EVERY LENS SPACE CONTAINS A GENUS ONE HOMOLOGICALLY FIBERED KNOT

YUTA NOZAKI

ABSTRACT. We prove that every lens space contains a genus one homologically fibered knot, which is contrast to the fact that some lens spaces contain no genus one fibered knot. In the proof, the Chebotarev density theorem and binary quadratic forms in number theory play a key role. We also discuss the Alexander polynomial of homologically fibered knots.

1. Introduction

It is well known that every connected oriented closed (namely, compact and without boundary) 3-manifold X contains a fibered knot. In other words, X admits an open book decomposition with connected binding. The minimal genus $\mathrm{op}(X)$ of pages of all such open book decompositions of X is a fundamental invariant of X. For instance, $\mathrm{op}(X) = 0$ if and only if $X \cong S^3$. The concept of the invariant $\mathrm{op}(X)$ is similar to the support genus $\mathrm{sg}(\xi)$ introduced by Etnyre and Ozbagci [3], where ξ is a contact structure on X. The invariant $\mathrm{sg}(\xi)$ is defined to be the minimal genus of a page of all open book decompositions (whose bindings are not necessarily connected) of X supporting ξ.

Morimoto [8] started to study genus one fibered knots (GOF-knots) in lens spaces, and Baker [2, Theorem 4.3] completely determined which lens space $L(p, q)$ contains a GOF-knot, that is, we already know when $\mathrm{op}(L(p,q)) = 1$ holds. However, computation of $\mathrm{op}(X)$ is difficult in general.

Sakasai [10, Remark 6.10] introduced a homological analogue $\mathrm{hc}(X)$ of $\mathrm{op}(X)$, which is roughly defined to be the minimal genus of surfaces Σ whose complements are homologically $\Sigma \times [-1, 1]$. Precisely, $\mathrm{hc}(X)$ is defined in terms

of homology cobordisms or homologically fibered knots (see Definition 2.2), and $\mathrm{hc}(X) \le \mathrm{op}(X)$ holds by definition. The author was informed by Sakasai the following sufficient condition for $\mathrm{hc}(L(p,q)) = 1$ when q is odd: $p(p+4)$ or $p(p-4)$ is a quadratic residue mod q.

The purpose of this paper is to prove the following theorem and corollary which contain new results on the computation of $\mathrm{hc}(X)$ for various 3-manifolds X.

THEOREM 1.1. $\mathrm{hc}(L(p,q)) = 1$ holds for any lens space $L(p,q)$, or equivalently $L(p,q)$ contains a genus one homologically fibered knot.

Let $d(G)$ denote the minimum number of generators of a group G.

COROLLARY 1.2. The following hold for $g \in \mathbb{Z}_{\ge 1}$ and $p, n \in \mathbb{Z}_{\ge 2}$.
(1) $\mathrm{hc}(X) = 0$ if and only if $H_1(X) = 0$.
(2) $\mathrm{hc}(X) = g$ if $H_1(X)$ is isomorphic to $\mathbb{Z}^{2g-1}$ or $\mathbb{Z}^{2g}$.
(3) $\mathrm{hc}(X) = 1$ if $H_1(X) \cong \mathbb{Z}/p$.
(4) If X is a rational homology 3-sphere and the subgroup of $H_1(X)$ consisting of 2-torsions is cyclic (possibly trivial), then $\mathrm{hc}(X) \le d(H_1(X))$.
(5) $\mathrm{hc}(L(p_1, q_1) \sharp L(p_2, q_2)) = 2$ if p_1 divides p_2 and neither $q_1 q_2$ nor $-q_1 q_2$ is a quadratic residue mod p_1.
(6) Suppose $H_1(X) \cong \mathbb{Z} \oplus \mathbb{Z}/p$. Then, $\mathrm{hc}(X) = 1$ if there is $q \in \mathbb{Z}$ such that the torsion linking form λ_X is isomorphic to (q/p) and q or $-q$ is a quadratic residue mod p. Otherwise, $\mathrm{hc}(X) = 2$.

Note that $\mathrm{hc}(X)$ is *not* determined only by the isomorphism class of $H_1(X)$. Indeed, for two 3-manifolds $X_i = L(5,1) \sharp L(5,i)$ ($i = 1, 2$), we have $\mathrm{hc}(X_1) = 1 \ne \mathrm{hc}(X_2) = 2$ ([10, Remark 6.10]). On the other hand, Sakasai proved the following theorem.

THEOREM 1.3 ([10, Remark 6.10]). The invariant $\mathrm{hc}(X)$ depends only on the isomorphism class of the pair of $H_1(X)$ and the torsion linking form $\lambda_X \colon TH_1(X) \times TH_1(X) \to \mathbb{Q}/\mathbb{Z}$, where $TH_1(X)$ denotes the torsion subgroup of $H_1(X) := H_1(X; \mathbb{Z})$.

In fact, the torsion linking form of X_i is $(1/5) \oplus (i/5)$, and they are not isomorphic for $i = 1, 2$. In order to prove Theorem 1.1, we find a surface $\Sigma \subset L(p,q)$ of genus one whose complement $L(p,q) \setminus \mathrm{Int}(\Sigma \times [-1, 1])$ is a homology cobordism. (It is easy to see that $\mathrm{hc}(X) = 0$ if and only if X is an integral homology 3-sphere.) The following theorem (to be proved in Section 3 by using the Chebotarev density theorem) and a well-known fact about binary quadratic forms allow us to construct a desired surface Σ.

THEOREM 1.4. Let $m \in \mathbb{Z}$ and $n \in \mathbb{Z}_{>0} \setminus \{5\}$ be coprime. Then there exist $\varepsilon \in \{1, -1\}$ and an odd prime l such that the congruence equation $nx(x+1) \equiv \varepsilon$ mod l is solvable and $l \equiv m \mod n$.

