March 5, 2012 in Hiroshima

Linear representations over a finite field of a knot group and the Alexander polynomial as an obstruction

KITANO Teruaki (Soka Univ.)

Table of Contents:

1 Example

- K: a knot in S^3.
- $G(K) = \pi_1(S^3 - K)$: its knot group.

In the knot theory

- to find a representation of a knot group into/onto a finite group

is a fundamental tool related with branched coverings.

Here we consider $K = 3_1$, the trefoil knot.
We take and fix the following presentation:

$$G(3_1) = \langle x, y \mid xyx = yxy \rangle$$

Define a map

$$\varphi : \{x, y\} \to GL(2, \mathbb{Z}/3)$$

by

$$\varphi(x) = \varphi(y) = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}.$$

Clearly it gives an abelian representation of $G(3_1)$ for any $a = 1, 2$.
Next define a map by

$$\varphi(x) = \begin{pmatrix} a & 1 \\ 0 & 1 \end{pmatrix}, \varphi(y) = \begin{pmatrix} a & 2 \\ 0 & 1 \end{pmatrix}.$$

Then does it give a representation

$$\hat{\varphi} : G(3_1) \to GL(2, \mathbb{Z}/3)?$$

By easy computation of matrices, we can see

- it does so for $a = 1$,
- but not so for $a = 2$.

If we define a map over $\mathbb{Z}/5$ by

$$\varphi(x) = \begin{pmatrix} a & 1 \\ 0 & 1 \end{pmatrix}, \varphi(y) = \begin{pmatrix} a & 2 \\ 0 & 1 \end{pmatrix},$$

it never gives a representation from $G(3_1)$ to $GL(2, \mathbb{Z}/5)$ for any $a = 1, 2, 3, 4$.

How we can see and explain what happens?

- It can be explained by the de Rham's result.
- Roughly speaking, when a is a zero of the Alexander polynomial, above map gives a representation.

2 Introduction

we give some definition and fix some notations in this talk:

- K: a knot in S^3.
- $G(K) = \pi_1(S^3 - K)$: its knot group.
- $H_1(G(K); \mathbb{Z}) \cong \mathbb{Z} \cong \langle t \rangle$.
- $\alpha : G(K) \to \langle t \rangle$: the abelianization of $G(K)$.
- $\alpha_* : \mathbb{Z}G(K) \to \mathbb{Z}\langle\ t\ \rangle = \mathbb{Z}[t, t^{-1}]$: induced map on the integral group ring.

- $A \in M((n-1) \times n; \mathbb{Z}[t, t^{-1}])$: Alexander matrix of $G(K)$ defined by the presentation.
- $A(a) = A|_{t=a} \in M((n-1) \times n; \mathbb{Z}[a, a^{-1}])$: the matrix obtained by substituting $t = a$ to A.
- $\mathfrak{S}_d$:the symmetric group of degree d.

In this talk we suppose

- any presentation of $G(K)$ is a Wirtinger presentation:

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

defined by a regular diagram of K:

– its deficiency=1.

– any r_i is a form of $x_i x_j x_i^{-1} x_k^{-1}$ or $x_i^{-1} x_j x_i x_k^{-1}$.

Recall Fox's free differentials:

$$\frac{\partial}{\partial x_1}, \ldots, \frac{\partial}{\partial x_n} : \mathbb{Z}F_n \to \mathbb{Z}F_n.$$

Here

- $F_n = \langle x_1, \ldots, x_n \rangle$: the free group generated by $x_1, \ldots, x_n$.
- $\mathbb{Z}F_n$:its group ring.

Free differentials can be characterized by the following.

1. A linear map over $\mathbb{Z}$.
2. For any i, j,
$$\frac{\partial}{\partial x_j}(x_i) = \delta_{ij}.$$
3. For any $g, g' \in F_n$,
$$\frac{\partial}{\partial x_j}(gg') = \frac{\partial}{\partial x_j}(g) + g\frac{\partial}{\partial x_j}(g').$$

Since any relator is an element of F_n, we can apply Fox's free differentials to the relator. Then Alexander matrix is defined by

$$A = \left(\alpha_* \left(\frac{\partial}{\partial x_j} (r_i) \right) \right)_{ij}.$$

Remark 2.1. *By the definition* $\frac{\partial}{\partial x_j}(r_i) \in \mathbb{Z}F_n$*. Here it can be projected in* $\mathbb{Z}G(K)$ *and it maps in* $\mathbb{Z}[t, t^{-1}]$ *by* α_**.*

Definition 2.2. *The Alexander polynomial of* K

$$\Delta_K(t) \in \mathbb{Z}[t, t^{-1}]$$

is defined to be a $(n-1)$*-minor.*

Remark 2.3. $\Delta_K(t)$ *is well defined up to* $\pm t^l$*.* *Here after changing a presentation if we need, we can assume that some* $(n-1)$*-minor, that is, its Alexander polynomial is a polynomial, not a Laurent polynomial.*

As we mentioned before, the set of

- linear representations,
- conjugacy classes of representations

are important subject to study in the low dimensional topology.

