CONSTRUCTION OF UNRAMIFIED GALOIS EXTENSIONS OVER MAXIMAL ABELIAN EXTENSIONS OF ALGEBRAIC NUMBER FIELDS

SACHIKO OHTANI

Series #489. August 2000

HOKKAIDO UNIVERSITY
PREPRINT SERIES IN MATHEMATICS

#465 N. Kawazumi and Y. Shibukawa, The meromorphic solutions of the Bruschi-Calogero equation, 20 pages. 1999.

#466 S. Izumiya, G. Kossioris and G. Makrakis, Multivalued solutions to the eikonal equation in stratified media, 24 pages. 1999.

#467 K. Kubota and K. Yokoyama, Global existence of classical solutions to systems of nonlinear wave equations with different speed of propagation, 105 pages. 1999.

#468 A. Higuchi, K. Matsue and T. Tsujishita, Deductive hyperdigraphs – a method of describing diversity of coherences, 35 pages. 1999.

#469 M. Nakamura and T. Ozawa, Small solutions to nonlinear Schrödinger equations in the Sobolev spaces, 26 pages. 1999.

#470 M. Nakamura and T. Ozawa, Small solutions to nonlinear wave equations in the Sobolev spaces, 27 pages. 1999.

#471 K. Ito and Y. Kohsaka, Stability of a stationary solution for evolving boundaries of symmetric three-phases driven by surface diffusion, 36 pages. 1999.

#472 Y. Giga and M.-H. Sato, A level set approach to semicontinuous viscosity solutions for Cauchy problems, 32 pages. 1999.

#473 R. Yoneda, Characterization of Bloch space and Besov spaces by oscillations, 31 pages. 1999.

#474 T. Nakazi, Norm inequalities for some singular integral operators, 13 pages. 1999.

#475 A. Inoue and Y. Kasahara, Asymptotics for prediction errors of stationary processes with reflection positivity, 15 pages. 1999.

#476 T. Sano, On affine parallels of generic plane curves, 8 pages. 1999.

#477 T. Nakazi, On an invariant subspace whose common zero set is the zeros of some function, 11 pages. 1999.

#478 M.-H. Giga and Y. Giga, Generalized motion by nonlocal curvature in the plane, 68 pages. 2000.

#479 M.-H. Giga and Y. Giga, Crystalline and level set flow – Convergence of a crystalline algorithm for a general anisotropic curvature flow in the plane, 16 pages. 2000.

#480 A. Arai and M. Hirokawa, Stability of ground states in sectors and its application to the Wigner-Weisskopf model, 16 pages. 2000.

#481 T. Nakazi, Two dimensional Q-algebras, 11 pages. 2000.

#482 N. H. Bingham and A. Inoue, Tauberian and Mercerian theorems for systems of kernels, 16 pages. 2000.

#483 N. H. Bingham and A. Inoue, Abelian, Tauberian and Mercerian theorems for arithmetic sums, 29 pages. 2000.

#484 I. A. Bogaevski and G. Ishikawa, Lagrange mappings of the first open Whitney umbrella, 22 pages. 2000.

#485 A. Arai and H. Kawano, A class of deformations of the Schrödinger representation of the Heisenberg commutation relation and exact solution to a Heisenberg equation and a Schrödinger equation, 22 pages. 2000.

#486 T. Nakazi, Functions in N_+ with the positive real parts on the boundary, 21 pages. 2000.

#487 Y. Shibukawa, Classification of the R-operator, 36 pages. 2000.

#488 A. Inoue, Asymptotic behaviour for partial autocorrelation functions of fractional ARIMA processes, 20 pages. 2000.

CONSTRUCTION OF UNRAMIFIED GALOIS EXTENSIONS OVER MAXIMAL ABELIAN EXTENSIONS OF ALGEBRAIC NUMBER FIELDS

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. Suppose 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 we replace K by a suitable finite extension L of K, then the abelian variety $A \otimes_K L$ over L satisfies the condition (A0) by the *semistable reduction theorem* (*cf.* Grothendieck [8], Proposition 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

Theorem 0.1. *Let A, K and p be as above, and F 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 the 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 $K_{n+1} \cap K_1 K_2 \cdots K_n = k$ for any $n \geq 1$, then we say that the extensions are *linearly independent* over k.

We shall now 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 [19] 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 order 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 give a general construction, at the expense of enlarging the base field, using abelian varieties which have everywhere semistable reduction.

