J. Fac. Sci. Univ. Tokyo
Sect. IA, Math.
32 (1985), 397-415.

Construction of certain non-solvable unramified Galois extensions over the total cyclotomic field

By Mamoru ASADA

(Communicated by Y. Ihara)

§ 0. Introduction

This is a continuation of our previous paper [1].

Let Q be the field of rational numbers, Q_{ab} be the maximum abelian extension of Q, i.e., the total cyclotomic field, and M be the maximum unramified Galois extension of Q_{ab}. Let Q_{ab}^t denote the maximum tamely ramified abelian extension of Q, i.e., the field obtained by adjoining to Q the p-th roots of unity, where p runs over all prime numbers, and M^t be the maximum unramified Galois extension of Q_{ab}^t. Furthermore, let M_0 be the composite of M^t and Q_{ab}, so that $Q_{ab} \subset M_0 \subset M$. Our result in this paper is summarized as the following

THEOREM 3. *Let $p \geq 5$ be a prime number and r be a positive integer. Then, there exist infinitely many linearly independent Galois extensions of Q_{ab} (resp. M_0) contained in M having $\mathrm{PSL}_2(Z/p^rZ)$ as the Galois group over Q_{ab} (resp. M_0).*

We shall now explain the background of this theorem. Unramified abelian extensions of Q_{ab}, or more generally, those of k_{ab}, the maximum abelian extension of an algebraic number field k of finite degree over Q, have been investigated in Cornell [3] and Brumer [2]. Uchida [18] determined the structure of the Galois group of the maximum unramified solvable extension of k_{ab}, where k is as above (a special case of his results). As for non-solvable unramified extensions of M_0, we showed, in our previous paper [1], that there exist infinitely many linearly independent unramified Galois extensions of M_0 having A_n, the alternating group of degree n, as the Galois group over M_0, where n is any odd integer ([1] Theorem 2). Thus, Theorem 3 is a new result about the non-solvable unramified extensions of Q_{ab} and M_0. (The group $\mathrm{PSL}_2(Z/p^rZ)$ is non-solvable for p and r as above.)

We shall sketch the idea to construct those extensions of Q_{ab} and M_0 in Theorem 3. Let p, r be as in Theorem 3 and E be an elliptic curve over Q.

Let K'_{p^r} denote the field obtained by adjoining to Q the "x-coordinates" of the p^r-division points on E. We shall obtain the extensions of Q_{ab} (resp. M_0) in Theorem 3 as the composite of K'_{p^r} and Q_{ab} (resp. M_0) by suitably choosing a family of elliptic curves over Q. The most important property of our elliptic curve is that it is isomorphic (over a quadratic extension of Q_p) to a Tate curve over Q_p with the period "divisible by p^r". (Q_p denotes the field of p-adic numbers.) By using this and some other special properties, we can show that $K'_{p^r}Q_{ab}$ (resp. $K'_{p^r}M_0$) is unramified over Q_{ab} (resp. M_0). We can also determine the Galois group of $K'_{p^r}Q_{ab}$ (resp. $K'_{p^r}M_0$) over Q_{ab} (resp. M_0) by using the precise results on the rational points on modular curves by Serre, Mazur, and Momose. To show the infinite existence, we choose infinitely many elliptic curves suitably. The main tools are Čebotarev's density theorem, a classical result of the theory of complex multiplication, and some properties of the group $\mathrm{SL}_2(Z_p)$ mainly due to Serre.

The author wishes to express his sincere gratitude to Professor F. Momose for his help and encouragement, especially for providing him with the theory of the rational points on modular curves.

This paper is a part of the author's doctoral dissertation submitted to Tokyo University (1985). He wishes to express his sincere gratitude to Professor Yasutaka Ihara for his advice and encouragement.

Notation. Z and Q denote the ring of rational integers and the field of rational numbers respectively. For a prime number p, Z_p, Q_p, and F_p denote the ring of p-adic integers, the field of p-adic numbers, and the prime field Z/pZ, respectively.

When a field K is a finite or an infinite Galois extension of a field k, the Galois group of K over k is denoted by $\mathrm{Gal}(K/k)$.

§ 1. Some preliminaries

In this section we introduce elliptic curves defined over Q, which we shall use throughout this paper.

Let $p \geq 5$ be a prime number and n be a positive integer. Let $E_{j(n)}$ be the elliptic curve defined by the following Weierstrass equation;

$$E_{j(n)}: \ y^2 = 4x^3 - \frac{3^3 j(n)}{j(n)-12^3}x - \frac{3^3 j(n)}{j(n)-12^3}$$

$$(1) \qquad j(n) = -\frac{1}{(\varepsilon p)^{3n}}\{(1-3(\varepsilon p)^n)(1+3^2(\varepsilon p)^n)\}^3, \quad \varepsilon = \left(\frac{-1}{p}\right).$$

As $j(n) \in \boldsymbol{Q}$ and $j(n) \neq 0, 12^3$, $E_{j(n)}$ is actually an elliptic curve defined over $\boldsymbol{Q}$ with the modular invariant $j(n)$. Until the end of § 3, for the sake of simplicity, we write $j(n)=j$ and $E_{j(n)}=E_j$.

