

# LINEAR REPRESENTATIONS OF A KNOT GROUP OVER A FINITE RING AND ALEXANDER POLYNOMIAL AS AN OBSTRUCTION

TERUAKI KITANO

## 1. INTRODUCTION

Let  $K$  be a knot in  $S^3$  and  $G(K)$  its knot group  $\pi_1(S^3 - K)$ . Here we write  $\alpha : G(K) \rightarrow \mathbb{Z} = \langle t \rangle$  for the abelianization of  $G(K)$ . In this paper, we assume

- any presentation of  $G(K)$  is a Wirtinger presentation,
- its Alexander polynomial  $\Delta_K(t)$  is a polynomial, that is, its lowest degree term is a constant term.

There are many studies on linear representations of  $G(K)$  over a finite field or a finite ring. In general it is not easy to see when the set of non commutative  $SL(2, \mathbb{Z}/d)$ -representations is not empty.

Then we consider the following problem to be easier.

**Problem 1.1.** *Does there exist a non commutative representation of  $G(K)$  in  $SL(2, \mathbb{Z}/d)$  for infinitely many integers  $d \in \mathbb{Z}_+ = \{n \in \mathbb{Z} \mid n > 0\}$ ?*

We can prove the following by using zeros of Alexander polynomial.

**Theorem 1.2.** *If  $\Delta_K(t) \neq 1$ , then there exists a non commutative representation  $G(K) \rightarrow GL(2, \mathbb{Z}/d)$  for infinitely many  $d \in \mathbb{Z}_+$ .*

Further if the Alexander polynomial has a special form, we can prove the following.

**Theorem 1.3.** *If  $\Delta_K(t)$  can be decomposed to a product  $f(t)g(t)$  of polynomials with  $f(t) = at^2 - bt + a$ ,  $b \geq a > 0$  and  $2a - b = \pm 1$ , then there exists a non commutative representation  $G(K) \rightarrow SL(2, \mathbb{Z}/p)$  for infinitely many prime numbers  $p \in \mathbb{Z}_+$ .*

**Remark 1.4.** If there exists an epimorphism  $G(K) \rightarrow G(K')$ , then  $\Delta_K(t)$  has the form as above.

## 2. THEOREM OF DE RHAM

We recall a formulation of the Alexander polynomial by de Rham from the point of deformations of linear representations.

We fix a Wirtinger presentation of  $K$  as

$$G(K) = \langle x_1, \dots, x_n \mid r_1, \dots, r_{n-1} \rangle.$$

Under this presentation, we can assume  $\alpha(x_1) = \dots = \alpha(x_n) = t$ .

Any homomorphism  $\varphi_0 : G(K) \rightarrow \mathbb{C}^* = \mathbb{C} - \{0\}$  can be decomposed to  $\varphi_0 = \bar{\varphi}_0 \circ \alpha$  where  $\bar{\varphi}_0 : \langle t \rangle \cong \mathbb{Z} \rightarrow \mathbb{C}^*$  because  $\mathbb{C}^*$  is an abelian group.

Now we take a map  $\varphi : \{x_1, \dots, x_n\} \rightarrow GL(2; \mathbb{C})$  as

$$\varphi(x_1) = \begin{pmatrix} a & b_1 \\ 0 & 1 \end{pmatrix}, \dots, \varphi(x_n) = \begin{pmatrix} a & b_n \\ 0 & 1 \end{pmatrix}$$

where  $a = \varphi_0(x_1) = \dots = \varphi_0(x_n) \in \mathbb{C}^*$  and  $b_1, \dots, b_n \in \mathbb{C}$ .

We consider the problem when  $\varphi$  can be extended to the whole  $G(K)$  as a homomorphism. We put

$$\mathbf{b} = {}^t(b_1, \dots, b_n) \in \mathbb{C}^n.$$

**Remark 2.1.** If  $b_1 = \dots = b_n = b \in \mathbb{C}$ , that is,  $\mathbf{b} = {}^t(b, b, \dots, b)$ , then it can be done as an abelian representation, because  $\varphi(x_1) = \dots = \varphi(x_n)$ .

