We remark that (12) in the case $n = 1$ is in the literature (see [4, p. 59]). In this special case, the algebraic integers $v_{j/p}$, with $j \in S(p)$, are rationally independent, but if $n \geq 2$, the algebraic integers v_{j/p^n}, $j \in S(p^n)$, are not rationally independent. They satisfy certain relations which we describe in the next lemma in a slightly generalized form. We expand our bookkeeping to $T(p^n) = \{j \mid 1 \leq j \leq (p^n - 1)/2\}$ and note that $T(p^n)$ is the union of $S(p^n)$ and the union of the sets $\{p^k j \mid j \in S(p^{n-k})\}$ as k varies from 1 to $n - 1$. Our next lemma expresses v_{j/p^n} with counter $j \in T(p^{n-1})$, in terms of v_{j/p^n} with counter j in $T(p^n) \setminus T(p^{n-1})$.

Lemma 3.2. *If $j \in S(p^{n-k})$, with $1 \leq k \leq n-1$, then*

$$v_{p^{k-1}j/p^n} = \sum_{\ell=1}^{\mu} \left(v_{p^{k-1}(\ell p^{n-k} - j)/p^n} - v_{p^{k-1}(\ell p^{n-k} + j)/p^n} \right). \tag{14}$$

Proof. Formula (14) will follow if we can show that, for $j_0 \in S(p^{n-1})$, we have

$$v_{j_0/p^n} = \sum_{\ell=1}^{\mu} \left(v_{(\ell p^{n-1} - j_0)/p^n} - v_{(\ell p^{n-1} + j_0)/p^n} \right). \tag{15}$$

To see that (15) holds, write $\Phi_{p^n}(\lambda) = 0$ as

$$\sum_{\ell=0}^{\mu} \lambda^{\ell p^{n-1}} + \sum_{\ell=1}^{\mu} \lambda^{-\ell p^{n-1}} = 0 . \tag{16}$$

Formula (15) is obtained by multiplying (16) by λ^{j_0} to obtain a first equation, then multiplying (16) by λ^{-j_0} to obtain a second equation and then subtracting the second equation from the first. Formula (14) is (15) at level $j \in S(p^{n-k})$. □

The numbers α_{j/p^n} satisfy relations like (14), where $j \in T(p^n)$. They reflect the fact that $\alpha_{S(p^n)}$ is a maximal set of rationally independent numbers in the set $\alpha_{T(p^n)}$ (see [3, (3.3) Lemma]). If $j_0 \in S(p^{n-1})$, then the numbers $\alpha_{j_0/p^{n-1}}$ satisfy relations in $\mathrm{Span}_{\mathbb{Z}}\, \alpha_{S(p^n)}$ which are presented next in a generalized form.

Lemma 3.3. *If $j \in S(p^{n-k})$, with $1 \leq k \leq n-1$, then*

$$p\alpha_{p^k j/p^n} = \sum_{\ell=0}^{\mu} \alpha_{p^{k-1}(\ell p^{n-k} + j)/p^n} - \sum_{\ell=1}^{\mu} \alpha_{p^{k-1}(\ell p^{n-k} - j)/p^n} . \tag{17}$$

Proof. As in the proof of (14), (17) follows if we can show that for $j_0 \in S(p^{n-1})$, $n \geq 2$,

$$p\alpha_{j_0/p^{n-1}} = \sum_{\ell=0}^{\mu} \alpha_{(\ell p^{n-1} + j_0)/p^n} - \sum_{\ell=1}^{\mu} \alpha_{(\ell p^{n-1} - j_0)/p^n} . \tag{18}$$

Formula (18) follows by taking alternating column sums in (12) over rows congruent to $\pm j_0 \pmod{p^{n-1}}$, with $\pm$ sign chosen accordingly, and then appealing to (7) and (15). Formula (17) is (18) at level $j \in S(p^{n-k})$. It is interesting to note that (18) also follows from the identity $i\alpha_{j/p^n} = \cot(\pi j/p^n)$ (see [5, 29.1.3, p. 202]). □

The next step is a study of $\mathrm{Span}_{\mathbb{Z}}\,\alpha_{T(p^n)}/\,\mathrm{Span}_{\mathbb{Z}}\,\alpha_{S(p^n)}$ and the proof of Theorem 1.4. It follows from (17) that if $[\alpha_{p^k j/p^n}]$ is the image of $\alpha_{p^k j/p^n}$ in this quotient group, then the order of $[\alpha_{p^k j/p^n}]$ divides p^k. The completeness of the relations (17) established next will imply that this order is p^k.

