J. Math. Sci. Univ. Tokyo
9 (2002), 405–423.

Construction of Unramified Galois Extensions Over Maximal Abelian Extensions of Algebraic Number Fields

By Sachiko Ohtani

Abstract. We construct unramified Galois extensions over maximal abelian extensions of algebraic number fields by using division points of abelian varieties which have everywhere semistable reduction. Further, by using division points of elliptic curves, we construct infinitely many linearly independent unramified Galois extensions of $\mathbb{Q}(\zeta_{p^\infty})^{\mathrm{ab}}$ having $SL_2(\mathbb{Z}_p)$ as the Galois group over $\mathbb{Q}(\zeta_{p^\infty})^{\mathrm{ab}}$.

0. Introduction

Our purpose in this paper is to construct unramified Galois extensions over maximal abelian extensions of algebraic number fields by using division points of abelian varieties.

Let A be an abelian variety over an algebraic number field K and $p \geq 5$ a prime number. Assume that the pair (A, p) satisfies the following conditions:

(A0) A has everywhere semistable reduction over $\mathcal{O}_K$, where $\mathcal{O}_K$ is the ring of integers of K.

(A1) A has bad reduction at all extensions of p to K.

Note that, if A is an arbitrary abelian variety over an algebraic number field K, then we can find a finite extension L of K such that $A \otimes_K L$ satisfies the condition (A0) by the *semistable reduction theorem* (*cf.* Grothendieck [8], Theorem 3.6).

For a place v of K, we denote by $\mathcal{A}_v^0$ the identity component of the special fibre of the Néron model of A at v. For an algebraic number field k, we denote by k^{ab} the maximal abelian extension of k.

Our main result is the following

2000 *Mathematics Subject Classification.* Primary 11R32; Secondary 11G10, 11G05.

THEOREM 0.1. *Let A be an abelian variety over an algebraic number field K and $p \geq 5$ a prime number. Assume that the pair (A, p) satisfies the conditions* (A0) *and* (A1). *Let F be the field obtained by adjoining to K the coordinates of all p-power division points on A.*
(a) If $\mathcal{A}_v^0$ is a split torus for every place v of K such that A has bad reduction at v, then $FK(\zeta_{p^\infty})^{\mathrm{ab}}$ is an unramified Galois extension of $K(\zeta_{p^\infty})^{\mathrm{ab}}$, where $K(\zeta_{p^\infty})$ is the field obtained by adjoining to K all p-power roots of unity.
(b) If $\mathcal{A}_v^0$ is a split torus for every place v of K lying above p, then $F(K\mathbb{Q}^{\mathrm{ab}})^{\mathrm{ab}}$ is an unramified Galois extension of $(K\mathbb{Q}^{\mathrm{ab}})^{\mathrm{ab}}$.

Further, by using division points of elliptic curves (*i.e.*, abelian varieties of dimension one), we obtain the following

THEOREM 0.2. *Let $p \geq 5$ be a prime number. Then there exist infinitely many linearly independent unramified Galois extensions of $\mathbb{Q}(\zeta_{p^\infty})^{\mathrm{ab}}$ having $SL_2(\mathbb{Z}_p)$ as the Galois group over $\mathbb{Q}(\zeta_{p^\infty})^{\mathrm{ab}}$.*

Here, for a sequence of extensions $K_1, K_2, \cdots$ of an algebraic number field k, if $K_{n+1} \cap K_1K_2 \cdots K_n = k$ for any $n \geq 1$, then we say that the extensions are *linearly independent* over k.

Now we explain the background of these results. Unramified abelian extensions over maximal abelian extensions of algebraic number fields have been investigated by many people, *e.g.*, Cornell [4], Brumer [3] and Kurihara [10]. Uchida [21] and Horie [9] determined the structure of the Galois group of the maximal unramified solvable extension over maximal abelian extensions of algebraic number fields. For unramified non-solvable extensions, Asada [1], [2] gave some results. First, Asada [1] considered elliptic curves over $\mathbb{Q}$ whose modular invariants are integral and which have good reduction at a supersingular prime p, and then constructed unramified Galois extensions over maximal abelian extensions of algebraic number fields by using their p-power division points. Second, Asada [2] constructed an infinite family of elliptic curves over $\mathbb{Q}$ which have multiplicative reduction at a prime p and of which the orders at p of the modular invariants are divisible by p, and then constructed unramified Galois extensions over $\mathbb{Q}^{\mathrm{ab}}$ having $PSL_2(\mathbb{Z}/p^r\mathbb{Z})$ as the Galois group over $\mathbb{Q}^{\mathrm{ab}}$ by using their p^r-division

points. Further this paper contains an example of unramified Galois extensions having $SL_2(\mathbb{Z}_p)$ as the Galois group using results of [1]. Asada's family in [2] is chosen so carefully that it appears very special. Also his elliptic curves in [1] have everywhere potential good reduction. So we would like to find more general phenomena. In this paper, we shall give a general construction, at the expense of enlarging the base field, using abelian varieties which have everywhere semistable reduction.

Next we give an outline of this paper. In Section 1, we shall prove Theorem 0.1. By a lemma due to Y. Ihara, for a finite Galois extension K/k, the extension $Kk^{\mathrm{ab}}/k^{\mathrm{ab}}$ is unramified if and only if the local Galois extension Kk_v/k_v is abelian for every place v of k. Then we shall apply Mumford's construction (*cf.* Faltings-Chai [6]) and a result by Grothendieck (*cf.* [8]) on p-adic representations associated to semistable abelian varieties, which imply that the local Galois extension is abelian. In Section 2, we shall give examples of abelian varieties and algebraic number fields which satisfy the conditions of Theorem 0.1. In Section 3, by using division points of elliptic curves over $\mathbb{Q}$ which satisfy the conditions of Theorem 0.1 and some additional assumptions, we shall construct infinitely many unramified Galois extensions of $\mathbb{Q}(\zeta_{p^\infty})^{\mathrm{ab}}$ having $SL_2(\mathbb{Z}_p)$ as the Galois group over $\mathbb{Q}(\zeta_{p^\infty})^{\mathrm{ab}}$. To determine the Galois group, we use a criterion by Serre (*cf.* [15]) on the surjectivity of p-adic representations associated to non-CM elliptic curves. To prove the infinite existence of linearly independent unramified extensions, we use an infinite family of elliptic curves of the form $y^2 = x(x-p)(x+p_i)$, where p_i's ≥ 5 are distinct prime numbers different from p. Thus we can prove Theorem 0.2. In Section 4, we shall consider elliptic curves of prime conductor p of Setzer [19], and construct unramified Galois extensions over finite extensions over $\mathbb{Q}$ having $SL_2(\mathbb{Z}/p^r\mathbb{Z})$ as the Galois group.