In Section 2, we shall review the invariant $\mathrm{hc}(X)$ and prove Theorem 1.1. Section 3 is devoted to proving Theorem 1.4 based on number theory. In the final section, we focus on Seifert matrices of (homologically fibered) knots which are useful to study $\mathrm{hc}(X)$. Throughout this paper, $\Sigma_{g,b}$ denotes a connected oriented compact surface of genus g with b boundary components, and $L(p,q)$ denotes the lens space obtained from S^3 by Dehn surgery on an unknot along the slope $-p/q$, where $p \geq 2$ and q are coprime.

2. Homology cobordisms and proof of Theorem 1.1

We first review homology cobordisms following Garoufalidis and Levine [4, Section 2.4].

DEFINITION 2.1. A *homology cobordism over* $\Sigma_{g,1}$ is a triad (M, i_+, i_-), where M is an oriented compact 3-manifold and $i_+, i_- \colon \Sigma_{g,1} \to \partial M$ are embeddings satisfying

- i_+ is orientation-preserving and i_- is orientation-reversing;
- $i_+|_{\partial \Sigma_{g,1}} = i_-|_{\partial \Sigma_{g,1}}$;
- $i_+(\Sigma_{g,1}) \cup i_-(\Sigma_{g,1}) = \partial M$ and $i_+(\Sigma_{g,1}) \cap i_-(\Sigma_{g,1}) = i_\pm(\partial \Sigma_{g,1})$;
- The induced maps $(i_+)_*, (i_-)_* \colon H_*(\Sigma_{g,1}) \to H_*(M)$ are isomorphisms.

Note that the fourth condition is equivalent to the condition that M is connected and $i_\pm$ induce isomorphisms on $H_1(-)$. Sakasai [10, Definition 6.9, Remark 6.10] introduced the following invariant of 3-manifolds by using homology cobordisms.

DEFINITION 2.2. For a connected oriented closed 3-manifold X, $\mathrm{hc}(X) \in \mathbb{Z}_{\geq 0}$ is defined by

$$\mathrm{hc}(X) := \min\{g \in \mathbb{Z}_{\geq 0} \mid X \cong C_M \text{ for some } (M, i_+, i_-)\},$$

where C_M is the *closure* of a homology cobordism (M, i_+, i_-) over $\Sigma_{g,1}$ defined by

$$C_M := M/(i_+(x) \sim i_-(x), x \in \Sigma_{g,1}).$$

REMARK 2.3. The inequalities $\mathrm{hc}(X) \leq \mathrm{op}(X)$ and $\mathrm{hc}(X\sharp Y) \leq \mathrm{hc}(X) + \mathrm{hc}(Y)$ hold for any X, Y by definition. The gap $\mathrm{op}(X) - \mathrm{hc}(X)$ can be arbitrarily large. Indeed, let X be the connected sum of n copies of the Poincaré homology 3-sphere. Then we conclude that $\mathrm{hc}(X) = 0$ and $\mathrm{op}(X) \geq n$ by Remark 2.6.

For an embedding $\iota \colon \Sigma_{g,1} \xrightarrow{\cong} \Sigma \subset X$, we obtain the triad $(X \setminus \mathrm{Int}(\Sigma \times [-1,1]), \iota^-, \iota^+)$, where $\iota^\pm := \iota \times (\pm 1)$. Whether this triad is a homology cobordism or not depends only on the image of ι, and we simply say that $X \setminus \mathrm{Int}(\Sigma \times [-1,1])$ is a homology cobordism if the triad is so.

The following key lemma is a corollary of Proposition 4.1, though we give a direct proof in this section. Note that for coprime integers p, q there is an
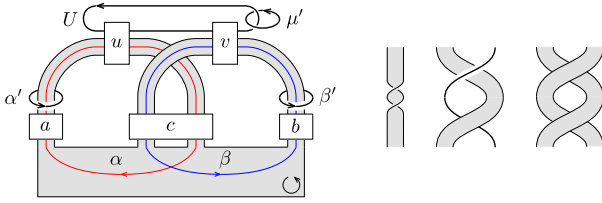
FIGURE 1. The surface $\Sigma_{a,b,c,u,v} \subset S^3_U(-p/q) = L(p,q)$, where $a, b, c, u, v \in \mathbb{Z}$. The box with $n \geq 0$ (resp. $n < 0$) represents suitable $|n|$ positive (resp. negative) full twists on the right.

integer solution $(x, y) = (r_0, s_0)$ of $py - qx = 1$, and then the other solutions have the form $(r_k, s_k) := (r_0 + kp, s_0 + kq)$ for each $k \in \mathbb{Z}$.

LEMMA 2.4. *The complement* $L(p, q) \setminus \mathrm{Int}(\Sigma \times [-1, 1])$ *of the surface* $\Sigma = \Sigma_{a,b,c,u,v}$ *illustrated in Figure* 1 *is a homology cobordism if and only if there exist* $\varepsilon \in \{1, -1\}$ *and* $k \in \mathbb{Z}$ *such that*

$$(2.1) \qquad \begin{pmatrix} bu^2 + (2c+1)uv + av^2 \\ c^2 + c - ab \end{pmatrix} = \varepsilon \begin{pmatrix} r_k \\ s_k \end{pmatrix}.$$

Proof. Let $N(U)$ denote a (closed) tubular neighborhood of U disjoint from $\Sigma \times [-1, 1]$ and μ'. Consider the Mayer–Vietoris sequence for

$$L(p, q) \setminus \mathrm{Int}\big(\Sigma \times [-1, 1]\big) = \big(S^3 \setminus \mathrm{Int}\big(\Sigma \times [-1, 1] \sqcup N(U)\big)\big) \cup_{\partial} D^2 \times S^1,$$

where the solid torus $D^2 \times S^1$ is glued by (the isotopy class of) a homeomorphism $\partial(D^2 \times S^1) \to \partial N(U)$ corresponding to $\left(\begin{smallmatrix} -p & r_0 \\ q & -s_0 \end{smallmatrix}\right) \in SL(2, \mathbb{Z})$. Then we have $H_1(L(p, q) \setminus \Sigma) \cong \mathrm{Coker}\, \iota$, where ι is the map

$$\iota \colon H_1\big(\partial(D^2 \times S^1)\big) \rightarrowtail H_1\big(S^3 \setminus (\Sigma \sqcup N(U))\big) \oplus H_1\big(D^2 \times S^1\big).$$

By the definition of Dehn surgery, the matrix of ι with respect to the bases $\{\mu, \lambda\}$ and $\{\alpha', \beta', \mu', \lambda\}$ is

$$A := \begin{pmatrix} qu & -s_0 u \\ -qv & s_0 v \\ -p & r_0 \\ 0 & 1 \end{pmatrix},$$

where μ and λ denote a meridian and longitude on $\partial(D^2 \times S^1)$, respectively.