Lemma 3.4. *Suppose that $n-1 \geq k_1 \geq k_2 \geq \cdots \geq k_s \geq 1$. Let $j_\iota \in S(p^{n-k_\iota})$, with $1 \leq \iota \leq s$, and assume that if any of the inequalities are equalities, then the corresponding j values are distinct. If there is a relation*

$$\sum_{\iota=1}^{s} n_\iota \alpha_{p^{k_\iota} j_\iota/p^n} = \sum_{k\in S(p^n)} a_k \alpha_{k/p^n} \tag{19}$$

in $\mathrm{Span}_{\mathbb{Z}}\,\alpha_{T(p^n)}$, where $n_\iota \in \mathbb{Z}$, with $1 \leq \iota \leq s$, and $a_k \in \mathbb{Z}$, with $k \in S(p^n)$, then

$$n_\iota \equiv 0 \pmod{p^{k_\iota}}, \text{ with } 1 \leq \iota \leq s\,. \tag{20}$$

Proof. It follows from (17) that $p^k \alpha_{p^k j/p^n}$, with $j \in S(p^{n-k})$ and $1 \leq k \leq n-1$, is a sum of p^k numbers in $\alpha_{S(p^n)}$ each with coefficient ± 1. If (19) holds under the above conditions, then

$$\sum_{\iota=1}^{s} p^{k_1-k_\iota} n_\iota A_\iota = \sum_{k\in S(p^n)} p^{k_1} a_k \alpha_{k/p^n} \tag{21}$$

where A_ι is a sum of p^{k_ι} numbers in $\alpha_{S(p^n)}$ each with coefficient ± 1. We will use induction on ι to establish (20). Formula (20) at the initial value $\iota = 1$ holds because our assumptions guarantee that there is at least one term in A_1 which does not occur in A_ι, with $\iota > 1$, and so (21) implies that $n_1 \equiv 0 \pmod{p^{k_1}}$ in view of the rational independence of $\alpha_{S(p^n)}$ (see [3, (3.3) Lemma]). Inductively, assume that for $\iota \geq 2$ we have $n_\eta \equiv 0 \pmod{p^{k_\eta}}$, with $\eta < \iota$. There is at least one term in A_ι which does not occur in A_κ, where $\kappa > \iota$, and so (21) and the rational independence of $\alpha_{S(p^n)}$ imply that

$$p^{k_1-k_\iota} n_\iota + p^{k_1-k_{\iota-1}} n_{\iota-1} + \cdots + n_1 \equiv 0 \pmod{p^{k_1}}.$$

It follows from the inductive hypothesis that $n_\iota \equiv 0 \pmod{p^{k_\iota}}$ and so the inductive proof of (20) is complete. □

Corollary 3.5. *If $j \in S(p^{n-k})$, with $1 \leq k \leq n-1$, then the order of $[\alpha_{p^k j/p^n}]$ is p^k.*

Proof. We have remarked that (17) implies that the order of $[\alpha_{p^k j/p^n}]$ divides p^k. Formulas (19) and (20) in the case $s = 1$ imply that p^k divides the order of $[\alpha_{p^k j/p^n}]$. □

Lemma 3.3 and Corollary 3.5 suggest that $\mathrm{Span}_{\mathbb{Z}}\,\alpha_{T(p^n)}/\,\mathrm{Span}_{\mathbb{Z}}\,\alpha_{S(p^n)}$ is related to the group

$$C(p^n) = \coprod_{k=1}^{n-1} \coprod_{j\in S(p^{n-k})} (\mathbb{Z}/p^k\mathbb{Z})_j$$

where the notation means that for each k, with $1 \leq k \leq n-1$, a direct sum of $|S(p^{n-k})| = (p^{n-k} - p^{n-k-1})/2$ copies of $\mathbb{Z}/p^k\mathbb{Z}$ is included as a summand. The

generator of $(\mathbb{Z}/p^k\mathbb{Z})_j$ will correspond to $[\alpha_{p^k j/p^n}]$. If $2 \le k \le n-1$ and $j \in S(p^{n-k})$, let $D_{k,j}$ be the cyclic subgroup of $C(p^n)$ of order p^{k-1} generated by the left side of (17) minus the right side (17) under the correspondence described in the previous sentence. Let $D(p^n)$ be the subgroup of $C(p^n)$ defined by

$$D(p^n) = \coprod_{k=2}^{n-1} \coprod_{j \in S(p^{n-k})} D_{k,j} \, .$$

Theorem 3.6 below contains Theorem 1.4.