- Representation spaces,
- Character varieties,
- some kinds of topological invariants,
- $\cdots$.

Here we consider representations over a finite prime field $\mathbb{Z}/p$.

- The set of all $SL(2, \mathbb{Z}/p)$-representations is an algebraic set over a finite field $\mathbb{Z}/p$.
- It is hard to check whether the set of representations is empty or not, because to solve an equation over a finite field is so.

Suzuki-Kitano (JKTR, 2012) computed the followings for the Reidemeister-Rolfsen's list;

- the number of the conjugacy classes of $SL(2,\mathbb{Z}/p)$-representations,
- the number of the conjugacy classes of non abelian $SL(2,\mathbb{Z}/p)$-representations,
- the number of the conjugacy classes of surjective $SL(2,\mathbb{Z}/p)$-representations,

where p is a prime number with $p \leq 23$.

表1: Number of non abelian representations

K	2	3	5	7	11	13	17	19	23
3_1	1	4	10	14	18	30	44	38	42
4_1	0	4	8	20	16	28	28	32	36
6_2	0	0	0	4	4	26	36	36	34
6_3	0	0	4	8	32	12	24	40	40
7_1	0	0	0	12	0	78	0	0	0
7_5	0	0	0	8	8	8	28	28	40
8_{12}	0	0	0	0	12	4	12	24	28
8_{18}	4	20	48	84	112	308	300	248	340
9_9	0	0	0	12	6	32	32	32	32
9_{48}	4	0	20	64	60	132	194	138	200
10_{98}	4	20	84	200	340	692	870	870	1352
10_{99}	4	20	128	320	736	1368	1832	2176	2984
10_{124}	0	0	16	0	88	0	0	152	0

There are lots of zeros. It is hard to see the law on the numbers at first glance.

Then we consider the following problem:

Problem 2.4. *Does there exist a non abelian representation*

$$G(K) \to SL(2, \mathbb{Z}/p)$$

for infinitely many prime numbers p*?*

Along this direction, there are known results:

Theorem 2.5 (Magnus-Pelso, 1967)**.**
$G(KT)$ has a quotient group isomorphic to $PSL(2,\mathbb{Z}/p)$ for infinitely many prime numbers p.

Theorem 2.6 (Riley, 1970')**.** *There exists a parabolic representation of 2-bridge knot group in $PSL(2,\mathbb{Z}/p)$ for infinitely many prime numbers p.*

Remark 2.7. *By easy arguments, projective representations*

$$G(K) \to PSL(2, \mathbb{Z}/p)$$

can be lifted to

$$G(K) \to SL(2, \mathbb{Z}/p).$$

In this talk, we study the existence of a linear representation from the Alexander polynomial.

Theorem 2.8. *If* $\Delta_K(t) \neq 1$*, then there exists a non abelian representation* $G(K) \to SL(2, \mathbb{Z}/d)$ *for infinitely many* $d \in \mathbb{Z}_+$*.*

Remark 2.9. *We do not know whether there exists infinitely many prime numbers in the set of* d*'s.*

If $\Delta_K(t)$ has a special form, we can prove the following.

Theorem 2.10. *If the degree of $\Delta_K(t)$ is 2, then there exist a non abelian representation $G(K) \to GL(2, \mathbb{Z}/p)$ for infinitely many prime numbers $p \in \mathbb{Z}_+$.*

More generally, we can obtain the following as a corollary.

Corollary 2.11. *If $\Delta_K(t) = f(t)g(t)$ with the degree of $f(t)$ is two and $f(1) = 1$, then there exists a non abelian representation $G(K) \to GL(2, \mathbb{Z}/p)$ for infinitely many prime numbers $p \in \mathbb{Z}_+$.*

The main tool to study is a classical theory by de Rham:
G. De Rham, Introduction aux polynomes d’un nœud, L’Enseignement Mathématique, Vol.13 (1967).

Remark 2.12. *This work is one origin of twisted Alexander polynomials of a knot.*

3 Theorem of de Rham

Recall the theorem by de Rham.

We fix a Wirtinger presentation of K as

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

Now we take a map

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

where $a \neq 0 \in \mathbb{C}$ and $b_1, \ldots, b_n \in \mathbb{C}$.