The author would like to express her sincere gratitude to Professor Yuichiro Taguchi who suggested her to consider this problem and gave her many valuable suggestions. The author also thanks Professor Iku Nakamura for enjoyable discussions on degeneration of abelian varieties, and Professor Kenneth A. Ribet for his suggesting an improvement of the exposition of the proof of Theorem 0.1, which made her original proof more elegant. She also thanks the referee for his/her many kind and careful comments.

In this paper we use the following notation:

$\mathbb{Q}$: the field of rational numbers.

$\mathbb{Z}$: the ring of rational integers.

For a rational prime number p,

$\mathbb{Q}_p$: the field of p-adic numbers,

$\mathbb{Z}_p$: the ring of p-adic integers,

$\mathbb{F}_p$: the prime field of p elements.

For an algebraic number field K,

K^{ab} : the maximal abelian extension of K,

K_v : the completion of K at a place v of K,

$\mathcal{O}_K$: the ring of integers of K,

G_K : the absolute Galois group over K.

For a positive integer m,

ζ_m : a primitive m-th root of unity,

$A[m]$: the group of the m-division points of an abelian variety A.

1. Division Points of Abelian Varieties

First we introduce a lemma due to Y. Ihara, which is a key in our construction of unramified Galois extensions over maximal abelian extensions of algebraic number fields.

LEMMA 1.1 (*cf.* Asada [1], Proposition 1). *Let k be an algebraic number field, k^{ab} the maximal abelian extension of k, and K a finite Galois extension of k. Then Kk^{ab} is unramified over k^{ab} if and only if the decomposition group in K over k is commutative for any prime divisor of K.*

Next we shall give a proof of Theorem 0.1 by using an application of *Mumford's construction* of degenerating abelian varieties (*cf.* Faltings-Chai [6]). Let A be an abelian variety of dimension g over an algebraic number field K and $p \geq 5$ a prime number. Assume that the pair (A, p) satisfies the following conditions:

(A0) A has everywhere semistable reduction over $\mathcal{O}_K$.

(A1) A has bad reduction at all extensions of p to K.

Let r be a positive integer and F_r the field obtained by adjoining to K the coordinates of the p^r-division points on A. Theorem 0.1 (a) follows from the following

THEOREM 1.2. *Assume that $\mathcal{A}_v^0$ is a split torus for every place v of K such that A has bad reduction at v. Then $F_rK(\zeta_{p^r})^{\mathrm{ab}}$ is an unramified Galois extension of $K(\zeta_{p^r})^{\mathrm{ab}}$.*

PROOF. By Lemma 1.1, it suffices to prove that F_rK_v is an abelian extension of $K_v(\zeta_{p^r})$ for every place v of K. If v is unramified in F_r, then there is nothing to prove. Hence we only have to prove it for the places which are ramified in F_r. By the *criterion of Néron-Ogg-Shafarevich* (*cf.* Serre-Tate [18], Theorem 1), such places are the bad places of A. (Recall that we assumed that A has bad reduction at all extensions of p to K.) Let v be a place of K such that A has bad reduction at v. We have the following representation:

$$\rho_r : G_{K_v} \longrightarrow \mathrm{Aut}\,(A[p^r]) \simeq GL_{2g}(\mathbb{Z}/p^r\mathbb{Z}).$$

If we put $H = \mathrm{Gal}\,(\bar{K}_v/K_v(\zeta_{p^r}))$, then it suffices to prove that $\rho_r(\sigma)\rho_r(\tau) = \rho_r(\tau)\rho_r(\sigma)$ for any σ and τ in H.

Let G be the identity component of the Néron model of A at v. By the condition (A0), G is a semi-abelian scheme over $\mathrm{Spec}\,(\mathcal{O}_{K_v})$ whose generic fibre G_η is abelian. Then we have the exact sequence

$$0 \longrightarrow T \longrightarrow \tilde{G} \longrightarrow B \longrightarrow 0$$

called the *Raynaud extension associated to* G (*cf.* Faltings-Chai [6], Ch.II, 1), where T is a torus, $\tilde{G}$ is a semi-abelian scheme over $\mathrm{Spec}\,(\mathcal{O}_{K_v})$ and B is an abelian variety. Similarly, we can construct a semi-abelian scheme G^t from the dual abelian variety of the generic fibre G_η. Then we denote the Raynaud extension associated to G^t by

$$0 \longrightarrow T^t \longrightarrow \tilde{G}^t \longrightarrow B^t \longrightarrow 0.$$

Let $\underline{X} = \mathrm{Hom}\,(T, \mathbb{G}_m)$ and $\underline{Y} = \mathrm{Hom}\,(T^t, \mathbb{G}_m)$. We regard $\underline{X}$ and $\underline{Y}$ as étale sheaf over $\mathrm{Spec}\,(\mathcal{O}_{K_v})$. Now we assume that the special fibre $\mathcal{A}_v^0$ of G

is a split torus. Hence T is split and isomorphic to $\tilde{G}$, and $\underline{X}$ and $\underline{Y}$ are constant, with values X and Y. Here X and Y are free $\mathbb{Z}$-modules of rank g. Further we obtain the following exact sequence as G_{K_v}-modules:

$$0 \longrightarrow \mathrm{Hom}\,(X, \boldsymbol{\mu}_{p^r}) \xrightarrow{\phi} A[p^r] \xrightarrow{\psi} Y/p^rY \longrightarrow 0,$$

where $\boldsymbol{\mu}_{p^r}$ is the group of the p^r-th roots of unity (*cf.* Faltings-Chai [6], Ch.III, 7.3, or see also Ribet [13], Lemma (3.3.1)).