Theorem 3.6. *The groups* $\operatorname{Span}_{\mathbb{Z}} \alpha_{T(p^n)} / \operatorname{Span}_{\mathbb{Z}} \alpha_{S(p^n)}$ *and* $C(p^n)/D(p^n)$ *are isomorphic via the rule which sends* $[\alpha_{p^k j/p^n}]$ *to the generator of* $(\mathbb{Z}/p^k\mathbb{Z})_j$*, with* $j \in S(p^{n-k})$ *and* $1 \le k \le n-1$*. In particular, the index of* $\operatorname{Span}_{\mathbb{Z}} \alpha_{S(p^n)}$ *in* $\operatorname{Span}_{\mathbb{Z}} \alpha_{T(p^n)}$ *is* $p^{(p^{n-1}-1)/2}$*.*

Proof. The rule described in the statement of the theorem is well defined because of Corollary 3.5. It is onto by definition and injective because of (17) and Lemma 3.4. The assertion about the index of $\operatorname{Span}_{\mathbb{Z}} \alpha_{S(p^n)}$ in $\operatorname{Span}_{\mathbb{Z}} \alpha_{T(p^n)}$ follows from the formulas

$$|C(p^n)| = \exp_p \left(\sum_{k=1}^{n-1} k \left| S(p^{n-k}) \right| \right)$$

and

$$|D(p^n)| = \exp_p \left(\sum_{k=1}^{n-1} (k-1) \left| S(p^{n-k}) \right| \right) \, ,$$

where $\exp_p(x) = p^x$. □

Our next observation is that (12) can be simplified if $B(p^n)$ is replaced by another matrix $B^*(p^n)$. There is a connection with Theorem 3.6. We will see that up to sign, the determinant of $B^*(p^n)$ is $p^{(p^{n-1}-1)/2}$ times the determinant of $B(p^n)$.

Lemma 3.7. *The algebraic integers in the set*

$$v_{T(p^n) \setminus T(p^{n-1})} = \left\{ v_{j/p^n} \mid j \in T(p^n) \setminus T(p^{n-1}) \right\}$$

are rationally independent and there is a $\phi(p^n)/2$ *by* $\phi(p^n)/2$ *rational matrix* $B^*(p^n)$ *such that*

$$\left[\alpha_{j/p^n} \mid j \in S(p^n) \right]^T = B^*(p^n) \left[v_{j/p^n} \mid j \in T(p^n) \setminus T(p^{n-1}) \right]^T \, . \tag{22}$$

Proof. The set $v_{T(p^n) \setminus T(p^{n-1})}$ is rationally independent since a nontrivial dependency would contradict the minimality of the cyclotomic polynomial. The existence of $B^*(p^n)$ and (22) follows from (12), (15), and induction. □

It follows from (22) and the independence of $\alpha_{S(p^n)}$ and $v_{T(p^n) \setminus T(p^{n-1})}$ that $B^*(p^n)$ is invertible. Note that $B^*(p) = B(p)$ since (12) and (22) are the same in the case $n = 1$. Our next lemma will lead to the computation of the determinant of $B^*(p^n)$. It relates $\det B^*(p^n)$ to $\det B^*(p^{n-1})$ and $\det A(p^n)$, where $A(p^n)$ is the matrix in Lemma 2.6 and Corollary 2.7.