From now we assume that  $\mathbf{b} \neq {}^t(b, b, \dots, b)$ . Here we define a map  $\psi : \{x_1, \dots, x_n\} \rightarrow \mathbb{C}$  by  $\psi(x_i) = b_i$ .

**Definition 2.2.** A map  $\chi : G(K) \rightarrow \mathbb{C}$  is called to be a crossed homomorphism with respect to  $\varphi_0$  if it satisfies  $\chi(xy) = \chi(x) + \varphi_0(x)\chi(y)$  for any  $x, y \in G(K)$ .

**Lemma 2.3.** *The above map  $\varphi$  can be extended to  $G(K)$  as a homomorphism if and only if  $\psi$  can be extended to  $G(K)$  as a crossed homomorphism.*

Hence we consider when  $\psi$  can be done to  $G(K)$  as a crossed homomorphism.

Let  $F_n$  denote the free group of rank  $n$  generated by  $x_1, \dots, x_n$ . We fix a natural surjection  $F_n \rightarrow G(K)$ .

**Definition 2.4.** The  $\mathbb{Z}F_n$ -module  $DF_n$  is defined as follows.

- generators:  $dg$  ( $g \in F_n$ ),
- relators:  $d(gg') = dg + gdg'$  ( $g, g' \in F_n$ ).

**Remark 2.5.**  $DF_n$  is the free  $\mathbb{Z}F_n$ -module generated by  $dx_1, \dots, dx_n$ .

The  $\mathbb{Z}G(K)$ -module  $DG(K)$  can be defined similarly by adding relations  $dr_1 = \dots = dr_{n-1} = 0$ .

Here we consider a map

$$d : F_n \ni g \mapsto dg \in DF_n.$$

This is a crossed homomorphism with respect to the natural action of  $F_n$  on  $DF_n$  because  $d(gg') = dg + gdg'$  in  $DF_n$ . The following equality is well known in the theory of Fox's free derivatives;

$$dg = \sum_{i=1}^n \frac{\partial g}{\partial x_i} dx_i.$$

By the natural map  $F_n \rightarrow G(K)$ , we consider  $\varphi$  and  $\psi$  as maps on  $F_n$ . We use the same symbol for them.

Now we define  $\mathbb{Z}F_n$ -homomorphism  $\bar{\psi} : DF_n \rightarrow \mathbb{C}$  by

$$\begin{aligned} \bar{\psi} \left( \sum_{i=1}^n \lambda_i g_i dx_i \right) &= \sum_{i=1}^n \lambda_i \varphi_0(g_i) \psi(x_i) \\ &= \sum_{i=1}^n \lambda_i \varphi_0(g_i) b_i \end{aligned}$$

for any  $\sum_{i=1}^n \lambda_i g_i dx_i \in DF_n$  where  $\lambda_i \in \mathbb{Z}, g_i \in F_n$ .

**Lemma 2.6.** *The composite map*

$$\psi = \bar{\psi} \circ d : F_n \rightarrow \mathbb{C}$$

*is a crossed homomorphism with respect to  $\varphi_0$ .*

*Proof.* For any  $g, g' \in F_n$ , we have

$$\begin{aligned} \psi(gg') &= \bar{\psi}(d(gg')) \\ &= \bar{\psi}(dg + gdg') \\ &= \bar{\psi}(dg) + \bar{\psi}(gdg') \\ &= \psi(g) + \varphi_0(g)\psi(g'). \end{aligned}$$

□

**Lemma 2.7.** *The map  $\bar{\psi}$  gives a  $\mathbb{Z}G(K)$ -homomorphism on  $DG(K)$  if and only if  $\bar{\psi}(dr_i) = 0$  for any relator  $r_i$  of  $G(K)$ . This is also equivalent to*

$$\bar{\psi} \left( \sum_{j=1}^n \frac{\partial r_i}{\partial x_j} dx_j \right) = \sum_{j=1}^n \varphi_0 \left( \frac{\partial r_i}{\partial x_j} \right) \psi(x_j) = 0.$$

**Remark 2.8.** Here we use the same symbol  $\varphi_0$  to the extended map  $\mathbb{Z}G(K) \rightarrow \mathbb{Z}\mathbb{C}^* = \mathbb{C}$  on the integral group ring  $\mathbb{Z}G(K)$ .