X and Y are trivial G_{K_v}-modules, and $\mathrm{Hom}\,(X, \boldsymbol{\mu}_{p^r})$ is a trivial H-module. Hence $\rho_r(\sigma) - 1 = 0$ on $\mathrm{Im}(\phi)$ for any σ in H. While $\rho_r(\sigma) - 1$ maps $A[p^r]$ into $\mathrm{Ker}\,(\psi)$ for any σ in H because Y/p^rY is a trivial H-module. Hence $(\rho_r(\sigma) - 1)(\rho_r(\tau) - 1) = 0$ for any σ and τ in H. Therefore $\rho_r(\sigma)\rho_r(\tau) = \rho_r(\tau) + \rho_r(\sigma) - 1 = \rho_r(\tau)\rho_r(\sigma)$ for any σ and τ in H. This completes the proof of Theorem 1.2. □

REMARK 1.3. We also see that the field F_rK_v is a Kummer extension over $K_v(\zeta_{p^r})$ for every place v such that A has bad reduction at v.

Theorem 0.1 (b) follows from the following

THEOREM 1.4. *If $\mathcal{A}_v^0$ is a split torus for every place v of K lying above p, then $F_r(K\mathbb{Q}^{\mathrm{ab}})^{\mathrm{ab}}$ is an unramified Galois extension of $(K\mathbb{Q}^{\mathrm{ab}})^{\mathrm{ab}}$.*

PROOF. By Lemma 1.1 again and Theorem 1.2, it suffices to prove that $F_rK_v\mathbb{Q}^{\mathrm{ab}}$ is an abelian extension of $K_v\mathbb{Q}^{\mathrm{ab}}$ for the places v of K prime to p such that A has bad reduction at v.

Let v be a place of K prime to p such that A has bad reduction at v and $T_p(A)$ the p-adic Tate module associated to A. We have the following representation:

$$\rho : G_{K_v} \longrightarrow \mathrm{Aut}\,(T_p(A)) \simeq GL_{2g}(\mathbb{Z}_p).$$

Since A has semistable reduction at v, we see that the image of the inertia subgroup of G_{K_v} by ρ is isomorphic to $\mathbb{Z}_p(1) = \varprojlim_r \boldsymbol{\mu}_{p^r}$ by Grothendieck [8], Proposition 3.5, Corollary 3.5.2. Hence $F_rK_v^{\mathrm{ur}}$ is abelian over K_v^{ur}, where K_v^{ur} is the maximal unramified extension of K_v. Since K_v^{ur} is cyclotomic over K_v, we see that $F_rK_v\mathbb{Q}^{\mathrm{ab}}$ is an abelian extension of $K_v\mathbb{Q}^{\mathrm{ab}}$. □

2. Examples

In this section, we shall give examples of abelian varieties and algebraic number fields which satisfy the conditions of Theorem 0.1.

2.1. The case of dim $A = 1$

Let E be an elliptic curve over an algebraic number field k with modular invariant $j = j(E)$ and $p \geq 5$ a prime number. Assume that $v(j) < 0$ for any place v of k lying above p. Then the pair (E, p) satisfies the condition (A1) of Theorem 0.1. Further there exists a finite Galois extension K of k such that the elliptic curve $E \otimes_k K$ over K satisfies the condition (A0) of Theorem 0.1 by the semistable reduction theorem (*cf.* [8], Theorem 3.6), and the assumption of Theorem 0.1 (a) by *Tate's theory* (*cf.* Lang [11], Ch.15).

If k is equal to $\mathbb{Q}$, then we can find a field K explicitly such that $FK(\zeta_{p^\infty})^{\mathrm{ab}}$ is unramified over $K(\zeta_{p^\infty})^{\mathrm{ab}}$. In particular, we can take a solvable extension of $\mathbb{Q}$ as such a field K. Further if E satisfies a certain assumption, then we can also determine the Galois group of $FK(\zeta_{p^\infty})^{\mathrm{ab}}$ over $K(\zeta_{p^\infty})^{\mathrm{ab}}$ which is an unramified Galois extension of Theorem 0.1.

PROPOSITION 2.1. *(a) Let E be an elliptic curve over $\mathbb{Q}$ and $p \geq 5$ a prime number. Assume that the modular invariant $j(E)$ is non-integral. Let r be a positive integer and F_r the field obtained by adjoining to $\mathbb{Q}$ the coordinates of the p^r-division points on E. Then there exists a finite solvable extension K over $\mathbb{Q}$ depending only on E such that $F_rK(\zeta_{p^r})^{\mathrm{ab}}$ is an unramified Galois extension of $K(\zeta_{p^r})^{\mathrm{ab}}$.*
(b) Let F_1 be the field obtained by adjoining to $\mathbb{Q}$ the coordinates of the p-division points on E. If $\mathrm{Gal}\,(F_1/\mathbb{Q})$ is isomorphic to $GL_2(\mathbb{F}_p)$, then

$$\mathrm{Gal}\,(F_rK(\zeta_{p^r})^{\mathrm{ab}}/K(\zeta_{p^r})^{\mathrm{ab}}) \simeq SL_2(\mathbb{Z}/p^r\mathbb{Z}).$$

Note that it is well-known that $\mathrm{Gal}\,(F_1/\mathbb{Q}) \simeq GL_2(\mathbb{F}_p)$ for almost all prime numbers p in this case by Serre [16], Théorème 2.

PROOF. (*a*) Let E be an elliptic curve over $\mathbb{Q}$. We may assume that E has the *Legendre form* (*cf.* Silverman [20], Ch.III, §1) over a finite solvable extension L of $\mathbb{Q}$ given by the following equation:

$$(*) \qquad y^2 = x(x-1)(x-\lambda), \qquad \lambda \neq 0, 1.$$

Indeed, we may assume that E is defined over $\mathbb{Q}$ by the equation

$$E \ : \ y^2 = (x-e_1)(x-e_2)(x-e_3), \qquad e_1, e_2, e_3 \in \bar{\mathbb{Q}},$$

by [20], Ch.III, §1. Further, by the proof of Proposition 1.7 (a) in [20], Ch.III, we see that E has the Legendre form (*) with $\lambda = (e_3-e_1)/(e_2-e_1)$ over the Galois closure L of $\mathbb{Q}(\sqrt{e_2-e_1}, e_1)$. Note that L is solvable over $\mathbb{Q}$.