Lemma 3.8. *If $n \geq 2$, then*

$$\det B^*(p^n) = \pm \det(pB^*(p^{n-1})) \det A(p^n)\,. \tag{23}$$

Proof. Start with the sequence of Type III elementary row operations described in (9) with $B(p^n)$ replaced by $B^*(p^n)$ on $\mathrm{Row}_{j_0} B^*(p^n)$, with $j_0 \in S(p^{n-1})$. The j_0-th row of the new matrix has zeros in every column except those with counter divisible by p where the entry is the corresponding entry of $\mathrm{Row}_{j_0}(pB^*(p^{n-1}))$ because of (18), (22) and the independence of $v_{T(p^n)\setminus T(p^{n-1})}$ established in Lemma 3.7. A sequence of Type I column operations transforms this matrix into a matrix with $pB^*(p^{n-1})$ in the upper left hand $\phi(p^{n-1})/2$ by $\phi(p^{n-1})/2$ square, a $\phi(p^{n-1})/2$ by $(\phi(p^n)-\phi(p^{n-1}))/2$ rectangle of zeros upper right, untouched $B^*(p^n)$ lower left and $A(p^n)$ in the lower right hand $(\phi(p^n)-\phi(p^{n-1}))/2$ by $(\phi(p^n)-\phi(p^{n-1}))/2$ square. To see that the lower right square is $A(p^n)$, recall that $A(p^n)$ is constructed using the column operations dictated by the relations (15) which led to the columns in $B^*(p^n)$ with counters prime to p. Formula (23) follows from the fact that operations of Types I and III only effect the sign of the determinant. □

Corollary 3.9. *If $n \geq 1$, then*

$$\det\left(B^*(p^n)B(p^n)^{-1}\right) = \pm p^{(p^{n-1}-1)/2}\,. \tag{24}$$

Proof. Formula (24) follows from (11), (23), the facts that $B(p^n)$ is invertible and $B^*(p) = B(p)$, and induction. □

Note that the right hand side of (24) is the index of $\mathrm{Span}_{\mathbb{Z}}\, \alpha_{S(p^n)}$ in $\mathrm{Span}_{\mathbb{Z}}\, \alpha_{T(p^n)}$ up to sign by Theorem 3.6. We will exploit this fact in the next section.

4. The index formulas

If p is an odd prime and $n \geq 1$, let $R_2(\mathbb{Z}/p^n\mathbb{Z})$ be the subgroup of $\mathrm{Span}_{\mathbb{Z}}\, v_{T(p^n)}$ defined by

$$R_2(\mathbb{Z}/p^n\mathbb{Z}) = \left\{ \sum_{k\in T(p^n)} n_k v_{k/p^n} \;\middle|\; n_k \equiv n_{k'} \pmod 2 \right\}.$$

It follows from the properties of the $\mathbb{Z}/p^n\mathbb{Z}$–signature that $G(p^n) \subset R_2(\mathbb{Z}/p^n\mathbb{Z})$ (see [4, p. 56]). It will be useful to reformulate $R_2(\mathbb{Z}/p^n\mathbb{Z})$ in terms of the set of independent algebraic integers $v_{T(p^n)\setminus T(p^{n-1})}$. It is not hard to see that (14) implies that $R_2(\mathbb{Z}/p^n\mathbb{Z})$ satisfies the equation below where $\mathrm{ord}_p\, k$ is the exponent of p in the prime factorization of k:

$$R_2(\mathbb{Z}/p^n\mathbb{Z}) = \left\{ \sum_{k\in T(p^n)\setminus T(p^{n-1})} n_k v_{k/p^n} \;\middle|\; \begin{array}{l} n_k \equiv 0 \pmod 2, \\ \mathrm{ord}_p\, k < n-1, \\ n_k \equiv n_{k'} \pmod 2, \\ \mathrm{ord}_p\, k = \mathrm{ord}_p\, k' = n-1. \end{array} \right\}$$

Lemma 4.1. *The index of $R_2(\mathbb{Z}/p^n\mathbb{Z})$ in $\mathrm{Span}_{\mathbb{Z}}\, v_{T(p^n)\setminus T(p^{n-1})}$ is $2^{(\phi(p^n)/2)-1}$.*

Proof. Let $a(p^n) = \big|\{k \in T(p^n) \setminus T(p^{n-1}) \mid \operatorname{ord}_p k = n-1\}\big|$. The quotient of $\operatorname{Span}_{\mathbb{Z}} v_{T(p^n)\setminus T(p^{n-1})}$ by $R_2(\mathbb{Z}/p^n\mathbb{Z})$ is isomorphic to the direct sum of two groups. The first is a direct sum of $(\phi(p^n)/2) - a(p^n)$ copies of $\mathbb{Z}/2\mathbb{Z}$ coming from values of k with $\operatorname{ord}_p k < n-1$ and the second is a group of order $2^{a(p^n)-1}$ coming from those values of k with $\operatorname{ord}_p k = n-1$ (see [4, p. 59]). □