*Proof.* Recall that any relator of  $DG(K)$  can be given from relators of  $G(K)$ , and

$$dr_i = \sum_{j=1}^n \frac{\partial r_i}{\partial x_j} dx_j$$

in  $DF_n$ . By using them, it is easily seen. □

Now we define an  $(n-1) \times n$ -matrix  $A_{\varphi_0} \in M(n-1, n; \mathbb{C})$  as follows:

$$A_{\varphi_0} = \left( \tilde{\varphi}_0 \left( \frac{\partial r_i}{\partial x_j} \right) \right).$$

It is clear that  $A_{\varphi_0}$  can be obtained from the Alexander matrix of  $G(K)$  by substituting  $t = a$ . From the above argument, the condition for  $\psi$  to be a crossed homomorphism as follows.

**Lemma 2.9.**  *$\psi$  is a crossed homomorphism if and only if  $A_{\varphi_0} \mathbf{b} = \mathbf{0}$ .*

de Rham proved the following [3]. From this theorem, we see that there exists a representation when  $\Delta_K(a) = 0$  and can say the Alexander polynomial is an obstruction for the existence of representations. See also [1, 6].

**Theorem 2.10** (de Rham). *The map*

$$\varphi : \{x_1, \dots, x_n\} \ni x_i \mapsto \begin{pmatrix} a & \psi(x_i) \\ 0 & 1 \end{pmatrix} \in GL(2; \mathbb{C})$$

*can be extend to  $G(K)$  as a homomorphism if and only if  $A_{\varphi_0} \mathbf{b} = \mathbf{0}$ . In particular then it holds  $a = \varphi_0(x_i) = \bar{\varphi}_0(t)$  is a zero of  $\Delta_K(t) = 0$ .*

*Proof.* First we note that a map  $\varphi$  can be extend to the  $G(K)$  as a homomorphism if and only if the image of any relator is the identity matrix  $E$ .

For example, we take a relator  $r_i = x_i x_j x_i^{-1} x_k^{-1}$ . Then the condition is

$$\begin{aligned}\varphi(r_i) &= \varphi(x_i)\varphi(x_j)\varphi(x_i)^{-1}\varphi(x_k)^{-1} \\ &= E.\end{aligned}$$

This is equivalent to  $\varphi(x_i)\varphi(x_j) = \varphi(x_k)\varphi(x_i)$ . Then we compute the both sides.

$$\begin{aligned}\varphi(x_i)\varphi(x_j) &= \begin{pmatrix} a & b_i \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b_j \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a^2 & ab_j + b_i \\ 0 & 1 \end{pmatrix} \\ \varphi(x_k)\varphi(x_i) &= \begin{pmatrix} a & b_k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b_i \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a^2 & ab_i + b_k \\ 0 & 1 \end{pmatrix}.\end{aligned}$$

By comparing entries of the both, we have

$$(1 - a)b_i + ab_j - b_k = 0.$$

By Fox's free differential calculus

$$\begin{aligned}\alpha_* \left( \frac{\partial}{\partial x_i} (x_i x_j - x_k x_i) \right) &= 1 - t, \\ \alpha_* \left( \frac{\partial}{\partial x_j} (x_i x_j - x_k x_i) \right) &= t, \\ \alpha_* \left( \frac{\partial}{\partial x_k} (x_i x_j - x_k x_i) \right) &= -1.\end{aligned}$$

we see the above condition  $(1 - a)b_i + ab_j - b_k = 0$  is the same with the  $i$ -th entry of  $A|_{t=a}\mathbf{b}$  equals zero. Therefore the condition to be extended is given by the following linear system