Suppose that the complement is a homology cobordism, namely $\{\alpha_\sigma, \beta_\sigma\}$ is a basis of $\mathrm{Coker}\, \iota$ for each $\sigma = \pm$, where $\alpha_\pm := \alpha \times \{\pm 1\}$, $\beta_\pm := \beta \times \{\pm 1\}$. Then there is a basis $\mathcal{B}_\sigma = \{\alpha_\sigma, \beta_\sigma, *\}$ of $H_1(S^3 \setminus (\Sigma \sqcup N(U)))$ for each $\sigma = \pm$. Let $Q_\sigma \in GL(3, \mathbb{Z})$ be the matrix changing the basis $\{\alpha', \beta', \mu'\}$ to $\mathcal{B}_\sigma$. Then

we see that

$$Q_+ = \begin{pmatrix} a & c & * \\ c+1 & b & * \\ u & -v & * \end{pmatrix}, \qquad Q_- = \begin{pmatrix} a & c+1 & * \\ c & b & * \\ u & -v & * \end{pmatrix}.$$

Since $\{\alpha_\sigma, \beta_\sigma\}$ is a basis of $\operatorname{Coker} \iota$, the (2×2)-matrix at the bottom of the new matrix $(Q_\sigma^{-1} \oplus I_1)A$ of ι must belong to $GL(2, \mathbb{Z})$. Hence, the absolute value of its $(1, 3)$-entry equals 1, namely one has

$$(Q_\sigma)^{-1} \begin{pmatrix} qu \\ -qv \\ -p \end{pmatrix} = \begin{pmatrix} * \\ * \\ 1 \end{pmatrix}.$$

Here, since choosing another basis $\mathcal{B}'_\pm = \{\alpha_\sigma, \beta_\sigma, *'\}$ corresponds to elementary row operations using the entry 1, we may assume $*$'s in the last equality are zero. Then we conclude that

$$Q_+ = \begin{pmatrix} a & c & qu \\ c+1 & b & -qv \\ u & -v & -p \end{pmatrix}, \qquad Q_- = \begin{pmatrix} a & c+1 & qu \\ c & b & -qv \\ u & -v & -p \end{pmatrix}.$$

It follows from $|\det Q'_\pm| = 1$ that

$$\left| p\big(c^2 + c - ab\big) - q\big(bu^2 + (2c+1)uv + av^2\big) \right| = 1.$$

This completes one direction, and the other is shown by reversing the above argument. □

Let us prove the main theorem by using Lemma 2.4, Theorem 1.4 (to be proved later) and the following fact (see, for example, [1, Section 5.3]): For $n, \Delta \in \mathbb{Z}$, the congruence equation $z^2 \equiv \Delta \mod 4n$ is solvable if and only if there is a binary quadratic form $f(x, y)$ with discriminant Δ such that $f(x, y) = n$ has a primitive solution.

Proof of Theorem 1.1. We first consider the case $p = 5$. Since $L(5, 1) \cong L(5, 4)$ and $L(5, 2) \cong L(5, 3)$, it is enough to see the cases $q = 1, 3$. Lemma 2.4 shows that $L(5, 1) \setminus \Sigma_{0,0,0,1,1}$ is a homology cobordism. Indeed, $(r_0, s_0) = (-1, 0)$ and $\varepsilon = -1$ satisfy equation (2.1). Similarly, letting $(r_0, s_0) = (3, 2)$ and $\varepsilon = 1$, $L(5, 3) \setminus \Sigma_{0,0,1,1,1}$ is a homology cobordism.

Suppose $p \neq 5$. Putting $m = r_0$, $n = p$ in Theorem 1.4, we conclude that there are $\varepsilon \in \{1, -1\}$ and $k \in \mathbb{Z}$ such that $px(x+1) \equiv \varepsilon \mod r_k$ has a solution $x = x_0$. Here, $z_0 := 1 + 2x_0$ satisfies $z_0^2 \equiv 1 + 4\varepsilon s_k \mod 4\varepsilon r_k$. By the above fact, there is a quadratic form $f(x, y) = a'x^2 + b'xy + c'y^2$ such that $b'^2 - 4a'c' = 1 + 4\varepsilon s_k$ and $f(x, y) = \varepsilon r_k$ has a solution $(x, y) = (u, v)$. Then, integers $a := c'$, $b := a'$ and $c := (b' - 1)/2$ satisfy

$$\begin{pmatrix} bu^2 + (2c+1)uv + av^2 \\ c^2 + c - ab \end{pmatrix} = \varepsilon \begin{pmatrix} r_k \\ s_k \end{pmatrix}.$$

Therefore, we conclude from Lemma 2.4 that $\operatorname{hc}(L(p, q)) = 1$. □

REMARK 2.5. It follows from the proof of the above fact about quadratic forms that integers a, b, c, u, v are represented by $z_0, \varepsilon, r_k, s_k$. However, it seems difficult to represent these integers explicitly by p, q.

We sum up values or estimates of $\mathrm{hc}(X)$ for various X's as a corollary of Theorem 1.1. Recall that $d(G)$ denotes the minimum number of generators of a group G. (We set $d(\{1\}) = 0$ by convention.)