Theorem 4.2. *If H is a subgroup of $G(p^n)$ of finite index, then the index of H in $\operatorname{Span}_{\mathbb{Z}} \alpha_{S(p^n)}$ is finite and*

$$\big[R_2(\mathbb{Z}/p^n\mathbb{Z}) : H\big] = \big[\operatorname{Span}_{\mathbb{Z}} \alpha_{S(p^n)} : H\big] \cdot p^{((p^{n-1}-1)/2)-n} h^-(p^n)\,. \tag{25}$$

Proof. Consider the diagram below where all the maps are inclusion and the top horizontal map follows from (22):

$$\begin{array}{ccc}
\operatorname{Span}_{\mathbb{Q}} \alpha_{S(p^n)} & \xrightarrow{B^*(p^n)} & \operatorname{Span}_{\mathbb{Q}} v_{T(p^n)\setminus T(p^{n-1})} \\
\uparrow & & \uparrow \\
\operatorname{Span}_{\mathbb{Z}} \alpha_{S(p^n)} & & \operatorname{Span}_{\mathbb{Z}} v_{T(p^n)\setminus T(p^{n-1})} \\
\uparrow & & \uparrow \\
H & \longrightarrow & R_2(\mathbb{Z}/p^n\mathbb{Z})\,.
\end{array}$$

The index of H in $\operatorname{Span}_{\mathbb{Z}} \alpha_{S(p^n)}$ is finite because the index $E(p^n)$ in $\operatorname{Span}_{\mathbb{Z}} \alpha_{S(p^n)}$ is finite (proof of Theorem 4.3). The independence of $\alpha_{S(p^n)}$ (see [3, (3.3) Lemma]) implies that $E(p^n)$ has maximal rank. It follows that $G(p^n)$ has maximal rank. We may therefore assume that H has maximal rank and so the equation below follows from Lemma 4.1 and some linear algebra (see [4, p. 59] for instance):

$$\big[R_2(\mathbb{Z}/p^n\mathbb{Z}) : H\big] = \big[\operatorname{Span}_{\mathbb{Z}} \alpha_{S(p^n)} : H\big] \cdot \big(2^{-(\phi(p^n)/2)+1}\big) \det B^*(p^n)\,. \tag{26}$$

Formula (25) follows from (1), (24) and (26). □

Theorem 4.2 coincides with the first assertion in Theorem 1.1. We will offer next an important example of the subgroup H in Theorem 4.2, and prove the second assertion in Theorem 1.1 and Corollary 1.2. If $j \in S(p^n)$, let S_j be the surface defined by

$$S_j = \Big\{ \big[z_0, z_1, z_2\big] \in \mathbb{C}P^2 \;\Big|\; z_0^{p^n} - z_1^{p^n} + z_1^{p^n-k_j} z_2^{k_j} = 0 \Big\}\,. \tag{27}$$

In (27), k_j is defined by the conditions $k_j j \equiv -1 \pmod{p^n}$ and $0 < k_j < p^n$. A map of period p^n is defined in S_j by $f_j([z_0, z_1, z_2]) = \big[\lambda z_0, z_1, z_2\big]$. The fixed point set of f_j is the set $\big\{[0, \eta, 1] \mid \eta^{k_j} = 1\big\}$ together with the point $[0, 0, 1]$. The character of the equivariant signature of the cobordism class $[f_j, S_j]$ satisfies the equation $\operatorname{sign}([f_j, S_j]) = \varepsilon_{j/p^n}$, where

$$\varepsilon_{j/p^n} = k_j \alpha_{1/p^n} + \alpha_{j/p^n} \tag{28}$$

(see [1, Theorems 5.2], [4, p. 59], [6, 3.1 Lemma]). If $E(p^n) = \operatorname{Span}_{\mathbb{Z}} \varepsilon_{S(p^n)}$, then $E(p^n) \subset G(p^n)$. We will see that the index of $E(p^n)$ in $\operatorname{Span}_{\mathbb{Z}} \alpha_{S(p^n)}$ is finite and we will compute the index of $E(p^n)$ in $R_2(\mathbb{Z}/p^n\mathbb{Z})$ explicitly in our next theorem.