$$A|_{t=a}\mathbf{b} = \mathbf{0}.$$

Hence it is seen that  $t = a$  is a zero of  $\Delta_K(t) = 0$  and then

$$\varphi : \{x_1, \dots, x_n\} \ni \mapsto \begin{pmatrix} a & b_i \\ 0 & 1 \end{pmatrix}$$

can be extended to  $G(K)$  as a homomorphism. □

Note that the condition for the extension is given by linear equations. Then if  $\varphi$  can be done to  $G(K)$  as a homomorphism

$$\varphi_s(x_i) = \begin{pmatrix} a & sb_i \\ 0 & 1 \end{pmatrix}$$

can also be done to  $G(K)$  for any  $s \in \mathbb{C}^*$ . Then  $\varphi_s$  is a deformation of the direct sum of  $\varphi_0$  and the 1-dimensional trivial representation in  $GL(2; \mathbb{C})$ .

Now we consider deformations in  $SL(2; \mathbb{C})$ .

The map

$$\varphi : \{x_1, \dots, x_n\} \rightarrow SL(2; \mathbb{C})$$

is given by  $\varphi(x_i) = \begin{pmatrix} a & b_i \\ 0 & a^{-1} \end{pmatrix}$  and

$$\varphi_0 : \{x_1, \dots, x_n\} \rightarrow \mathbb{C}^*$$

by  $\varphi_0(x_1) = \dots = \varphi_0(x_n) = a$ .

Starting from this map  $\varphi$ , the condition for  $\varphi$  to be a homomorphism on  $G(K)$  can be obtained as follows.

$$\begin{aligned}\varphi(x_i)\varphi(x_j) &= \begin{pmatrix} a & b_i \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} a & b_j \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} a^2 & ab_j + a^{-1}b_i \\ 0 & a^{-1} \end{pmatrix}, \\ \varphi(x_k)\varphi(x_i) &= \begin{pmatrix} a & b_k \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} a & b_i \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} a^2 & ab_i + a^{-1}b_k \\ 0 & a^{-1} \end{pmatrix}.\end{aligned}$$

By comparing of entries,

$$(1 - a^2)b_i + a^2b_j - b_k = 0$$

is obtained as a condition. By similar arguments, we obtain the following condition

$$A|_{t=a^2}\mathbf{b} = \mathbf{0}.$$

In particular we have

$$\Delta_K(a^2) = 0,$$

that is,  $t = a^2$  is a zero of  $\Delta_K(t) = 0$ . Then

$$\varphi_0 \oplus \varphi_0^{-1} : G(K) \ni x \mapsto \begin{pmatrix} \varphi_0(x) & 0 \\ 0 & \varphi_0(x)^{-1} \end{pmatrix} \in SL(2; \mathbb{C})$$

can be deformed in  $SL(2; \mathbb{C})$  to  $\varphi : G(K) \rightarrow SL(2; \mathbb{C})$ .

### 3. CONSTRUCTION OF A HOMOMORPHISM OF $G(K)$ INTO SYMMETRIC GROUPS

We can construct a deformation of an abelian representation in  $GL(2, \mathbb{C})$ , or  $SL(2, \mathbb{C})$ . From the above observation, we can get also a homomorphism of  $G(K)$  into symmetric groups. This argument was given in [4].

We recall  $\Delta_K(t)$  is well defined up to  $\pm t^k$ . Namely it depends on a Wirtinger presentation of  $G(K)$ . When we change a presentation, the new one equals to the  $\pm t^k$  times old one. It means special value of  $\Delta_K(t)$  is not well-defined as a knot invariant in general. However if we substitute an absolute value one complex number  $\xi = e^{\sqrt{-1}\theta}$  to  $t$ , then its absolute value  $|\Delta_K(\xi)|$  gives a knot invariant.