We put $S = \{v : \text{place of } L \,|\, v(\lambda) < 0\}$. If S is empty, then E has everywhere semistable reduction over $\mathcal{O}_L$ by Remark 1.1 and Proposition 5.1 in [20], Ch.VII. In this case we can take L as the field K of the statement of (a). Next assume that S is non-empty. Let H be the Hilbert class field of L and $\mathfrak{p}_v$ a prime divisor of L corresponding to $v \in S$. Since the extensions of all prime divisors of L to H are principal, there exists an element π_v in $\mathcal{O}_H$ such that $\mathfrak{p}_v\mathcal{O}_H = (\pi_v)$. Then there exist positive integers r_v such that $v'(\lambda \prod_{v\in S} \pi_v^{r_v}) = 0$ for any place v' of H lying above a place in S. We put $\pi = \prod_{v\in S} \pi_v^{r_v}$ and $u = \lambda\pi$. In a way similar to Case 3 in [20], p.182, we may assume that E is isomorphic over $H(\sqrt{\pi})$ to an elliptic curve E' having the following form:

$$E' \ : \ (y')^2 = x'(x'-u)(x'-\pi).$$

Let w be an extension of v' to $H(\sqrt{\pi})$. Then we see that the equation of E' is minimal and E' has multiplicative reduction over $H(\sqrt{\pi})_w$ by Remark 1.1 and Proposition 5.1 in [20], Ch.VII. Since E is isomorphic to E' over $H(\sqrt{\pi})$, E also has multiplicative reduction over $H(\sqrt{\pi})_w$. In this case we can take $H(\sqrt{\pi})$ as the field K of the statement of (a). Note that $H(\sqrt{\pi})$ is also solvable over $\mathbb{Q}$. Thus we see that there exists a solvable extension K of $\mathbb{Q}$ such that $E \otimes_{\mathbb{Q}} K$ has everywhere semistable reduction over $\mathcal{O}_K$.

Next we prove that $F_rK(\zeta_{p^r})^{\mathrm{ab}}$ is an unramified Galois extension of $K(\zeta_{p^r})^{\mathrm{ab}}$. Let v be a place of K at which $E \otimes_K K_v$ has bad reduction. By Tate's theory (*cf.* Lang [11], Ch.15), over the unramified quadratic extension K_v' of K_v, we see that $E \otimes_K K_v$ is isomorphic to a Tate curve $E(q)$ over K_v with modular invariant $j(E)$. Let $F(q)_r$ be the field obtained by adjoining to K_v the coordinates of the p^r-division points on $E(q)$. Then $F(q)_r$ is equal to $K_v(\zeta_{p^r}, q^{1/p^r})$, where q is the element of $K_v^\times$ which corresponds to $j(E)$ by Tate's theory again. Hence $F(q)_rK_v$ is a Kummer extension over $K_v(\zeta_{p^r})$, in particular, it is abelian. Then F_rK_v' is also an abelian extension of $K_v(\zeta_{p^r})$. Hence we see that F_rK_v is also abelian over $K_v(\zeta_{p^r})$.

(b) By the assumption, we have

$$\mathrm{Gal}\,(F_1/\mathbb{Q}(\zeta_p)) \cong SL_2(\mathbb{F}_p).$$

Since $SL_2(\mathbb{F}_p)$ has no non-trivial abelian quotient, we see that

$$K(\zeta_{p^r})^{\mathrm{ab}} \cap F_1 = \mathbb{Q}(\zeta_p).$$

Hence we see

$$\mathrm{Gal}\,(F_1K(\zeta_{p^r})^{\mathrm{ab}}/K(\zeta_{p^r})^{\mathrm{ab}}) \cong SL_2(\mathbb{F}_p).$$

The proposition follows from the following

LEMMA 2.2 (Serre [15], Ch.IV, 3.4, Lemma 3). *Let X be a closed subgroup of $SL_2(\mathbb{Z}_p)$ whose image in $SL_2(\mathbb{F}_p)$ is $SL_2(\mathbb{F}_p)$. If $p \geq 5$, then $X = SL_2(\mathbb{Z}_p)$.* □

By Proposition 2.1, we obtain the following

COROLLARY 2.3. (a) *Let E and p be as above, and F the field obtained by adjoining to $\mathbb{Q}$ the coordinates of all p-power division points on E. Then there exists a finite solvable extension K over $\mathbb{Q}$ depending only on E such that $FK(\zeta_{p^\infty})^{\mathrm{ab}}$ is an unramified Galois extension of $K(\zeta_{p^\infty})^{\mathrm{ab}}$.*
(b) *Let F_1 be the field obtained by adjoining to $\mathbb{Q}$ the coordinates of the p-division points on E. If $\mathrm{Gal}\,(F_1/\mathbb{Q})$ is isomorphic to $GL_2(\mathbb{F}_p)$, then*

$$\mathrm{Gal}\,(FK(\zeta_{p^\infty})^{\mathrm{ab}}/K(\zeta_{p^\infty})^{\mathrm{ab}}) \simeq SL_2(\mathbb{Z}_p).$$

2.2. The jacobian variety of the modular curve of level p

For any integer m and a subgroup H of $GL_2(\mathbb{Z}/m\mathbb{Z})$, we have an algebraic stack proper over $\mathrm{Spec}\,\mathbb{Z}$, which may be interpreted over $\mathrm{Spec}\,\mathbb{Z}[1/m]$ as the fine moduli stack classifying *generalized* elliptic curves with level H-structure (*cf.* Deligne-Rapoport [5], IV, (3.1)). Its associated *coarse* moduli stack (*cf.* [5], I, (8.1)) may be denoted by M_H. If $H = \Gamma_0(N) = \left\{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \mid c \equiv 0 \pmod{N}\right\}$, then we write $M_H = M_0(N)$.

LEMMA 2.4 (Mazur [12], Appendix, Theorem (A.1)). *Let $p \geq 5$ be a prime number, J the jacobian variety of dimension g of the modular curve*

$M_0(p)$ and $\mathcal{J}$ the Néron model of J at p. The identity component $\mathcal{J}_p^0$ of the fibre at $\mathbb{F}_p$ of $\mathcal{J}$ is a group scheme of multiplicative type, in other words, if we consider it over $\bar{\mathbb{F}}_p$, then $\mathcal{J}_p^0 \otimes_{\mathbb{F}_p} \bar{\mathbb{F}}_p \simeq \mathbb{G}_m^g$.