Next we shall explain the contents of this paper. In Section 1, we give the proof of Theorem 0.1. In Section 2, we 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 construct infinitely many unramified Galois extensions over $\mathbb{Q}(\zeta_{p^\infty})^{\mathrm{ab}}$ having $SL_2(\mathbb{Z}_p)$ as the Galois group over $\mathbb{Q}(\zeta_{p^\infty})^{\mathrm{ab}}$, and we give the proof of Theorem 0.2. In Section 4, we consider elliptic curves of prime conductor p of Setzer [17], 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.

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 m-division points of an abelian variety A.

1. Division Points of Abelian Varieties

In this section, we shall give the proof of Theorem 0.1.

1.1. **Key lemmas.** In our construction of unramified Galois extensions over maximal abelian extensions of algebraic number fields, a key is the following lemma due to Y. Ihara.

Lemma 1.1 (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 $Kk^{\mathrm{ab}}/k^{\mathrm{ab}}$ is unramified if and only if its decomposition group in K/k is commutative for any prime divisor of K.*

Next we shall give an application of *Mumford's construction* of degenerate 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. Suppose 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 v be a place of K such that A has bad reduction at v, and G the identity component of the Néron model of A at v. By the condition (A0), G is a semi-abelian group scheme over $\mathrm{Spec}\,(\mathcal{O}_{K_v})$. If the special fibre $\mathcal{A}_v^0$ of G is a split torus, then there exists a group isomorphism

$$\phi : (K_v^\times)^g/\Lambda \xrightarrow{\sim} G(K_v) \simeq A(K_v), \quad \Lambda \simeq \mathbb{Z}^g,$$

by Faltings-Chai [6], Ch.III, Proposition 8.1. Hence we obtain the following

Lemma 1.2. (*a*) *Let $m \geq 2$ be an integer and $\Lambda^{1/m} = \{x \in (K_v^\times)^g \mid x^m \in \Lambda\}$. Then the group isomorphism ϕ induces an isomorphism of G_{K_v}-modules*

$$\Lambda^{1/m}/\Lambda \simeq A[m].$$

(*b*) *Further, $\Lambda^{1/m}/\Lambda$ fits into the following exact sequence of G_{K_v}-modules:*

$$1 \longrightarrow \boldsymbol{\mu}_m{}^g \longrightarrow \Lambda^{1/m}/\Lambda \longrightarrow (\mathbb{Z}/m\mathbb{Z})^g \longrightarrow 0$$

where $\boldsymbol{\mu}_m$ is the group of m-th roots of unity.
(*c*) *Let $(q_i)_{1\le i\le g}$ be a basis of Λ, and put $q_i = (q_{i1}, q_{i2}, \cdots, q_{ig}) \in (K_v^\times)^g$ for each $1 \le i \le g$. Then*

$$K_v(A[m]) = K_v\left(\zeta_m, \{q_{ij}^{1/m}\}_{1\le i,j\le g}\right),$$

where $K_v(A[m])$ is the field obtained by adjoining to K the coordinates of m-division points on A.

Proof. The group isomorphism ϕ above induces a homomorphism

$$\tilde{\phi} : \Lambda^{1/m} \longrightarrow A[m],$$

and the kernel is equal to Λ. Let $(q_i)_{1\le i\le g}$ be a basis of Λ, and put $q_i = (q_{i1}, q_{i2}, \cdots, q_{ig}) \in (K_v^\times)^g$ for each $1 \le i \le g$. If $x \in \Lambda^{1/m}$, then x may be written as follows:

$$(*) \qquad x = \left(\zeta_m^{r_1} \prod_{i=1}^{g} q_{i1}^{s_i/m}, \cdots, \zeta_m^{r_g} \prod_{i=1}^{g} q_{ig}^{s_i/m}\right),$$

where $r_1, \cdots, r_g \in \mathbb{Z}/m\mathbb{Z}, s_1, \cdots, s_g \in \mathbb{Z}$. Since the order of the group $\Lambda^{1/m}/\Lambda$ is equal to the order of the group $A[m]$, we see that $\tilde{\phi}$ is surjective. Further if $x \in \Lambda^{1/m}$, then we see that $\tilde{\phi}(\sigma(x)) = \tilde{\phi}(x)^\sigma$ for any $\sigma \in G_{K_v}$. Hence we obtain an isomorphism of G_{K_v}-modules $\Lambda^{1/m}/\Lambda \longrightarrow A[m]$. From the equation (*), we see that $\Lambda^{1/m}/\Lambda$ fits into the exact sequence of the statement of (b), and we obtain the following isomorphisms:

$$K_v(A[m]) = K_v(\Lambda^{1/m}/\Lambda) = K_v\left(\zeta_m, \{q_{ij}^{1/m}\}_{1\le i,j\le g}\right).$$