**Remark 3.1.** The integer  $d_K = |\Delta_K(-1)| \in \mathbb{Z}$  is called the determinant of  $K$ .

Because the Alexander matrix  $A$  of a Wirtinger presentation of  $G(K)$  is a matrix over  $\mathbb{Z}[t, t^{-1}]$ , then by substituting  $t = -1$ , we have a matrix over the integers

$$A|_{t=-1} \in M((n-1) \times n; \mathbb{Z}).$$

Then a linear equation system for the extension is defined over  $\mathbb{Z}$ . When we consider

$$A|_{t=-1}\mathbf{b} = \mathbf{0}$$

over  $\mathbb{Z}/d_K$ , any  $(n-1) \times (n-1)$ -minor  $A|_{t=-1}$  is zero mod  $d_K$ . Hence there exists the solution

$$\mathbf{b} = {}^t(b_1, \dots, b_n) \in (\mathbb{Z}/d_K)^n.$$

At that time a representation

$$\bar{\varphi} : G(K) \rightarrow GL(2; \mathbb{Z}/d_K)$$

over  $\mathbb{Z}/d_K$  can be given by

$$\bar{\varphi}(x_i) = \begin{pmatrix} -1 & b_i \\ 0 & 1 \end{pmatrix}.$$

Here an affine transformation

$$\bar{\varphi}(x_i) = \begin{pmatrix} -1 & b_i \\ 0 & 1 \end{pmatrix}$$

can be consider a permutation

$$\mathbb{Z}/d_K \ni m \mapsto -m + b_i \in \mathbb{Z}/d_K$$

on  $\mathbb{Z}/d_K$ . Therefore we obtain a homomorphism into a symmetric group,

$$G(K) \rightarrow \mathfrak{S}_{d_K}.$$

Next we consider to substitute any positive integer to  $t$ . If we put  $t = m \in \mathbb{Z}$  and consider the linear sytem mod  $d_{K,m} = |\Delta_K(m)|$ , then

$$A|_{t=m} \mathbf{b} \equiv 0 \pmod{d_{K,m}}$$

has a solution over  $\mathbb{Z}/d_{K,m}$ . Of course  $d_{K,m}$  depends on the choice of a Wirtinger presentation. However we can obtain a representation defined by using a fixed presentation.

Then we obtain a representation

$$\bar{\varphi} : G(K) \rightarrow GL(2; \mathbb{Z}/d_{K,m}).$$

For any generator, its image is given by

$$G(K) \ni x_i \mapsto \begin{pmatrix} m & b_i \\ 0 & 1 \end{pmatrix}$$

and it gives

$$\mathbb{Z}/d_{K,m} \ni k \mapsto mk + b_i \in \mathbb{Z}/d_{K,m}.$$

Therefore we obtain a homomorphism of  $G(K)$  into the symmetric group of degree  $d_{K,m}$

$$G(K) \rightarrow \mathfrak{S}_{d_{K,m}}.$$

**Problem 3.2.** *What kind of property does the above homomorphism  $G(K) \rightarrow \mathfrak{S}_{d_{K,m}}$  have?*

#### 4. $SL(2, \mathbb{Z}/d)$ -REPRESENTATION OF $G(K)$

In this section, we give a proof of Theorem 1.2.

We assume that the Alexander polynomial of  $K$  is given by

$$\Delta_K(t) = a_{2k}t^{2k} + a_{2k-1}t^{2k-1} + \cdots + a_1t + a_0,$$

where  $a_{2k} = a_0 > 0$ ,  $\sum_{i=0}^{2k} a_i = \pm 1$ , and it can be defined by the Wirtinger presentation

$$\langle x_1, \dots, x_n \mid r_1, \dots, r_n \rangle.$$

If we substitute  $t = p^2$  for  $\Delta_K(t)$ , then

$$d_{p^2} = \Delta_K(p^2) = a_{2k}p^{4k} + a_{2k-1}p^{4k-2} + \cdots + a_1p^2 + a_0.$$

If  $p$  is a sufficient large prime number,

$$d_{p^2} = \Delta_K(p^2) > p^2 > p.$$

Further we put the condition  $(a_0, p) = 1$ , then

$$(d_{p^2}, p) = 1.$$

Then for any prime number  $p$  as above,  $p$  is a unit in  $\mathbb{Z}/d_{p^2}$ .