Note that J has good reduction outside p. By this lemma, we see that there exists a finite extension k over $\mathbb{F}_p$ such that $\mathcal{J}_p^0 \otimes_{\mathbb{F}_p} k \simeq \mathbb{G}_m^g$. Hence there exists a finite Galois extension K over $\mathbb{Q}$ such that the abelian variety J over K satisfies the condition (A0), (A1) and the assumption of Theorem 0.1 (a).

Now we describe k and K explicitly. We put $X(\mathcal{J}_p^0) = \mathrm{Hom}_{\mathbb{F}_p}(\mathcal{J}_p^0, \mathbb{G}_m)$. We see that $X(\mathcal{J}_p^0) = \mathrm{Hom}\,(\mathbb{G}_m^g, \mathbb{G}_m) \simeq \mathbb{Z}^g$ since we have $\mathcal{J}_p^0 \otimes_{\mathbb{F}_p} \bar{\mathbb{F}}_p \simeq \mathbb{G}_m^g$ by Lemma 2.4. We have the following representation defined by a continuous action of $G_{\mathbb{F}_p}$ on $X(\mathcal{J}_p^0)$:

$$\rho \ : \ G_{\mathbb{F}_p} \longrightarrow \mathrm{Aut}\,(X(\mathcal{J}_p^0)) \simeq GL_{2g}(\mathbb{Z}).$$

By Ribet [14], Proposition 3.7 and 3.8 (ii), we see that $G_{\mathbb{F}_p}$ acts on $X(\mathcal{J}_p^0)$ as an automorphism of order 1 or 2. Hence we can take as the field k a quadratic field of $\mathbb{F}_p$ and as the field K a quadratic extension of $\mathbb{Q}$ in which p is inert.

Thus we obtain the following

PROPOSITION 2.5. *Let J and p be as above, and F the field obtained by adjoining to $\mathbb{Q}$ the coordinates of all p-power division points on J. If K is a quadratic extension over $\mathbb{Q}$ in which p is inert, then $FK(\zeta_{p^\infty})^{\mathrm{ab}}$ is an unramified Galois extension of $K(\zeta_{p^\infty})^{\mathrm{ab}}$.*

3. Division Points of Elliptic Curves

In this section, we shall prove Theorem 0.2. Throughout this section, let k be the field obtained by adjoining to $\mathbb{Q}$ all p-power roots of unity and k_r the field obtained by adjoining to $\mathbb{Q}$ the p^r-th roots of unity.

3.1. Unramifiedness over $\mathbb{Q}(\zeta_{p^\infty})^{\mathrm{ab}}$

In this subsection, by using division points of elliptic curves over $\mathbb{Q}$, we construct unramified Galois extensions over k^{ab}.

Let E be an elliptic curve over $\mathbb{Q}$ and $p \geq 5$ a prime number. Assume that the pair (E, p) satisfies the following conditions:

(E0) E has everywhere semistable reduction over $\mathbb{Z}$.

(E1) E has bad reduction at p.

PROPOSITION 3.1. *Let E and p be as above. Let r be a positive integer and F_r the field obtained by adjoining to $\mathbb{Q}$ the coordinates of the p^r-division points on E. Then $F_r k_r^{\mathrm{ab}}$ is an unramified Galois extension of k_r^{ab}.*

PROOF. We can prove this proposition in a way similar to the proof of Proposition 2.1. In this case, we can take $\mathbb{Q}$ itself as the field K in Proposition 2.1. □

By Proposition 3.1, we obtain the following

COROLLARY 3.2. *Let E, p and k be as above. Let F be the field obtained by adjoining to $\mathbb{Q}$ the coordinates of all p-power division points on E. Then Fk^{ab} is an unramified Galois extension of k^{ab}.*

3.2. Determination of the Galois group

Let E be an elliptic curve over $\mathbb{Q}$ and $p \geq 5$ a prime number. Assume that the pair (E, p) satisfies the conditions (E0) and (E1) of 3.1 and the following conditions:

(E2) E has three $\mathbb{Q}$-rational points of order 2.

(E3) p does not divide the valuation at p of the modular invariant $j(E)$ of E.

In this subsection, for such E and p, we shall prove that the unramified extension Fk^{ab} over k^{ab} which we constructed in Corollary 3.2 has $SL_2(\mathbb{Z}_p)$ as the Galois group over k^{ab}. By Corollary 2.3 (b), it suffices to prove the following

PROPOSITION 3.3. *Let E and p be as above, and F_1 the field obtained by adjoining to $\mathbb{Q}$ the coordinates of the p-division points on E. Then*

$$\mathrm{Gal}\,(F_1/\mathbb{Q}) \cong GL_2(\mathbb{F}_p).$$

PROOF. In general, let E be an arbitrary elliptic curve defined over $\mathbb{Q}$. Let $l \geq 5$ be a prime number, and $E[l]$ the group of the l-division points of E. Then we have the following representation:

$$\bar{\rho} \ : \ G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}\,(E[l]) \cong GL_2(\mathbb{F}_l).$$

Now we denote $G_l = \mathrm{Im}\,\bar{\rho}$. To prove this proposition, we verify the conditions of the following lemma (*cf.* Serre [15], Ch.IV, 3.2, Lemma 2).

LEMMA 3.4. *If G_l satisfies the next three conditions $(a), (b)$ and (c), then G_l is equal to $GL_2(\mathbb{Z}/l\mathbb{Z})$.*
(a) $\det G_l = \mathbb{F}_l^{\times}$.
(b) G_l contains the element $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ *with respect to a suitable basis of $E[l]$.*
(c) $E[l]$ is irreducible as a $G_{\mathbb{Q}}$-module.

Apply this to our E and $l = p$. The condition (a) is satisfied for $l = p$ since F_1 contains ζ_p. The condition (b) is also satisfied for $l = p$ by the condition (E3) and Lemma 1 of Serre [15], Ch.IV, 3.2. Hence we prove that the condition (c) is satisfied for $l = p$.

Assume that this is not the case, *i.e.*, $E[p]$ is reducible as a $G_{\mathbb{Q}}$-module. Then E contains a subgroup X whose order is p and which is stable under the action of $G_{\mathbb{Q}}$. The action of $G_{\mathbb{Q}}$ on X and $E[p]/X$ gives two characters $\chi', \chi'' \ : \ G_{\mathbb{Q}} \longrightarrow \mathbb{F}_p^{\times}$. Since E has everywhere semistable reduction and multiplicative reduction at p, by Serre [16], p.307, we have $\chi' = 1$, $\chi'' = \chi$ or $\chi' = \chi$, $\chi'' = 1$, where $\chi : G_{\mathbb{Q}} \longrightarrow \mathbb{F}_p^{\times}$ is the cyclotomic character.