Theorem 4.3. *The index of $E(p^n)$ in $R_2(\mathbb{Z}/p^n\mathbb{Z})$ is $p^{(p^{n-1}-1)/2} h^-(p^n)$.*

Proof. It follows from formula (28) that $\mathrm{Span}_{\mathbb{Z}}\,\alpha_{S(p^n)}/E(p^n)$ is cyclic with generator $[\alpha_{1/p^n}]$ and that $p^n[\alpha_{1/p^n}] = 0$, that is the order of $[\alpha_{1/p^n}]$ divides p^n. If $q[\alpha_{1/p^n}] = 0$, then

$$q\alpha_{1/p^n} = \sum_{j\in S(p^n)} n_j(k_j\alpha_{1/p^n} + \alpha_{j/p^n}),$$

with $n_j \in \mathbb{Z}$. The set $\alpha_{S(p^n)}$ is rationally independent by [3, (3.3) Lemma], and so $n_j = 0$, $j \neq 1$, and $q = p^n n_1$. This means that the order of $[\alpha_{1/p^n}]$ is p^n, so $\mathrm{Span}_{\mathbb{Z}}\,\alpha_{S(p^n)}/E(p^n)$ is cyclic of order p^n. In particular $\big[\mathrm{Span}_{\mathbb{Z}}\,\alpha_{S(p^n)} : E(p^n)\big] = p^n$ and so Theorem 4.3 follows from (25). □

Corollary 4.4. ([4, Theorem 3.2]) *The index of $G(p)$ in $R_2(\mathbb{Z}/p\mathbb{Z})$ is $h^-(p)$.*

Proof. Corollary 4.4 follows from Theorem 4.3 in the special case $n = 1$ since $E(p) = G(p)$ (see [4, p. 59]). □

Theorem 4.3 and Corollary 4.4 are the same as the second assertion in Theorem 1.1 and Corollary 1.2, respectively. Theorem 4.2 is the first assertion in Theorem 1.1 and Theorem 3.6 contains Theorem 1.4. It remains to establish Theorems 1.3 and 1.5.

Corollary 4.5. *The index of $G(p^n)$ in $\mathrm{Span}_{\mathbb{Z}}\,\alpha_{S(p^n)}$ divides p^n and the index of $G(p^n)$ in $R_2(\mathbb{Z}/p^n\mathbb{Z})$ divides $p^{(p^{n-1}-1)/2}h^-(p^n)$.*

Proof. The assertions follow from Theorem 4.3 and (25) with $H = G(p^n)$. □

Corollary 4.6. *If H is a subgroup of $G(p^n)$ of finite index, then the index of H in $\mathrm{Span}_{\mathbb{Z}}\,\alpha_{T(p^n)}$ is finite and*

$$\big[R_2(\mathbb{Z}/p^n\mathbb{Z}) : H\big] = \big[\mathrm{Span}_{\mathbb{Z}}\,\alpha_{T(p^n)} : H\big]\cdot p^{-n}h^-(p^n)\,.$$

Proof. The assertions follow immediately from Theorems 3.6 and 4.2. □

Corollary 4.5 is Theorem 1.3 and Corollary 4.6 is Theorem 1.5. This completes the proofs of the theorems in the introduction since Theorem 1.1 is contained in Theorems 4.2 and 4.3, Corollary 1.2 is Corollary 4.4, and Theorem 1.4 is contained in Theorem 3.6.

REFERENCES

[1] D. Berend and G. Katz, *Separating topology and number theory in the Atiyah-Singer g-signature formula*, Duke Math. J. **61** (1990), no. 3, 939–971.

[2] A. I. Borevich and I. R. Shafarevich, *Number theory*, Translated from the Russian by Newcomb Greenleaf, Pure and Applied Mathematics, Vol. 20 Academic Press, New York-London 1966, x+435 pp.

[3] A. L. Edmonds and J. H. Ewing, *Remarks on the cobordism group of surface diffeomorphisms*, Math. Ann. **259** (1982), no. 4, 497–504.

[4] J. Ewing, *The image of the Atiyah-Bott map*, Math. Z. **165** (1979), no. 1, 53–71.

[5] E. R. Hansen, *A table of series and products*, Prentice-Hall Series in Automatic Computation, Englewood Cliffs, N.J., 1975, 523 pp.

[6] C. Kosniowski, *Generators of the $\mathbb{Z}/p$ bordism ring. Serendipity*, Math. Z. **149** (1976), no. 2, 121–130.

[7] R. D. Little, *Cyclic actions and divisible polynomials*, J. Pure Appl. Algebra **208** (2007), no. 3, 805–819.

[8] L. C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics, **83**, Springer-Verlag, New York, 1982, xi+389 pp.

R. D. LITTLE, DEPT. OF MATHEMATICS, U. OF HAWAII, HONOLULU, HAWAII 96822-2330
little@math.hawaii.edu