When φ can be extended to $G(K)$ as a homomorphism?

Remark 3.1. *If* $b_1 = \cdots = b_n = b \in \mathbb{C}$, *then it can be done as an abelian representation:*

$$\varphi : G(K) \ni x_i \mapsto \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in GL(2;\mathbb{C}).$$

Hence we assume that

$$\mathbf{b} = {}^t(b_1\ b_2\ \ldots b_n) \neq c\,{}^t(1\ 1\ \ldots 1).$$

Under the fixing presentation, we have the Alexander matrix

$$A \in M((n-1) \times n; \mathbb{Z}[t, t^{-1}]),$$

and by putting $t = a$,

$$A(a) \in M((n-1) \times n; \mathbb{C}).$$

Theorem 3.2 (de Rham). *The map*

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

can be extended to $G(K)$ as a *homomorphism* *if and only if $A(a)\mathbf{b} = \mathbf{0}$.*
In particular then it holds $t = a$ is a zero of $\Delta_K(t) = 0$.

Outline of Proof:
As a homomorphism, φ can be done to $G(K)$ if and only if any relator maps to E.
For example, we take one relator

$$r_i = x_i x_j x_i^{-1} x_k^{-1}.$$

Then the condition $\varphi(r_i) = E$ is equivalent to

$$\varphi(x_i)\varphi(x_j) = \varphi(x_k)\varphi(x_i).$$

Then we compute the both sides:

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

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

By comparing entries of the both, we have

$$ab_j + b_i = ab_i + b_k,$$

and then

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

Remark 3.3. *Here we note* $b_1, b_2, \ldots, b_n$ *are the variables.*

This condition can be also given by Fox's free differential calculus as follows.

$$\alpha_*\left(\frac{\partial}{\partial x_i}(x_i x_j - x_k x_i)\right) = 1 - t$$

$$\alpha_*\left(\frac{\partial}{\partial x_j}(x_i x_j - x_k x_i)\right) = t$$

$$\alpha_*\left(\frac{\partial}{\partial x_k}(x_i x_j - x_k x_i)\right) = -1.$$

Then the above condition is the same with the i-th entry of the vector $A(a)\mathbf{b}$ equals zero.

Therefore the conditon for φ to be extended is given by the linear system

$$A(a)\mathbf{b} = \mathbf{0}.$$

By the linear algebra, there exists $\mathbf{b} \neq \mathbf{0}$ if and only if any $(n-1)$-minors of $A(a)$ is zero. Hence, when $t = a$ is a zero of $\Delta_K(t) = 0$,

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

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

Remark 3.4. *Because the condition $A(a)\mathbf{b} = \mathbf{0}$ is a linear condition, if we find some a and $\mathbf{b}$, then for any $s \in \mathbb{C} - \{0\}$,*

$$\varphi_s : \{x_1, \ldots, x_n\} \ni \begin{pmatrix} a & sb_i \\ 0 & 1 \end{pmatrix} \mapsto \in GL(2, \mathbb{C})$$

gives a representation.

Here we consider a map into $SL(2;\mathbb{C})$.
Take a map

$$\hat{\varphi} : \{x_1, \ldots, x_n\} \to SL(2;\mathbb{C})$$

is given by $\hat{\varphi}(x_i) = \begin{pmatrix} a & b_i \\ 0 & a^{-1} \end{pmatrix}$.
By the similar computation, the condition to be extended for $\hat{\varphi}$ is given by

$$A(a^2)\mathbf{b} = 0.$$

In particular at that time, $t = a^2$ is a zero of $\Delta_K(t) = 0$.

4 Construction of a homomorphism of $G(K)$ into symmetric groups

From the above observation, we can get also a homomorphism of $G(K)$ into symmetric groups. Originally this argument was given in the famous paper by

- R. H. Fox, A quick trip through knot theory, Topology of 3-Manifolds edited by Fort.

We recall that $\Delta_K(t)$ is well defined up to $\pm t^k$ and a special value of $\Delta_K(t)$ is not well-defined as a knot invariant.
However we consider $|\Delta_K(m)|$ as a number, not invariant, under fixing Wiritinger presentation for any integer $m \in \mathbb{Z}$.