In the first case, E has a $\mathbb{Q}$-rational point of order p. Since E has three $\mathbb{Q}$-rational points of order 2, we have

$$|\, E(\mathbb{Q})_{\mathrm{tors}} \,| \geq 4p \geq 20.$$

Here $E(\mathbb{Q})_{\mathrm{tors}}$ is the torsion subgroup of the group $E(\mathbb{Q})$ of $\mathbb{Q}$-rational points of E. But it is impossible by *Mazur's Theorem* (*cf.* Mazur [12], Theorem 8).

In the second case, the quotient curve $E' = E/X$ has a $\mathbb{Q}$-rational point of order p. Further the curve E' also has three $\mathbb{Q}$-rational point of order 2 because $p \neq 2$. Hence we can apply the argument in the first case to E'. This completes the proof of Proposition 3.3. $\square$

3.3. Infinite existence

In this subsection, we shall give a proof of Theorem 0.2. Let p, $p_i \geq 5$ $(i = 1, 2, \cdots)$ be distinct prime numbers and $E^{(i)}$ the elliptic curve over $\mathbb{Q}$ defined by the following equation:

$$E^{(i)} : y^2 = x(x-p)(x+p_i).$$

By Serre [17], 4.1, the elliptic curve $E^{(i)}$ has everywhere semistable reduction over $\mathbb{Z}$, and multiplicative reduction at p, p_i and the prime divisors of $p+p_i$. Let $j(E^{(i)})$ be the modular invariant of $E^{(i)}$. Then, by simple calculations, we see that

$$j(E^{(i)}) = 2^8 \frac{(p^2 + pp_i + p_i^2)^3}{p^2 p_i^2 (p+p_i)^2}.$$

Hence $E^{(i)}$ satisfies the condition (E3). Thus we obtain an infinite family of elliptic curves over $\mathbb{Q}$ which satisfies the conditions (E0), (E1), (E2) and (E3). Let $F^{(i)}$ be the field obtained by adjoining to $\mathbb{Q}$ the coordinates of all p-power division points on $E^{(i)}$. Then, by Proposition 3.1 and 3.3, we see that the extensions $F^{(i)}k^{\mathrm{ab}}$ over k^{ab} are unramified Galois extensions having $SL_2(\mathbb{Z}_p)$ as the Galois group over k^{ab} for any $i \geq 1$.

Let $F_1^{(i)}$ be the field obtained by adjoining to $\mathbb{Q}$ the coordinates of the p-division points on $E^{(i)}$.

LEMMA 3.5. *Let p, $p_1 \geq 5$ be distinct prime numbers and $E^{(1)}$ as above. If we take a prime number p_2 such that $E^{(2)}$ has good reduction at p_1, then*

$$F_1^{(1)} \cap F_1^{(2)} = \mathbb{Q}(\zeta_p).$$

Note that $E^{(2)}$ has good reduction at p_1 if and only if $p_2 \not\equiv -p \pmod{p_1}$. By *Dirichlet's theorem*, there exist infinitely many prime numbers satisfying this condition.

PROOF. Since $E^{(2)}$ has good reduction at p_1, we see that p_1 is unramified in $F_1^{(2)}$. Next we consider the ramification of p_1 in $F_1^{(1)}$. The curve $E^{(1)} \otimes_{\mathbb{Q}} \mathbb{Q}_{p_1}$ is isomorphic to a Tate curve over $\mathbb{Q}_{p_1}$ with modular invariant $j(E^{(1)})$ over the unramified quadratic extension L of $\mathbb{Q}_{p_1}$. Then we have

$$F_1^{(1)} L \simeq L(\zeta_p, q^{1/p}),$$

where q is the element of $L^\times$ which corresponds to $j(E^{(1)})$ by Tate's theory. Since p_1 is unramified in L, if v_{p_1} is an extension of the normalized p_1-adic valuation of $\mathbb{Q}_{p_1}$ to L, then we see that

$$v_{p_1}(q) = -v_{p_1}(j(E^{(1)})) = -\operatorname{ord}_{p_1}(j(E^{(1)})) = 2.$$

Let v'_{p_1} be an extension of v_{p_1} to $L(\zeta_p)$ and w_{p_1} an extension of v'_{p_1} to $F_1^{(1)}L$. Since $L(\zeta_p)$ is unramified over L, if e_{p_1} is the ramification index of w_{p_1} over v'_{p_1}, then

$$w_{p_1}(q^{1/p}) = \frac{1}{p}\, w_{p_1}(q) = \frac{1}{p}\, e_{p_1} v'_{p_1}(q) = \frac{2}{p}\, e_{p_1}.$$

Since $p \geq 5$ and $w_{p_1}(q^{1/p})$ is in $\mathbb{Z}$, we see that $e_{p_1} \gneq 2$. In particular, p_1 is ramified in $F_1^{(1)}$ because L is unramified over $\mathbb{Q}_{p_1}$. Hence we obtain $F_1^{(1)} \neq F_1^{(2)}$. Let $F'^{(i)}_1$ be the subextension of $F_1^{(i)}$ over $\mathbb{Q}(\zeta_p)$ corresponding to the normal subgroup $\{\pm 1\}$ of $SL_2(\mathbb{F}_p)$ $(i = 1, 2)$. Assume that $F'^{(1)}_1 = F'^{(2)}_1$. Then the prime of $F'^{(1)}_1$ lying above p_1 must be ramified in $F_1^{(1)}$ and the ramification index is equal to e_{p_1} because p_1 is unramified in $F'^{(1)}_1$ and ramified in $F_1^{(1)}$. However

$$[F_1^{(1)} : F'^{(1)}_1] = 2 \lneq e_{p_1} \leq [F_1^{(1)} : F'^{(1)}_1].$$

It is impossible. Hence we see that $F'^{(1)}_1 \neq F'^{(2)}_1$. Since

$$\operatorname{Gal}(F'^{(i)}_1/\mathbb{Q}(\zeta_p)) \simeq PSL_2(\mathbb{F}_p),$$