□

1.2. **Proof of Theorem 0.1.** Let A be an abelian variety of dimension g over an algebraic number field K and $p \ge 5$ a prime number. Suppose that the pair (A, p) satisfies the conditions (A0) and (A1) in 1.1. Let r be a positive integer, and F_r the field obtained by adjoining to K the coordinates of p^r-division points on A. Theorem 0.1 (*a*) follows from the following

Theorem 1.3. *Suppose that 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 show 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, there is nothing to prove. Hence we only have to verify it for the places which are ramified in F_r. By the *criterion of Néron-Ogg-Shafarevich* (*cf.* Serre-Tate [16], 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. By Lemma 1.2 (c), we have

$$F_r K_v = K_v\left(\zeta_{p^r}, \{q_{ij}^{1/p^r}\}_{1\leq i,j\leq g}\right).$$

Hence $F_r K_v$ is a Kummer extension over $K_v(\zeta_{p^r})$. In particular, it is abelian. □

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. It suffices to show that $F_r K_v \mathbb{Q}^{\mathrm{ab}}$ 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, using Lemma 1.1 again.

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

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

Since A has semistable reduction at v, we see that the image of the absolute inertia subgroup of G_{K_v} by ρ_p is isomorphic to $\mathbb{Z}_p(1)$ by Grothendieck [8], Proposition 3.5, Corollary 3.5.2. Hence $F_r K_v^{\mathrm{nr}}$ is abelian over K_v^{nr}, where K_v^{nr} is the maximal unramified extension of K_v. Since K_v^{nr} is cyclotomic over K_v, we see that $F_r K_v \mathbb{Q}^{\mathrm{ab}}$ 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. Suppose that $v(j) < 0$ for any places 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], Proposition 3.6) and the assumption of Theorem 0.1 (a) by *Tate's theory* (*cf.* Lang [11], §15).

In particular, if $k = \mathbb{Q}$ then we can see a field K explicitly such that $FK(\zeta_{p^\infty})^{\mathrm{ab}}$ is an unramified over $K(\zeta_{p^\infty})^{\mathrm{ab}}$. We shall prove that we can take a solvable extension of $\mathbb{Q}$ as such a field K, and if $K/\mathbb{Q}$ is solvable and E satisfies an 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 unramified Galois extension of Theorem 0.1.

Proposition 2.1. *(a) Let E be an elliptic curve over $\mathbb{Q}$, $p \geq 5$ a prime number. Suppose 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 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 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 primes p in this case by Serre [14], Théorème 2.

Proof. (a) First we shall find a finite extension K of $\mathbb{Q}$ such that $E \otimes_{\mathbb{Q}} K$ has everywhere semistable reduction over $\mathcal{O}_K$. Suppose that E is defined by the following equation:

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

where e_1, e_2, e_3 are distinct. Then the change of coordinates

$$x = (e_2 - e_1)x' + e_1, \ y = (e_2 - e_1)^{3/2}y'$$

gives the following form:

$$E_\lambda \ : \ (y')^2 = x'(x' - 1)(x' - \lambda), \qquad \lambda = (e_3 - e_1)/(e_2 - e_1) \in \bar{\mathbb{Q}}.$$

Let L be the Galois closure of $\mathbb{Q}(\sqrt{e_2 - e_1}, e_1)$. Then L is solvable over $\mathbb{Q}$. Since E is isomorphic to E_λ over $\mathbb{Q}(\sqrt{e_2 - e_1}, e_1)$, so is over L. Hence we may regard E as defined over L and given by the following equation:

$$E \ : \ y^2 = x(x - 1)(x - \lambda).$$

Note that $\lambda \in L$. Now we shall use the notation of Silverman [18]. Then we see the quantity $c_4 = 16(\lambda^2 - \lambda + 1)$ and the discriminant $\Delta = 16\lambda^2(\lambda - 1)^2$ by simple calculations.

Now we put $S = \{v \ : \text{a place of } L \,|\, v(\lambda) < 0\}$. If $S = \varnothing$, then E has everywhere semistable reduction over $\mathcal{O}_L$. In this case we can take L as the field K of the statement of (a). Next suppose that $S \neq \varnothing$. 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 $\mathfrak{p}_v\mathcal{O}_H = (\pi_v)$. Further, for any v in S, there exist positive integers r_v such that $v(\lambda \prod_{v \in S} \pi_v^{r_v}) = 0$ for any $v \in S$. We put $\pi = \prod_{v \in S} \pi_v^{r_v}$ and $u = \lambda\pi$. Then the change of coordinates

$$x = \pi^{-1}x', \ y = \pi^{-3/2}y'$$

gives the following form:

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

Let w be the extension of $v \in S$ 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 Silverman

[18], Ch.VII, Remark 1.1, Proposition 3.6. 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). Thus we see that there exists the solvable extension K of $\mathbb{Q}$ such that $E \otimes_{\mathbb{Q}} K$ has everywhere semistable reduction over $\mathcal{O}_K$.