Remark 4.1. *We choice $\Delta_K(t)$ to be a polynomial as a minor of A by changing a presentation of $G(K)$.*

First example is the knot determinant

$$d_K = |\Delta_K(-1)| \in \mathbb{Z}.$$

Remark 4.2. *It is known that* $|\Delta_K(-1)| \neq 0$ *and it is a knot invariant.*

By substituting $t = -1$, we get

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

Then for the linear system $A(-1)\mathbf{b} \equiv \mathbf{0}$, clearly it has no nontrival solution, because

$$|\Delta_K(-1)| = d_K \neq 0.$$

However if we consider and treat

$$A(-1)\mathbf{b} \equiv \mathbf{0}$$

over $\mathbb{Z}/d_K$, clearly any $(n-1)$-minor of $A(-1)$ is zero mod d_K.

Hence there exists the solution

$$\mathbf{b} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \in (\mathbb{Z}/d_K)^n \, .$$

Then we can get a representation

$$\bar{\varphi} : G(K) \ni x_i \mapsto \begin{pmatrix} -1 & b_i \\ 0 & 1 \end{pmatrix} \in GL(2; \mathbb{Z}/d_K).$$

Here an affine transformation $\bar{\varphi}(x_i) = \begin{pmatrix} -1 & b_i \\ 0 & 1 \end{pmatrix}$ can be consider a permutation on $\mathbb{Z}/d_K$:

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

Therefore we obtain a homomorphism;

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

From here we consider $t = m \in \mathbb{Z}$ and

$$d_{K,m} = |\Delta_K(m)|.$$

Here if $d_{K,m}$ is not a prime number. we put the assumption:

$$(m, d_{K,m}) = 1.$$

In this case,

- m is a unit in $\mathbb{Z}/d_{K,m}$.
- the linear sytem: $A(m)\mathbf{b} \equiv \mathbf{0} \bmod d_{K,m}$ has a solution over $\mathbb{Z}/d_{K,m}$.

By finding a solution a and $\mathbf{b}$, we obtain a representation

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

For any generator x_i, its image $\bar{\varphi}(x_i) = \begin{pmatrix} m & b_i \\ 0 & 1 \end{pmatrix}$ gives a permutaion:

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

Therefore we obtain a homomorphism of $G(K)$;

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

5 Example:trefoil knot again

Here we consider $K = 3_1$, the trefoil knot. We take and fix the following presentation:

$$G(K) = \langle x, y \mid xyx = yxy \rangle$$

By applying the Fox's free derivatives $\dfrac{\partial}{\partial x}, \dfrac{\partial}{\partial y}$, we get

- $A = \begin{pmatrix} t^2 - t + 1 & -t^2 + t - 1 \end{pmatrix}$,
- $\Delta_{3_1}(t) = t^2 - t + 1$.

Example 5.1. *First we consider the case of* $t = -1$*.*

$$d_{3_1} = |\Delta_K(-1)| = 3.$$

Then we find a solution

$$A(3)\begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \equiv \mathbf{0} \ mod\, 3.$$

In this case, the Alexander matrix mod 3 :

$$A(3) \equiv \begin{pmatrix} 0 & 0 \end{pmatrix} \ mod\, 3.$$

Then

- *any* $n \in \mathbb{Z}/3$ *is zero of* $\Delta_{3_1}(t) \equiv 0$ *mod* 3,
- *any* $\mathbf{b} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \in (\mathbb{Z}/3)^2$ *is a solution.*

For examples, taking $n = 2$ *and* $b_1 = 1, b_2 = 2$, *a represenation*

$$\varphi : G(3_1) \to GL(2, \mathbb{Z}/3)$$

can be defined by

$$\varphi(x) = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}, \varphi(y) = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}.$$

Furthermore, if we define a map
$\hat{\varphi} : \{x, y\} \to SL(2, \mathbb{Z}/3)$ *by*

$$\hat{\varphi}(x) = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}, \hat{\varphi}(y) = \begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix},$$

it gives a representation

$$\hat{\varphi} : G(3_1) \to SL(2, \mathbb{Z}/3).$$

We put $m = 2$ and then obtain $d_2 = |\Delta(2)| = 3$. Then we have the same as above.

Example 5.2. *If we put $m = 3$, then $d_3 = |\Delta_{3_1}(3)| = 7$. In this case any n and any $\mathbf{b}$ satisfies also the linear equation, because*

$$A(3) = \begin{pmatrix} 0 & 0 \end{pmatrix} \textit{ mod } 7.$$

Hence we obtain a representation

$$\varphi : G(3_1) \to GL(2, \mathbb{Z}/7)$$

and

$$\hat{\varphi} : G(3_1) \to SL(2, \mathbb{Z}/7).$$

For examples,

$$\hat{\varphi}(x) = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}, \hat{\varphi}(y) = \begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix}$$

gives a representation

$$\hat{\varphi} : G(K) \to SL(2, \mathbb{Z}/7).$$

Finally we can see

Proposition 5.3. *There exit a non abelian representation of $G(3_1)$ in $SL(2,\mathbb{Z}/d)$ for infinitely many integers d.*

6 $SL(2, \mathbb{Z}/d)$-represenation of $G(K)$

In this section, we consider the following problem.