which is a simple group, we have

$$F_1^{(1)} \cap F_1^{(2)} = \mathbb{Q}(\zeta_p). \ \square$$

PROPOSITION 3.6. *Let k and $F^{(i)}$ be as in Lemma 3.5. Then*

$$F^{(1)}k^{\mathrm{ab}} \cap F^{(2)}k^{\mathrm{ab}} = k^{\mathrm{ab}}.$$

PROOF. By Lemma 3.5 and Proposition 3.3, we obtain

$$\begin{aligned}\operatorname{Gal}(F_1^{(1)}F_1^{(2)}/\mathbb{Q}(\zeta_p)) &\simeq \operatorname{Gal}(F_1^{(1)}/\mathbb{Q}(\zeta_p)) \times \operatorname{Gal}(F_1^{(2)}/\mathbb{Q}(\zeta_p)) \\ &\simeq SL_2(\mathbb{F}_p) \times SL_2(\mathbb{F}_p).\end{aligned}$$

Since there is no non-trivial abelian quotient of $SL_2(\mathbb{F}_p) \times SL_2(\mathbb{F}_p)$, we see

$$\mathrm{Gal}\,(F_1^{(1)}F_1^{(2)}k^{\mathrm{ab}}/k^{\mathrm{ab}}) \simeq SL_2(\mathbb{F}_p) \times SL_2(\mathbb{F}_p).$$

By Lemma 2.2, we obtain

$$F^{(1)}k^{\mathrm{ab}} \cap F^{(2)}k^{\mathrm{ab}} = k^{\mathrm{ab}}. \ \square$$

Now we can choose an infinite family of elliptic curves over $\mathbb{Q}$ inductively. Assume that we have taken $p_1, \cdots, p_n$ such that $F^{(1)}k^{\mathrm{ab}}, \cdots, F^{(n)}k^{\mathrm{ab}}$ are linearly independent over k^{ab} having $SL_2(\mathbb{Z}_p)$ as the Galois group over k^{ab}.

Let p_{n+1} be a prime number different from $p_1, \cdots, p_n$ such that $p_{n+1} \not\equiv -p \pmod{p_i}$ and $p_i \not\equiv -p \pmod{p_{n+1}}$ for all $1 \leq i \leq n$. By using Dirichlet's theorem again, we can take such a prime number. Then we see that $E^{(n+1)}$ has good reduction at p_i $(1 \leq i \leq n)$ from the first condition for p_{n+1}. In a way similar to the above argument, we obtain

$$F^{(n+1)}k^{\mathrm{ab}} \cap F^{(i)}k^{\mathrm{ab}} = k^{\mathrm{ab}}.$$

Further we see that $F_1^{(n+1)} \cap F_1^{(1)}F_1^{(2)} \cdots F_1^{(n)} = \mathbb{Q}(\zeta_p)$. Indeed, assume that $M = F_1^{(n+1)} \cap F_1^{(1)}F_1^{(2)} \cdots F_1^{(n)}$ is a non-trivial extension of $\mathbb{Q}(\zeta_p)$. Then the group $\mathrm{Gal}\,(F_1^{(n+1)}/M)$ must be isomorphic to the group $\{\pm 1\}$ or $\{1\}$ because $\mathrm{Gal}\,(F_1^{(n+1)}/\mathbb{Q}(\zeta_p)) \simeq SL_2(\mathbb{F}_p)$. By the same argument as in the proof of Lemma 3.5, the prime of $\mathbb{Q}(\zeta_p)$ lying above p_{n+1} is ramified in M. However p_{n+1} is unramified in $F_1^{(1)}F_1^{(2)} \cdots F_1^{(n)}$ by the latter condition for p_{n+1}. These cases are impossible. Hence we obtain

$$F^{(n+1)}k^{\mathrm{ab}} \cap F^{(1)}F^{(2)} \cdots F^{(n)}k^{\mathrm{ab}} = k^{\mathrm{ab}}.$$

This completes the proof of Theorem 0.2.

Remark 3.7. In Theorem 0.2 we have constructed unramified Galois extensions over algebraic number fields of infinite degree having $SL_2(\mathbb{Z}_p)$ as the Galois group. Then can we construct unramified Galois extensions over *finite* algebraic number fields having $SL_2(\mathbb{Z}_p)$ as the Galois group ? If the *Fontaine-Mazur conjecture* (*cf.* Fontaine-Mazur [7], Conjecture 5a) is true, then we cannot do this. Now we try to construct unramified Galois extensions having $SL_2(\mathbb{Z}/p^r\mathbb{Z})$ as the Galois group over *smaller* algebraic number fields. In the next section, we shall give an example of this problem.

4. Supplement

In this section, we shall construct unramified Galois extensions over a finite extension of $\mathbb{Q}$ having $SL_2(\mathbb{Z}/p^r\mathbb{Z})$ as the Galois group by using a family of elliptic curves of conductor p over $\mathbb{Q}$.

Let p be a prime number such that $p = u^2 + 64$ for some integer u, and E an elliptic curve of conductor p over $\mathbb{Q}$ with a non-trivial $\mathbb{Q}$-rational point of order 2.

By Theorem 2 of Setzer [19], if p is of the form $u^2 + 64$, where u is an integer, and the sign of u is chosen so that $u \equiv 1 \pmod 4$, then there exist, up to isomorphism, just two such curves. The two curves are connected by a 2-isogeny, and one of them is given by the following equation:

$$y^2 = x^3 + ux^2 - 16x.$$

Now we assume that E is given by this equation. The modular invariant $j(E)$ is $p^{-1}(p-16)^3$. Then we see that E has no complex multiplication.