COROLLARY 1.2. *The following hold for $g \in \mathbb{Z}_{\geq 1}$ and $p, n \in \mathbb{Z}_{\geq 2}$.*

(1) $\mathrm{hc}(X) = 0$ *if and only if $H_1(X) = 0$.*
(2) $\mathrm{hc}(X) = g$ *if $H_1(X)$ is isomorphic to $\mathbb{Z}^{2g-1}$ or $\mathbb{Z}^{2g}$.*
(3) $\mathrm{hc}(X) = 1$ *if $H_1(X) \cong \mathbb{Z}/p$.*
(4) *If X is a rational homology 3-sphere and the subgroup of $H_1(X)$ consisting of 2-torsions is cyclic (possibly trivial), then $\mathrm{hc}(X) \leq d(H_1(X))$.*
(5) $\mathrm{hc}(L(p_1, q_1) \sharp L(p_2, q_2)) = 2$ *if p_1 divides p_2 and neither $q_1 q_2$ nor $-q_1 q_2$ is a quadratic residue* mod p_1.
(6) *Suppose $H_1(X) \cong \mathbb{Z} \oplus \mathbb{Z}/p$. Then, $\mathrm{hc}(X) = 1$ if there is $q \in \mathbb{Z}$ such that the torsion linking form λ_X is isomorphic to (q/p) and q or $-q$ is a quadratic residue* mod p. *Otherwise, $\mathrm{hc}(X) = 2$.*

REMARK 2.6. We have well-known inequalities related to Corollary 1.2(4):

- $d(H_1(X)) \leq 2\,\mathrm{hc}(X) \leq 2\,\mathrm{op}(X)$ and
- $d(H_1(X)) \leq d(\pi_1(X)) \leq g(X) \leq 2\,\mathrm{op}(X)$,

where $g(X)$ denotes the Heegaard genus of X. The first inequality is found in [10, Remark 6.1]. The second inequality in the second row follows that a Heegaard splitting of genus g gives a presentation of $\pi_1(X)$ with g generators. Also, when X admits an open book decomposition with a page $\Sigma_{g,1}$, the union of two pages divides X into two handlebodies of genus $2g$, and thus the third inequality holds.

Proof of Corollary 1.2(1)–(4). We first prove (1). If $H_1(X) = 0$, then the complement of any disk in X is a homology cobordism over $\Sigma_{0,1}$. The converse follows from the inequality $d(H_1(X)) \leq 2\,\mathrm{hc}(X)$ in Remark 2.6. (2) is due to Sakasai [10]. (3) is a direct consequence of Theorems 1.1 and 1.3 since a non-degenerate symmetric bilinear form on $\mathbb{Z}/p$ is isomorphic to $(q/p) = \lambda_{L(p,q)}$ for some q.

We next prove (4). Since $H_1(X)$ is finite, it is isomorphic to $\bigoplus_{i=1}^{s} \mathbb{Z}/p_i$ for some p_i's with $p_i \mid p_{i+1}$, where $s := d(H_1(X))$. It follows from [12, Theorem (4)] that λ_X is isomorphic to $\bigoplus_{i=1}^{s} (q_i/p_i)$ for some q_i's, hence λ_X is isomorphic to $\lambda_{L(p_1,q_1)\sharp\cdots\sharp L(p_s,q_s)}$. Therefore, Theorem 1.1 shows $\mathrm{hc}(X) \leq s$. □

The proofs of (5) and (6) are given in the end of Section 4 since we need results of Section 4.

3. Number theory and proof of Theorem 1.4

The goal of this section is to prove Theorem 1.4, which was used in the proof of Theorem 1.1. We briefly review the Artin symbol of a prime ideal only for the case of Abelian extensions following [6, Chapter X, Section 1] and [9, Chapter VI, Section 7]. Let k be a number field (assumed to be finite over $\mathbb{Q}$) and K/k a finite Abelian extension. Let $\mathfrak{p} \neq 0$ be a prime ideal of $\mathfrak{o}_k$ unramified in K/k, where $\mathfrak{o}_k$ denotes the ring of integers of k. Let $\mathfrak{P}$ be a prime ideal of $\mathfrak{o}_K$ lying above $\mathfrak{p}$, that is, $\mathfrak{P} \cap k = \mathfrak{p}$. Then there exists a unique element of the decomposition group $\{\sigma \in \mathrm{Gal}(K/k) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$ of $\mathfrak{P}$ satisfying $\sigma(x) \equiv x^{N(\mathfrak{p})} \mod \mathfrak{P}$ for all $x \in \mathfrak{o}_K$, where $N(\mathfrak{p})$ denotes the order of the residue field $\mathfrak{o}_k/\mathfrak{p}$. The element is independent of the choice of $\mathfrak{P}$. It is denoted by $(\frac{K/k}{\mathfrak{p}})$ and called the *Artin symbol* of $\mathfrak{p}$.

EXAMPLE 3.1 ([6, Chapter X, Section 1]). We review two well-known examples used in this paper. Let $a \in \mathbb{Z}$ be not a square, Δ_a be the discriminant of $\mathbb{Q}(\sqrt{a})$, p be a prime with $\gcd(\Delta_a, p) = 1$. Then, $p\mathbb{Z}$ is unramified and we deduce

$$\left(\frac{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}{p\mathbb{Z}} \right) = \begin{cases} \mathrm{id}_{\mathbb{Q}(\sqrt{a})} & \text{if } \Delta_a \text{ is a quadratic residue mod } p, \\ [\sqrt{a} \mapsto -\sqrt{a}] & \text{otherwise.} \end{cases}$$

Next, for a primitive nth root of unity ζ_n and a prime p with $\gcd(n, p) = 1$, the ideal $p\mathbb{Z}$ is unramified and $(\frac{\mathbb{Q}(\zeta_n)/\mathbb{Q}}{p\mathbb{Z}}) = [\zeta_n \mapsto \zeta_n^p]$ holds.