Problem 6.1. *Does there exit a non abelian representation* $G(K) \to SL(2, \mathbb{Z}/d)$ *for infinitely many integers* d *?*

For simplicity we suppose

- The Alexander polynomial is given to be

$$\Delta_K(t) = a_{2k}t^{2k} + a_{2k-1}t^{2k-1} + \cdots + a_1 t + a_0,$$

where $a_{2k} = a_0 > 0, \sum_{i=0}^{2k} a_i = \pm 1.$

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

$$d_p = \Delta_K(p^2) = a_{2k}p^{4k} + a_{2k-1}p^{4k-2} + \cdots + a_1 p^2 + a_0.$$

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

$$\Delta_K(p^2) \equiv a_0 \mod p.$$

Hence

$$(\Delta_K(p^2), p) = 1.$$

Then for any prime number p as above, p and p^2 are units in $\mathbb{Z}/d_p^2$.

Because there exists a solution

$$A(p^2)\mathbf{b} \equiv \mathbf{0} \text{ mod } d_{p^2},$$

then a non abelian representation

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

is obtained.

Therefore we obtain the following.

Theorem 6.2. *There exits a non abelian representation* $G(K) \to SL(2, \mathbb{Z}/d_{p^2})$ *for infinitely many* $d_{p^2} = |\Delta_K(p^2)|$.

Remark 6.3. *We do not know whether* d_{p^2} *is a prime number or not.*

7 $GL(2,\mathbb{Z}/p)$-representation of $G(K)$

Here we consider $GL(2,\mathbb{Z}/p)$-representations as follows.

Problem 7.1. *Does there exit a non abelian representation* $G(K) \to GL(2,\mathbb{Z}/p)$ *for infinitely many prime numbers* p *?*

For any knot K with the Alexander polynomial of degree 2, we can give the answer as follows. Now 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 $2a - b = \pm 1$,

$$a = \frac{b \pm 1}{2}.$$

Now we can prove the following.

Proposition 7.2. *There exists a solution of the congruence* $\Delta_K(t) \equiv 0$ *mod* p *for infinitely many prime number* p.

If $\Delta_K(n) \equiv 0$ mod p, then we can find a non trivial solution $\mathbf{b}$ of $A(n)\mathbf{b} \equiv \mathbf{0}$ mod p. Then

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

gives a non abelian representation.

Theorem 7.3. *There exit a non abelian representation* $G(K) \to GL(2, \mathbb{Z}/p)$ *for infinitely many prime number* p.

Let us consider the congruence

$$at^2 - bt + a \equiv 0 \bmod p.$$

When we consider the equation

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

over $\mathbb{C}$, then the solutions are

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

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

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

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 can state the following.

Proposition 7.5. *For infinitely many prime numbers p*, *Legendre symbols of $D = D_+, D_+$ mod p is*

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

1. The case of $D_+ = 2b - 1$.
Here we assume that

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

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

Remark 7.6. *By the theorem of Dirichlet, there exisit infinitely many prime number as above.*

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

Assume that p is not a divisor of $2b-1$.

By the reciprocity law of the Jacobi symbol,

$$\left(\frac{2b-1}{p}\right)\left(\frac{p}{2b-1}\right) = (-1)^{\frac{p-1}{2}\,\frac{2b-1-1}{2}}$$

$$= (-1)^{2(2b-1)n(b-1)}$$

$$= 1.$$

Therefore

$$\left(\frac{2b-1}{p}\right) = \left(\frac{p}{2b-1}\right)$$
$$= \left(\frac{4(2b-1)n+1}{2b-1}\right)$$
$$= \left(\frac{1}{2b-1}\right)$$
$$= 1$$

2. The case of $D_{-} = -2b - 1$

Now assume that

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

is a prime number and is 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,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

$$= (-1)^{2(2b+1)n}$$

$$= 1.$$

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,

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

$$= (-1)^{2(2b+1)nb}$$

$$= 1.$$

Therefore we have

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

If $\Delta_K(t)$ is product of a degree 2 polynomial and another one, then by similar arguments, we obtain the following main result.

Theorem 7.7. *If $\Delta_K(t) = f(t)g(t)$ with the degree of $f(t)$ is two and $f(1) = 1$, then there exists a non abelian representation $G(K) \to GL(2, \mathbb{Z}/p)$ for infinitely many prime numbers $p \in \mathbb{Z}_+$.*