Next we shall show that $F_r K(\zeta_{p^r})^{\mathrm{ab}}$ 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.* Serre [13], Appendix, A.1.1), 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 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 (*cf.* Lang [11], Ch.15, §2). Hence $F(q)_r K_v$ is a Kummer extension over $K_v(\zeta_{p^r})$, in particular, it is abelian. Then $F_r K_v'$ is also an abelian extension of $K_v(\zeta_{p^r})$. Hence we see that $F_r K_v$ 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 quotients, we see that

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

Hence we see

$$\mathrm{Gal}\,(F_1 K(\zeta_{p^r})^{\mathrm{ab}}/K(\zeta_{p^r})^{\mathrm{ab}}) \cong SL_2(\mathbb{F}_p).$$

The proposition follows from the following

Lemma 2.2 (Serre [13], 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 $X = SL_2(\mathbb{Z}_p)$.*

□

From 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 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.* [5], IV, (3.1)). Its associated *coarse* moduli stack (*cf.* [5], I, (8.1)) may be denoted by M_H. If $H = \Gamma_0(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \mid c \equiv 0 \pmod{N}\}$, 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 $M_0(p)$, $\mathcal{J}$ 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. From 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 an 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 shall describe k and K explicitly. We put $X(\mathcal{J}_p^0) = \mathrm{Hom}_{\bar{\mathbb{F}}_p}(\mathcal{J}_p^0, \mathbb{G}_m)$. 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. Further $G_{\mathbb{F}_p}$ acts on $\mathbb{G}_m$. Hence we obtain a continuous representation

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

Note that the image of ρ is finite. Hence we see that there exists a positive integer N such that ρ factors through a finite quotient $\mathrm{Gal}\,(\mathbb{F}_{p^N}/\mathbb{F}_p) \simeq \mathbb{Z}/N\mathbb{Z}$. Thus $\mathcal{J}_p^0 \otimes_{\mathbb{F}_p} \mathbb{F}_{p^N}$ is a split torus. We can take as k the field $\mathbb{F}_{p^N} = \mathbb{F}_p(\zeta_{p^N-1})$. Further we may take as K a field such that the residue field of v contains $\mathbb{F}_{p^N}$ for every place v lying above p, for example, $\mathbb{Q}(\zeta_{p^N-1})$.

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. Then there exists a finite solvable extension K over $\mathbb{Q}$ such that $FK(\zeta_{p^\infty})^{\mathrm{ab}}$ is an unramified Galois extension of $K(\zeta_{p^\infty})^{\mathrm{ab}}$.*

3. Division Points of Elliptic Curves

In this section, we shall give the proof of Theorem 0.2. Throughout this section, let k be the field obtained by adjoining to $\mathbb{Q}$ the coodinates of all p-power roots of unity, k_r the field obtained by adjoining to $\mathbb{Q}$ the coodinates of 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 $\mathbb{Q}$, $p \geq 5$ a prime number. Suppose 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 p^r-th power 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 2.1. □

From Proposition 3.1, we obtain the following

Corollary 3.2. *Let E, p, k and F 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 $\mathbb{Q}$, $p \geq 5$ a prime number. Suppose that the pair (E, p) satisfies the condisions (E0), (E1) of 3.1 and the following conditions:

(E2) E has three rational 2-division points.

(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 extention 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 obtain a representation

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

Now we denote $G_l = \mathrm{Im}\rho_l$. To show this proposition, we shall verify the conditions of the following lemma (*cf.* Serre [13], Ch.IV, 3.2, Lemma 2).