PROPOSITION 4.1. *Let E and p be as above, and F_r the field obtained by adjoining to $\mathbb{Q}$ the coordinates of the p^r-division points on E. Then there exists a finite solvable extension K_r over $\mathbb{Q}$ of degree at most $2\varphi(p^r)p^r$ such that F_rK_r is an unramified Galois extension of K_r having $SL_2(\mathbb{Z}/p^r\mathbb{Z})$ as the Galois group over K_r, where φ is the Euler function.*

PROOF. By the assumption, the extension F_r is unramified outside p over $\mathbb{Q}$. Since E has multiplicative reduction at p, we have $F_rL = L(\zeta_{p^r}, q^{1/p^r})$ in a way similar to the proof of Proposition 2.1 (a), where L is the unramified quadratic extension of $\mathbb{Q}_p$ and q is the element of $L^\times$. Then there exists a finite extension K_r of $\mathbb{Q}$ such that $K_r\mathbb{Q}_p = L(\zeta_{p^r}, q^{1/p^r})$. In particular, $F_rK_r\mathbb{Q}_p$ is unramified over $K_r\mathbb{Q}_p$. Hence F_rK_r is unramified over K_r. Note that, if we take $q_0 \in \mathbb{Q}$ such that q_0 is close to q enough, we may take a quadratic extension of $\mathbb{Q}(\zeta_{p^r}, q_0^{1/p^r})$ as the field K_r of the statement of this proposition.

Next, to prove that $\mathrm{Gal}\,(F_rK_r/K_r)$ is isomorphic to $SL_2(\mathbb{Z}/p^r\mathbb{Z})$, we verify the conditions (a), (b) and (c) of Lemma 3.4. The condition (a) is equivalent to the fact that F_1 contains ζ_p. The condition (b) is also satisfied by the assumption and Lemma 1 of Serre [15], Ch.IV, 3.2. We prove that

the condition (c) is satisfied for p. Assume that $E[p]$ is reducible as a $G_{\mathbb{Q}}$-module. Then there is a one-dimensional subspace X of $E[p]$ which is a cyclic group of order p and stable under the action of $G_{\mathbb{Q}}$. Now we put $E' = E/X$. Then we have an exact sequence

$$0 \longrightarrow X \longrightarrow E \xrightarrow{\lambda} E' \longrightarrow 0,$$

where λ is a separable isogeny of degree p. Since E has no complex multiplication, E' is not isomorphic to E. Further E' has a non-trivial $\mathbb{Q}$-rational point of order 2, and we see that E' has conductor p by Serre-Tate [18], §1, Corollary 2. However we know that there exist just two such curves up to isomorphism. Hence we see that they are E and E'. Since they are connected by a 2-isogeny λ', we have

$$E \xrightarrow{\lambda} E' \xrightarrow{\lambda'} E.$$

Then $\lambda' \circ \lambda$ is an endomorphism of E of degree $2p$. But it is impossible since E has no complex multiplication.

Hence we obtain

$$\mathrm{Gal}\,(F_1/\mathbb{Q}(\zeta_p)) \cong SL_2(\mathbb{F}_p).$$

Since $K_r \cap F_1 = \mathbb{Q}(\zeta_p)$ for any positive integer r, we see that

$$\mathrm{Gal}\,(F_1K_r/K_r) \cong SL_2(\mathbb{F}_p).$$

By Lemma 2.2, we obtain

$$\mathrm{Gal}\,(F_rK_r/K_r) \cong SL_2(\mathbb{Z}/p^r\mathbb{Z}). \square$$

References

[1] Asada, M., *On unramified Galois extensions over maximum abelian extensions of algebraic number fields*, Math. Ann. **270** (1985), 477-487.

[2] Asada, M., *Construction of certain non-solvable unramified Galois extensions over the total cyclotomic field*, J. Fac. Sci. Univ. Tokyo, Sect. IA, Math. **32** (1985), 397–415.

[3] Brumer, A., *The class group of all cyclotomic integers*, J. Pure Appl. Algebra **20** (1981), 107–111.

[4] Cornell, G., *Abhyanker's lemma and the class group*, Lecture Notes in Math. **751**, Springer-Verlag, Berlin, 1979, pp. 82–88.

[5] Deligne, P. and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Lecture Notes in Math. **349**, Springer-Verlag, Berlin, 1973, pp. 143–316.

[6] Faltings, G. and C. L. Chai, *Degeneration of abelian varieties*, Ergeb. Math. Grenzgeb. (3) **22**, Springer-Verlag, Berlin, 1990.

[7] Fontaine, J.-M. and B. Mazur, *Geometric Galois representations*, Elliptic curves, modular forms, and Fermat's last theorem (Hong Kong, 1993), International Press, Cambridge, 1995, pp. 41–78.

[8] Grothendieck, A., *Modèles de Néron et monodromie*, in Groupes de monodromie en géometrie algébrique, SGA7 I, A. Grothendieck, ed., Lecture Notes in Math. **288**, Springer-Verlag, Berlin-NewYork, 1972, pp. 313–523.

[9] Horie, K., *CM-fields with all roots of unity*, Compositio Math. **74** (1990), 1–14.

[10] Kurihara, M., *On the ideal class groups of the maximal real subfields of number fields with all roots of unity*, J. Eur. Math. Soc. **1** (1999), 35–49.

[11] Lang, S., *Elliptic functions* (2nd edition), Graduate Texts in Math. **112**, Springer-Verlag, NewYork, 1987.

[12] Mazur, B., *Modular curves and the Eisenstein ideal*, Publ. Math. I.H.E.S. **47** (1977), 33–186.

[13] Ribet, K.A., *Galois action on division points of Abelian varieties with real multiplications*, Amer. J. Math. **98** (1976), 751–804.

[14] Ribet, K. A., *On modular representations of* $\mathrm{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), 431–476.

[15] Serre, J.-P., *Abelian l-adic representations and elliptic curves*, Benjamin, NewYork, 1968.

[16] Serre, J.-P., *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.

[17] Serre, J.-P., *Sur les représentation modulaires de degré* 2 *de* $\mathrm{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54** (1987), 179–230.

[18] Serre, J.-P. and J. Tate, *Good reduction of abelian varieties*, Ann. Math. **88** (1968), 492–517.

[19] Setzer, B., *Elliptic curves of prime conductor*, J. London Math. Soc. (2) **10** (1975), 367–378.

[20] Silverman, J. H., *The arithmetic of elliptic curves*, Graduate Texts in Math. **106**, Springer-Verlag, NewYork, 1986.

[21] Uchida, K., *Galois groups of unramified solvable extensions*, Tohoku Math. J. (2) **34** (1982), 311–317.

(Received February 16, 2001)

Department of Mathematics
Hokkaido University

Sapporo 060-0810, Japan

Current address:
Graduate School of Mathematics
Kyushu University 33
Fukuoka 812-8581, Japan
E-mail: sohtani@math.kyushu-u.ac.jp