LEMMA 3.2. *Let K_1/k, K_2/k be Abelian extensions, C be a subset of $G_1 \times G_2$ with $\iota^{-1}(C) \neq \emptyset$, where G_i denotes $\mathrm{Gal}(K_i/k)$ and $\iota \colon \mathrm{Gal}(K_1 K_2/k) \to G_1 \times G_2$ is defined by $\iota(\sigma) = (\sigma|_{K_1}, \sigma|_{K_2})$. Then*

$$S := \left\{ \mathfrak{p} \,\middle|\, \begin{array}{l} \mathfrak{p} \text{ is a prime ideal of } \mathfrak{o}_k \\ \text{unramified in } K_1 \text{ and } K_2 \end{array} \text{ and } \left(\left(\frac{K_1/k}{\mathfrak{p}} \right), \left(\frac{K_2/k}{\mathfrak{p}} \right) \right) \in C \right\}$$

is an infinite set.

Proof. First note that $K_1 K_2/k$ is a Galois extension with $G = \mathrm{Gal}(K_1 K_2/k)$ Abelian, and the homomorphism $\iota \colon G \to G_1 \times G_2$ is injective. We define the set S' by

$$S' := \left\{ \mathfrak{p} \,\middle|\, \begin{array}{l} \mathfrak{p} \text{ is a prime ideal of } \mathfrak{o}_k \\ \text{unramified in } K_1 K_2 \end{array} \text{ and } \left(\frac{K_1 K_2/k}{\mathfrak{p}} \right) \in \iota^{-1}(C) \right\}.$$

By the Chebotarev density theorem (see, for example, [6, Chapter VIII, Theorem 10], [9, Chapter VII, Theorem 13.4]), we have $d(S') = |\iota^{-1}(C)|/|G| > 0$, where $d(S')$ is the Dirichlet density of S' (see [6, Chapter VIII, Section 4], [9, Chapter VII, Section 13]). Hence, S' is infinite. On the other hand, the consistency property [6, Chapter X, Section 1] asserts $S' \subset S$, and thus S is also infinite. $\qquad\square$

LEMMA 3.3. *For $a, m \in \mathbb{Z}$, $n \in \mathbb{Z}_{>0}$ with $\sqrt{a} \notin \mathbb{Q}(\zeta_n)$ and $\gcd(m,n) = 1$,*

$$S := \{p \mid p \text{ is a prime, } a \text{ is a quadratic residue mod } p \text{ and } p \equiv m \mod n\}$$

is an infinite set.

Proof. Put $k = \mathbb{Q}$, $K_1 = k(\sqrt{a})$, $K_2 = k(\zeta_n)$ and $C = \{(\mathrm{id}_{K_1}, [\zeta_n \mapsto \zeta_n^m])\}$. Since $K_1 \cap K_2 = k$, the map ι in Lemma 3.2 is an isomorphism, and thus $\iota^{-1}(C) \neq \emptyset$. It follows from Lemma 3.2 that

$$\left\{ p \left| \begin{matrix} p > \max\{\Delta_a, n\} \\ \text{is a prime,} \end{matrix} \right. \left(\frac{K_1/k}{p\mathbb{Z}}\right) = \mathrm{id}_{K_1} \text{ and } \left(\frac{K_2/k}{p\mathbb{Z}}\right) = [\zeta_n \mapsto \zeta_n^m] \right\}$$

is infinite. Here, Example 3.1 implies that this set is contained in S. □

LEMMA 3.4. *For a positive integer $n \neq 5$, $\sqrt{n(n+4)}$ or $\sqrt{n(n-4)}$ does not belong to the nth cyclotomic field $\mathbb{Q}(\zeta_n)$.*

Proof. The cases $n = 1, 2$ are obvious since $\mathbb{Q}(\zeta_n) = \mathbb{Q}$. For $n > 2$, there are four cases: (i) $v_2(n) = 0$, (ii) $v_2(n) = 1$, (iii) $v_2(n) = 2$, (iv) $v_2(n) \geq 3$, where v_2 is the 2-adic valuation for $\mathbb{Z}$. We only discuss (i) and (iv), and the other cases are shown similarly. In general, $\sqrt{a} \in \mathbb{Q}(\zeta_n)$ if and only if $a \in \mathbb{Z}$ is a product of a square and some integers in

$$\left\{(-1)^{(p-1)/2} p \mid p \text{ is an odd prime factor of } n\right\} \cup \begin{cases} \emptyset & \text{if } v_2(n) < 2, \\ \{-1\} & \text{if } v_2(n) = 2, \\ \{-1, 2\} & \text{if } v_2(n) > 2 \end{cases}$$

(see, for example, [13, Corollary 4.5.4]).

(i) Assume that $\sqrt{n(n+4)}, \sqrt{n(n-4)} \in \mathbb{Q}(\zeta_n)$. Then $n(n \pm 4)$ must be certain products as mentioned above. It follows from $\gcd(n \pm 4, n) = 1$ that both $n + 4$ and $n - 4$ are squares, though that is impossible except when $n = 5$.

(iv) Assume that $\sqrt{n(n \pm 4)} \in \mathbb{Q}(\zeta_n)$. Since $\gcd((n \pm 4)/4, n) = 1$, the same argument shows that $n/4 \pm 1$ are squares. This is a contradiction. □

Proof of Theorem 1.4. It follows from Lemmas 3.3 and 3.4 that there are $\varepsilon \in \{1, -1\}$ and an odd prime l such that $n(n + 4\varepsilon)$ is a quadratic residue mod l and $l \equiv m \mod n$. Therefore, by $\gcd(l, n) = 1$, $n(n + 4\varepsilon)$ is a quadratic residue mod l if and only if $(2nx + n)^2 \equiv n^2 + 4\varepsilon n \mod l$ is solvable. Moreover, this congruence equation is equivalent to $nx(x + 1) \equiv \varepsilon \mod l$. □

REMARK 3.5. The above proof (and the case $p = 5$ in the proof of Theorem 1.1) claims that for any $L(p, q')$ there exists an odd integer q such that $L(p, q)$ is homeomorphic to $L(p, q')$ and $p(p + 4)$ or $p(p - 4)$ is a quadratic residue mod q, which is Sakasai's sufficient condition in Section 1.