Lemma 3.4. *If G_l satisfies the next three conditions $(a), (b), (c)$, 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_l-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 [13], Ch.IV, 3.2. Hence we shall show 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_p-module. Then E contains a subgroup X whose order is p and which is stable under the action of G_p. Since E has everywhere semistable reduction and multiplicative reduction at p, by Serre [14], p.307, the action of $G_{\mathbb{Q}}$) on X is described by two characters χ' and χ'' as follows: $\chi' = 1,\ \chi'' = \chi$ 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 rational 2-division points,

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

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

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

3.3. **Infinite existence.** In this subsection, we shall give the 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 [15], 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 all 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. By the assumption and the criterion of Néron-Ogg-Shafarevich ([16], Theorem 1), we see that p_1 is unramified in $F_1^{(2)}$. Next we consider the ramification of p_1 in $F_1^{(1)}$. $E^{(1)} \otimes_{\mathbb{Q}} \mathbb{Q}_{p_1}$ 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 $\mathbb{Q}$ to L, then we see that

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

Further since p_1 is unramified in $\mathbb{Q}(\zeta_p)$, if v'_{p_1} is an extension of v_{p_1} to $\mathbb{Q}(\zeta_p)$, then $v'_{p_1}(q) = 2$. Let w_{p_1} be an extension of v'_{p_1} to $F_1^{(1)}$ and e_{p_1} 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 $F_1^{(1)}$. So we obtain $F_1^{(1)} \neq F_1^{(2)}$. Let $F_1'^{(i)}$ be the subextension of $F_1^{(i)}$ of $\mathbb{Q}(\zeta_p)$ corresponding to the normal subgroup $\{\pm 1\}$ of $SL_2(\mathbb{F}_p)$ $(i = 1, 2)$. Suppose that $F_1'^{(1)} = F_1'^{(2)}$. 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 $F_1'^{(1)} \neq F_1'^{(2)}$. Since

$$\operatorname{Gal}(F_1'^{(i)}/\mathbb{Q}(\zeta_p)) \simeq PSL_2(\mathbb{F}_p),$$

which is a simple group, we have

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

□

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 are no non-trivial abelian quotients of $SL_2(\mathbb{F}_p) \times SL_2(\mathbb{F}_p)$, we see

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

By Lemma 2.2, we obtain

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

□

Now we can choose an infinite family of elliptic curves over $\mathbb{Q}$ inductively. Suppose 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}. Base 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 extension 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 rational prime such that $p = u^2 + 64$ for some rational integer u, and E an elliptic curve of conductor p over $\mathbb{Q}$ with a non-trivial rational 2-division point.

By Theorem 2 of Setzer [17], if p is of the form $u^2 + 64$, where u is a rational 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

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

Now we assume that E is given by this equation. The modurlar 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 p^r-th power 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 funtion.*

Proof. By the assumption, the extension F_r is unramified outside p over $\mathbb{Q}$. Since E has multiplicative reductiuon 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 shall verify the conditions (a),(b),(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 [13], Ch.IV, 3.2. Next we shall show that the condition (c) is satisfied for p. Assume $E[p]$ is reducible as G_p-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_p. Now we put $E' = E/X$, then we have an exact sequence

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

Here λ is a separable isogeny of degree p. E' is not isomorphic to E, because E has no complex multiplication. E' has a non-trivial rational 2-division point, and we see that E' has conductor p by Serre-Tate [16], §1, Corollary 1. 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 this 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

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

By Lemma 2.2, we obtain

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

□

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, 1979, pp.82-88.
[5] Deligne, P. and Rapoport, M., *Les schémas de modules de courbes elliptiques*, Lecture Notes in Math. **349**, Springer-Verlag, 1973, pp.143-316.
[6] Faltings, G. and Chai, C.L., *Degeneration of abelian varieties*, Ergeb. Math. Grenzgeb. (3) **22**, Springer-Verlag, 1990.
[7] Fontaine, J.-M. and Mazur, B., *Geometric Galois representations*, Proc. Conf. on elliptic curves and modular forms, Hong Kong, 1993, International Press, 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, 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*, Addison Wesley, Reading. Mass, 1970.
[12] Mazur, B., *Modular curves and the Eisenstein ideal*, Publ. Math. I.H.E.S. **47** (1977), 33-186.
[13] Serre, J.-P., *Abelian l-adic representations and elliptic curves*, Benjamin, NewYork, 1968.
[14] Serre, J.-P., *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259-331.
[15] 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.
[16] Serre, J.-P. and Tate, J., *Good reduction of abelian varieties*, Ann. of Math. **88** (1968), 492-517.
[17] Setzer, B., *Elliptic curves of prime conductor*, J. London Math. Soc.(2), **10** (1975), 367-378.
[18] Silverman, J.H., *The arithmetic of elliptic curves*, Graduate Texts in Math. **106**, Springer-Verlag, 1986.
[19] Uchida, K, *Galois groups of unramified solvable extensions*, Tohoku Math. J. (2) **34** (1982), 311-317.

DEPARTMENT OF MATHEMATICS, HOKKAIDO UNIVERSITY, SAPPORO 060-0810, JAPAN
E-mail address: sohtani@math.sci.hokudai.ac.jp