Since there exists a solution

$$A|_{t=p^2} \mathbf{b} = 0 \pmod{\mathbb{Z}/d_{p^2}},$$

then an abelian representation

$$\rho : G(K) \ni x_i \mapsto \begin{pmatrix} p & 0 \\ 0 & p^{-1} \end{pmatrix} \in SL(2, \mathbb{Z}/d_{p^2})$$

can be deformed to a non commutative representation

$$\tilde{\rho} : G(K) \ni x_i \mapsto \begin{pmatrix} p & b_i \\ 0 & p^{-1} \end{pmatrix} \in SL(2, \mathbb{Z}/d_{p^2}).$$

Therefore we obtain the following.

**Theorem 4.1.** *There exists a non commutative representation  $G(K) \rightarrow SL(2, \mathbb{Z}/d_{p^2})$  for infinitely many  $d_{p^2} = |\Delta_K(p^2)|$ .*

**Remark 4.2.** It is not easy to see which  $d_{p^2}$  is a prime number or not.

## 5. $GL(2, \mathbb{Z}/p)$ -REPRESENTATION OF $G(K)$

If  $d_p$  is not a prime number, then we cannot consider the twisted Alexander polynomial [7] for the representation as above. Then we want to consider the following problem.

**Problem 5.1.** *Does there exist a non commutative representation  $G(K) \rightarrow SL(2, \mathbb{Z}/p)$  for infinitely many prime number  $p$ ?*

In this section we prove the existence of  $GL(2, \mathbb{Z}/p)$ -representations by using the Alexander polynomial.

For any knot with the Alexander polynomial of degree 2, we can prove the problem for  $GL(2, \mathbb{Z}/p)$ -representations. We assume that the Alexander polynomial of  $K$  is given by

$$\Delta_K(t) = at^2 - bt + a,$$

where  $b \geq a > 0$ ,  $\Delta_K(1) = 2a - b = \pm 1$ . Then by the condition  $2a - b = \pm 1$ ,  $a = \frac{b \pm 1}{2}$ .

**Theorem 5.2.** *There exists a non commutative representation  $G(K) \rightarrow GL(2, \mathbb{Z}/p)$  for infinitely many prime number  $p$ .*

If we can prove the following proposition, for such a prime number  $p$  and  $t = n$ , an abelian representation of  $G(K)$  over  $\mathbb{Z}/p$

$$\rho : G(K) \ni x_i \mapsto \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} \in GL(2, \mathbb{Z}/p)$$

can be deformed to a non commutative representation

$$\tilde{\rho} : G(K) \ni x_i \mapsto \begin{pmatrix} n & b_i \\ 0 & 1 \end{pmatrix} \in GL(2, \mathbb{Z}/p),$$

and we get the theorem.

**Proposition 5.3.** *There exists a solution of  $\Delta_K(t) \equiv 0 \pmod{p}$  for infinitely many prime numbers  $p$ .*

Let us consider the congruence

$$at^2 - bt + a \equiv 0 \pmod{p}.$$

When we consider the equation

$$at^2 - bt + a = 0$$

over  $\mathbb{C}$ , then

$$t = \frac{b \pm \sqrt{b^2 - 4a^2}}{2a}$$

is the solutions. Here if  $D = b^2 - 4a$  is a square number mod  $p$ , that is, a quadratic residue mod  $p$ , then there exists a solution of the above congruence.

**Definition 5.4.** For an integer  $k$  and a prime number  $p$ , the Legendre symbol  $\left(\frac{k}{p}\right)$  is defined as follows.

$$\left(\frac{k}{p}\right) = \begin{cases} 1 & \text{if } x^2 \equiv k \pmod{p} \text{ has a solution} \\ -1 & \text{if } x^2 \equiv k \pmod{p} \text{ has no solution} \end{cases}$$

By using  $2a - b = \pm 1$ , we can eliminate  $a$  in  $D = b^2 - 4a^2$  and obtain  $D = \pm 2b - 1$ . Then we put  $D_+ = 2b - 1$  and  $D_- = -2b - 1$  for the both. By using Legendre symbol, we prove the following.