Even if $n = 5$, Theorem 1.4 holds for $m \equiv 1, 3, 4 \mod 5$. Indeed, one can choose $(\varepsilon, l) = (-1, 11), (1, 3), (1, 19)$ respectively. However, in the case $m \equiv 2 \mod 5$, Theorem 1.4 fails since neither $5(5 + 4)$ nor $5(5 - 4)$ is a quadratic residue mod m by the quadratic reciprocity law.
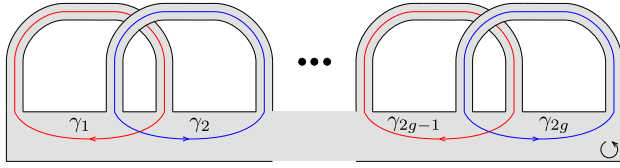
FIGURE 2. Oriented curves $\gamma_1, \ldots, \gamma_{2g}$ on the surface $\Sigma_{g,1}$.

4. Homologically fibered knots and the Alexander polynomial

The aims of this section are to complete the proof of Corollary 1.2 and to characterize homologically fibered knots in a rational homology 3-sphere in terms of the Alexander polynomial. These are achieved by Proposition 4.1 below.

Let Y be a rational homology 3-sphere, $\iota\colon \Sigma_{g,1} \xrightarrow{\cong} \Sigma \subset Y$ an embedding. Let $S = (s_{ij})_{i,j} \in M_{2g}(\mathbb{Q})$ be the Seifert matrix of Σ with respect to $\{\iota(\gamma_1), \ldots, \iota(\gamma_{2g})\}$ (see Figure 2), that is, $s_{ij} \in \mathbb{Q}$ is the linking number $\mathrm{lk}_Y(\iota(\gamma_i), \gamma_j^+)$ of two oriented curves $\iota(\gamma_i)$ and $\gamma_j^+ := \iota^+(\gamma_j)$ in Y (see [7, Section 1.2] for example). Here, S can be regarded as the matrix of the linear map $(\iota^+)_* \otimes \mathrm{id}_{\mathbb{Q}} \colon H_1(\Sigma_{g,1}; \mathbb{Q}) \to H_1(Y \setminus \Sigma; \mathbb{Q})$ with respect to $\{[\gamma_1], \ldots, [\gamma_{2g}]\}$ and $\{[\gamma_1'], \ldots, [\gamma_{2g}']\}$, where $\gamma_i' \subset Y \setminus \Sigma$ is a meridian of $\iota(\gamma_i)$. Indeed, by the definition of the linking number lk_Y, we have

$$[\gamma_j^+] = \sum_{i=1}^{2g} \mathrm{lk}_Y\big(\iota(\gamma_i), \gamma_j^+\big)[\gamma_i'] \in H_1\big(Y \setminus \iota(\gamma_1 \cup \cdots \cup \gamma_{2g}); \mathbb{Q}\big) \xleftarrow{\cong} H_1(Y \setminus \Sigma; \mathbb{Q}).$$

Similarly, S^T is regarded as the matrix of $(\iota^-)_* \otimes \mathrm{id}_{\mathbb{Q}}$. The definition of lk_Y also implies that $S - S^T = \bigoplus^g \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) =: J$.

PROPOSITION 4.1. $(Y \setminus \mathrm{Int}(\Sigma \times [-1,1]), \iota^-, \iota^+)$ *is a homology cobordism if and only if* $|H_1(Y)||\det S| = 1$.

Proof. Let $TH_1(Y \setminus \Sigma)$ denote the torsion subgroup of $H_1(Y \setminus \Sigma)$, and put $F := H_1(Y \setminus \Sigma)/T \cong \mathbb{Z}^{2g}$. Let $\mathcal{B}$ be a basis of F, $A_\pm \in GL(2g, \mathbb{Z})$ the matrices of $\mathrm{pr} \circ (\iota^\pm)_* \colon H_1(\Sigma_{g,1}) \to F$ with respect to $\{[\gamma_1], \ldots, [\gamma_{2g}]\}$ and $\mathcal{B}$. Since $\mathcal{B}$ can be regarded as a basis of $F \otimes \mathbb{Q} = H_1(Y \setminus \Sigma; \mathbb{Q})$, we have the matrix $Q \in GL(2g, \mathbb{Q})$ changing the basis $\mathcal{B}$ to $\{[\gamma_1'], \ldots, [\gamma_{2g}']\}$. Then one has $Q^{-1}A_+ = S$ and $Q^{-1}A_- = S^T = S - J$, and hence $A_+ - A_- = QJ \in M_{2g}(\mathbb{Z}) \cap GL(2g, \mathbb{Q})$.

Let $\widetilde{\Sigma} := \Sigma \times [-1,1]$. The Mayer–Vietoris sequence for $Y = (Y \setminus \mathrm{Int}\,\widetilde{\Sigma}) \cup \widetilde{\Sigma}$ gives the short exact sequence

$$0 \to H_1(\partial\widetilde{\Sigma}) \xrightarrow{\phi} H_1(Y \setminus \mathrm{Int}\,\widetilde{\Sigma}) \oplus H_1(\Sigma) \to H_1(Y) \to 0.$$

Identifying $H_1(\partial\widetilde{\Sigma})$ with $H_1(\Sigma \times \{1\}) \oplus H_1(\Sigma \times \{-1\})$, we have the commutative diagram

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z}^{2g} \oplus \mathbb{Z}^{2g} & \xrightarrow{\ \phi\ } & (\mathbb{Z}^{2g} \oplus T) \oplus \mathbb{Z}^{2g} & \longrightarrow & H_1(Y) & \longrightarrow & 0 \ \text{(exact)} \\
& & \Big\| & & \Big\downarrow{\mathrm{pr}} & & \Big\downarrow{\overline{\mathrm{pr}}} & & \\
0 & \longrightarrow & \mathbb{Z}^{2g} \oplus \mathbb{Z}^{2g} & \xrightarrow{\ \overline{\phi}\ } & \mathbb{Z}^{2g} \oplus \mathbb{Z}^{2g} & \longrightarrow & \mathrm{Coker}\,\overline{\phi} & \longrightarrow & 0 \ \text{(exact)},
\end{array}
$$

where $\overline{\phi}$ and $\overline{\mathrm{pr}}$ are, respectively, the induced maps by ϕ and pr in the diagram. Here, the matrix of $\overline{\phi}$ is $\left(\begin{smallmatrix} A_+ & A_- \\ I_{2g} & I_{2g} \end{smallmatrix}\right)$, which is transformed to $\left(\begin{smallmatrix} QJ & A_- \\ O & I_{2g} \end{smallmatrix}\right)$ by elementary column operations.