**Proposition 5.5.** For infinitely many prime numbers  $p$ , each of Legendre symbols of  $D_{\pm}$  is

$$\left(\frac{D_{\pm}}{p}\right) = 1.$$

We treat separately  $D_+$  and  $D_-$ .

**1. The case of  $D_+ = 2b - 1$ .**

Here we assume that

$$p = 4(2b - 1)n + 1$$

is a prime number and not a divisor of  $a$ .

**Remark 5.6.** By the theorem of Dirichlet, there exist infinitely many prime number as above.

If  $p$  is a divisor of  $2b - 1$ , then  $D_+ \equiv 0 \pmod{p}$ . Hence there exists a solution of  $\Delta_K(t) \equiv 0 \pmod{p}$ .

Assume that  $p$  is not a divisor of  $2b - 1$ . By the reciprocity law of the Jacobi symbol,

$$\begin{aligned} \left(\frac{2b-1}{p}\right) \left(\frac{p}{2b-1}\right) &= (-1)^{\frac{p-1}{2} \frac{2b-1-1}{2}} \\ &= (-1)^{2(2b-1)n(b-1)} \\ &= 1. \end{aligned}$$

Therefore we have

$$\begin{aligned}
 \left(\frac{2b-1}{p}\right) &= \left(\frac{p}{2b-1}\right) \\
 &= \left(\frac{4(2b-1)n+1}{2b-1}\right) \\
 &= \left(\frac{1}{2b-1}\right) \\
 &= 1.
 \end{aligned}$$

## 2. The case of $D_- = -2b-1$

Now assume that

$$p = 4(2b+1)n+1$$

is a prime number and not a divisor of  $a$ .

Now

$$\left(\frac{-2b-1}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{2b+1}{p}\right).$$

By the quadratic reciprocity law,

$$\begin{aligned}
 \left(\frac{-1}{p}\right) &= (-1)^{\frac{p-1}{2}} \\
 &= (-1)^{2(2b+1)n} \\
 &= 1.
 \end{aligned}$$

Hence

$$\left(\frac{-2b-1}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{2b+1}{p}\right) = \left(\frac{2b+1}{p}\right).$$

By using the reciprocity law of the Jacobi symbol,

$$\begin{aligned}
 \left(\frac{2b+1}{p}\right) \left(\frac{p}{2b+1}\right) &= (-1)^{\frac{p-1}{2} \frac{2b+1-1}{2}} \\
 &= (-1)^{2(2b+1)nb} \\
 &= 1.
 \end{aligned}$$

Therefore we have

$$\begin{aligned}
 \left(\frac{2b+1}{p}\right) &= \left(\frac{p}{2b+1}\right) \\
 &= \left(\frac{4(2b+1)n+1}{2b+1}\right) \\
 &= \left(\frac{1}{2b+1}\right) \\
 &= 1.
 \end{aligned}$$

## REFERENCES

- [1] G. Burde, *Darstellungen von Knotengruppen*, Math. Ann. **173** (1967), 24–33.
- [2] R. H. Crowell and R. H. Fox, *Introduction to knot theory*, GTM 7, Springer.
- [3] G. de Rham, *Introduction aux polynômes d'un nœud*, Enseign. Math. (2) **13** (1968), 187–194.
- [4] R. H. Fox, *A quick trip through knot theory*, in the book, Topology of 3-manifolds and related topics, (1962), 120–167.
- [5] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, second edition, GTM 84, Springer.
- [6] D. Silver and S. Williams, *On a theorem of Burde and de Rham*, J. Knot Theory Ramifications **20** (2011), 713–720.
- [7] M. Wada, *Twisted Alexander polynomial for finitely presentable groups*, Topology **33** (1994), 241–256.

DEPARTMENT OF INFORMATION SYSTEMS SCIENCE, FACULTY OF ENGINEERING, SOKA UNIVERSITY,  
TANGI-CHO 1-236, HACHIOJI, TOKYO 192-8577, JAPAN

*E-mail address:* kitano@soka.ac.jp