Suppose $|H_1(Y)||\det S| = 1$. The exactness of the lower row implies that

$$
|\mathrm{Coker}\,\overline{\phi}| = |\det Q| = \left|\det(A_+ S^{-1})\right| = |\det A_+||H_1(Y)|.
$$

It follows from the surjectivity of $\overline{\mathrm{pr}}$ that $|\det A_+| = 1$, and hence

$$
|\det A_-| = \left|\det(QS^T)\right| = \left|\det(QS)\right| = 1.
$$

Finally, the five lemma shows that $TH_1(Y \setminus \Sigma) = 0$, and thus the maps $(\iota^{\pm})_*$ are isomorphisms.

Conversely, if $Y \setminus \mathrm{Int}(\Sigma \times [-1,1])$ is a homology cobordism, then we have $TH_1(Y \setminus \Sigma) = 0$ and $|\det A_\pm| = 1$. It follows that

$$
\left|H_1(Y)\right||\det S| = |\det QJ|\left|\det Q^{-1}A_+\right| = 1.
$$

This completes the proof. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Alternative proof of Lemma 2.4. We first compute the Seifert matrix $S = (s_{ij})$ of $\Sigma = \Sigma_{a,b,c,u,v}$ with respect to $\{\alpha, \beta\}$. Let μ'' be a parallel copy of μ' drawn in Figure 1 with $\mathrm{lk}_{S^3}(\mu', \mu'') = 0$. We see that $\mathrm{lk}_{L(p,q)}(\mu', \mu'') = q/p$ by the definition of Dehn surgery and the linking number, and thus

$$
s_{12} = \mathrm{lk}_{L(p,q)}(\alpha, \beta^+) = c - uv\,\mathrm{lk}_{L(p,q)}(\mu', \mu'') = c - \frac{q}{p}uv.
$$

One can compute the other entries s_{ij} similarly and conclude that

$$
(4.1) \qquad\qquad S = \begin{pmatrix} a + \frac{q}{p}u^2 & c - \frac{q}{p}uv \\ c + 1 - \frac{q}{p}uv & b + \frac{q}{p}v^2 \end{pmatrix}.
$$

Since

$$
p\det S = -p(c^2 + c - ab) + q(bu^2 + (2c+1)uv + av^2),
$$

if the complement is a homology cobordism, then Proposition 4.1 shows that there are ε and k as in Lemma 2.4. Conversely, the existence of ε and k implies that $p|\det S| = 1$. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

The following terminology was introduced by Goda and Sakasai [5, Definition 3.1] in the case $X = S^3$ (see also [10, Definition 7.1]).

DEFINITION 4.2. An oriented knot K in a connected oriented closed 3-manifold X is called a *homologically fibered knot of genus g* if there is a Seifert surface of K such that $X \setminus \mathrm{Int}(\Sigma \times [-1, 1])$ is a homology cobordism over $\Sigma_{g,1}$.

By definition, $\mathrm{hc}(X) = g$ if and only if X contains a homologically fibered knot of genus g, but does not contain one of genus $g - 1$.

REMARK 4.3. If X is a rational homology 3-sphere, then Corollary 4.5 shows that g in Definition 4.2 must be equal to the *knot genus $g(K)$* of K.

We next see that homologically fibered knots are characterized by the Alexander polynomial. Let K be an oriented knot in a rational homology 3-sphere Y. We define the *Alexander polynomial $\Delta_K(t)$* of K by

$$\Delta_K(t) := |H_1(Y)| \det\left(t^{1/2} S - t^{-1/2} S^T\right) \in \mathbb{Z}\left[t, t^{-1}\right],$$

where S is a Seifert matrix of a Seifert surface Σ of K (see, for example, [7, Proposition 2.3.13]). By definition, $\Delta_K(t)$ should be palindromic and satisfy $\Delta_K(1) = |H_1(Y)|$, and its breadth is less than or equal to $2g(K)$.

EXAMPLE 4.4. Suppose that $L(p, q) \setminus \mathrm{Int}(\Sigma_{a,b,c,u,v} \times [-1, 1])$ is a homology cobordism (see Figure 1). Then there exists $\varepsilon \in \{1, -1\}$ as in Lemma 2.4, and using the Seifert matrix (4.1), one can compute the Alexander polynomial of $K = \partial \Sigma_{a,b,c,u,v}$ in $L(p, q)$:

$$\Delta_K(t) = p - \varepsilon\left(t - 2 + t^{-1}\right).$$

The next result is a corollary of Proposition 4.1, which is well known in the case $Y = S^3$ (see [5, Proposition 3.2]).

COROLLARY 4.5. *An oriented knot K in Y is homologically fibered if and only if $\Delta_K(t)$ is monic (up to sign) and its breadth equals $2g(K)$.*

Proof. In general, for $S \in GL(2g, \mathbb{Q})$, the highest degree term of $\det(t^{1/2}S - t^{-1/2}S^T)$ is equal to $(\det S)t^g$. Therefore, Proposition 4.1 proves the corollary. $\square$

Finally, we complete the rest of the proof of Corollary 1.2 by using Theorem 1.1 and Proposition 4.1.

Proofs of Corollary 1.2(5) and (6). (5) For $X = L(p_1, q_1) \sharp L(p_2, q_2)$ with $p_1 \mid p_2$, we know that $\mathrm{hc}(X)$ equals 1 or 2 by Theorem 1.1. Suppose that $\mathrm{hc}(X) = 1$, namely there is $\Sigma_{1,1}$ in X whose complement is a homology cobordism. We find a surface of the form $\Sigma_{a,b,c,u_1,u_2,v_1,v_2}$ (see Figure 3) whose Seifert matrix S is same as a Seifert matrix of $\Sigma_{1,1}$. Then, by an argument similar to the alternative proof of Lemma 2.4, one concludes that

$$S = \begin{pmatrix} a + \frac{q_1}{p_1}u_1^2 + \frac{q_2}{p_2}u_2^2 & c - \frac{q_1}{p_1}u_1v_1 - \frac{q_2}{p_2}u_2v_2 \\ c + 1 - \frac{q_1}{p_1}u_1v_1 - \frac{q_2}{p_2}u_2v_2 & b + \frac{q_1}{p_1}v_1^2 + \frac{q_2}{p_2}v_2^2 \end{pmatrix} \in \frac{1}{p_2}M_2(\mathbb{Z}).$$
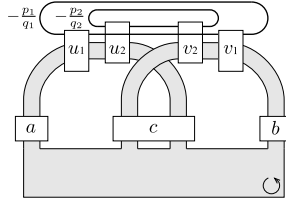
FIGURE 3. The surface $\Sigma_{a,b,c,u_1,u_2,v_1,v_2} \subset L(p_1,q_1)\sharp L(p_2,q_2)$, where the indices of Σ are integers like Figure 1.

It follows from Proposition 4.1 that

$$1 = \left|H_1(X)\right|\left|\det S\right| \equiv \varepsilon q_1 q_2 (u_1 u_2 - v_1 v_2)^2 \mod p_1$$

for some $\varepsilon \in \{1, -1\}$. Thus, $q_1 q_2$ or $-q_1 q_2$ is a quadratic residue mod p_1.

(6) Theorem 1.3 allows us to assume that $X = (S^1 \times S^2)\sharp L(p,q)$. By Theorem 1.1, it suffices to prove that $\mathrm{hc}(X) = 1$ if and only if q or $-q$ is a quadratic residue mod p. Suppose that $\mathrm{hc}(X) = 1$. There is $A \in SL(2,\mathbb{Z})$ such that the closure C of the homology cobordism $(\Sigma_{1,1} \times [-1,1], \mathrm{incl}, \widetilde{A})$ is Borromean surgery equivalent to X, where $\widetilde{A}$ is a homeomorphism of $\Sigma_{1,1}$ inducing A on $H_1(\Sigma_{1,1})$ (see [10, Section 6.3]). Here we have $\det(A - I_2) = 0$ since the Mayer–Vietoris sequence for $C = \Sigma_{1,1} \times [-1,0] \cup \Sigma_{1,1} \times [0,1]$ shows that $\mathrm{Coker}(A - I_2) \cong H_1(C)$. Therefore, by the proof of [11, Proposition 2], A is conjugate to $\left(\begin{smallmatrix} 1 & 0 \\ u & 1 \end{smallmatrix}\right)$ in $SL(2,\mathbb{Z})$ for some $u \in \mathbb{Z}$. Now, u must be εp for some $\varepsilon \in \{1, -1\}$, and one can choose $\widetilde{A}$ so that $C \cong (S^1 \times S^2)\sharp L(p,\varepsilon)$. Thus, the torsion linking form (q/p) is isomorphic to (ε/p).

In particular, the above argument implies that $(S^1 \times S^2)\sharp L(p,\varepsilon)$ is the closure of a homology cobordism over $\Sigma_{1,1}$ for each $\varepsilon = \pm 1$, which proves the converse. $\qquad\square$

REFERENCES

[1] A. Baker, *A concise introduction to the theory of numbers*, Cambridge University Press, Cambridge, 1984. MR 0781734

[2] K. L. Baker, *Counting genus one fibered knots in lens spaces*, Michigan Math. J. **63** (2014), no. 3, 553–569. MR 3255691

[3] J. B. Etnyre and B. Ozbagci, *Invariants of contact structures from open books*, Trans. Amer. Math. Soc. **360** (2008), no. 6, 3133–3151. MR 2379791

[4] S. Garoufalidis and J. Levine, *Tree-level invariants of three-manifolds, Massey products and the Johnson homomorphism*, Graphs and patterns in mathematics and theoretical physics, Proc. Sympos. Pure Math., vol. 73, Amer. Math. Soc., Providence, RI, 2005, pp. 173–203. MR 2131016

[5] H. Goda and T. Sakasai, *Homology cylinders and sutured manifolds for homologically fibered knots*, Tokyo J. Math. **36** (2013), no. 1, 85–111. MR 3112377

[6] S. Lang, *Algebraic number theory*, 2nd ed., Graduate Texts in Mathematics, vol. 110, Springer, New York, 1994. MR 1282723

[7] C. Lescop, *Global surgery formula for the Casson–Walker invariant*, Annals of Mathematics Studies, vol. 140, Princeton University Press, Princeton, NJ, 1996. MR 1372947

[8] K. Morimoto, *Genus one fibered knots in lens spaces*, J. Math. Soc. Japan **41** (1989), no. 1, 81–96. MR 0972166

[9] J. Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, with a foreword by G. Harder. MR 1697859

[10] T. Sakasai, *Johnson–Morita theory in mapping class groups and monoids of homology cobordisms of surfaces*, Winter Braids Lecture Notes **3** (2016), no. 4, 1–25. MR 3707745

[11] M. Takahashi and M. Ochiai, *Heegaard diagrams of torus bundles over S^1*, Comment. Math. Univ. St. Pauli **31** (1982), no. 1, 63–69. MR 0674582

[12] C. T. C. Wall, *Quadratic forms on finite groups, and related topics*, Topology **2** (1963), 281–298. MR 0156890

[13] S. H. Weintraub, *Galois theory*, 2nd ed., Universitext, Springer, New York, 2009. MR 2459247

Yuta Nozaki, Graduate School of Mathematical Sciences, The University of Tokyo, 3-8-1 Komaba, Meguro-ku, Tokyo, 153-8914, Japan

E-mail address: nozaki@ms.u-tokyo.ac.jp