Here, we summarize some fundamental properties of E_j as the following

LEMMA 1. (i) *Over the unramified quadratic extension of* $\boldsymbol{Q}_p$, $E_j \otimes_{\boldsymbol{Q}} \boldsymbol{Q}_p$ *is isomorphic to a Tate curve over* $\boldsymbol{Q}_p$.

(ii) *The elliptic curve* E_j *has good reduction at* 3.

(iii) *Let* $l(\neq p, 3)$ *be a rational prime. Then,* E_j *has potential good reduction at* l. *The prime* l *is a bad prime of* E_j *if and only if* l *is ramified in* K_3, *the field obtained by adjoining to* $\boldsymbol{Q}$ *all coordinates of the* 3*-division points on* E_j. *The field* K_3 *is explicitly given as*

$$K_3=\boldsymbol{Q}(\sqrt{-3},\ \mu,\ \sqrt{2\mu(\mu^3+8)(8+20\mu^3-\mu^6)}),$$

where μ *is a root of the equation*

$$x^2+\left\{\frac{1}{3(\varepsilon p)^n}+1\right\}x-\frac{1}{3(\varepsilon p)^n}+1=0. \tag{2}$$

PROOF. (i) We use the notation of Néron-Tate (cf. e.g. Tate [17]). Then, we have

$$\Delta=2^6 3^{12}\frac{j^2}{(j-12^3)^3},$$

$$c_4=12\,g_2=12\frac{3^3 j}{j-12^3}.$$

So, $v_p(\Delta)>0$, $v_p(c_4)=0$, where v_p is the p-adic additive valuation normalized as $v_p(p)=1$. Therefore, E_j has multiplicative reduction at p. So, by the general theory of Tate curves (cf. e.g. Serre [14], Tate [17]), over the unramified quadratic extension of $\boldsymbol{Q}_p$, $E_j \otimes_{\boldsymbol{Q}} \boldsymbol{Q}_p$ is isomorphic to the Tate curve over $\boldsymbol{Q}_p$ with modular invariant $j(E_j)$.

(ii) As is easily verified, E_j is isomorphic over $\boldsymbol{Q}$ to the elliptic curve E over $\boldsymbol{Q}$ defined by the equation

$$E:\ y^2+xy=x^3-\frac{j+2^6 3^2}{2^4(j-12^3)}x-\frac{j+2^6}{2^6(j-12^3)},$$

so E_j has good reduction at 3.

(iii) As j is l-integral, i.e., $v_l(j)\geq 0$, E_j has potential good reduction at l, and by the criterion of Néron-Ogg-Šafarevič (cf. e.g. Serre-Tate [16] 1), l is

a bad prime of E_j if and only if l is ramified in K_3. Now, let $\mathcal{E}_\mu$ be the following elliptic curve;

$$\mathcal{E}_\mu : x^3+y^3+z^3=3\mu xyz \,/\boldsymbol{Q}(\mu).$$

Then, by simple calculations, we get

$$j(n)=3^3\left\{\frac{\mu(\mu^3+2^3)}{\mu^3-1}\right\}^3 \text{ 1)},$$

so that E_j is isomorphic (over $\boldsymbol{Q}(\mu, \sqrt{2\mu(\mu^3+8)(8+20\mu^3-\mu^6)})$) to $\mathcal{E}_\mu$. The fact that $K_3=\boldsymbol{Q}(\sqrt{-3}, \mu, \sqrt{2\mu(\mu^3+8)(8+20\mu^3-\mu^6)})$ holds in the "generic" case is proved in Igusa [7] § 4. The proof of our special case is the same as that.

§ 2. Construction of unramified extensions over $\boldsymbol{Q}_{ab}$

In the rest of this paper, let $p\geq 5$ be a prime number and r be a fixed positive integer. Our aim in this section is to prove the following

THEOREM 1. *There exists an unramified Galois extension F of $\boldsymbol{Q}_{ab}$ such that* $\mathrm{Gal}(F/\boldsymbol{Q}_{ab})\simeq \mathrm{PSL}_2(\boldsymbol{Z}/p^r\boldsymbol{Z})$.

The proof of Theorem 1 is rather long and requires somewhat long preliminaries. Let n be a positive integer and $E_j=E_{j(n)}$ be the elliptic curve defined in § 1. Let K (resp. K') denote the field obtained by adjoining to $\boldsymbol{Q}$ all coordinates (resp. the "x-coordinates") of the p^r-division points on E_j. The fields K and K' are Galois extensions of $\boldsymbol{Q}$ and K' is a subfield of K. We shall obtain the field F in Theorem 1 as the composite of K' and $\boldsymbol{Q}_{ab}$, by suitably choosing n.

2.1. Unramifiedness of $K'\boldsymbol{Q}_{ab}/\boldsymbol{Q}_{ab}$

In this subsection, we shall show that $K'\boldsymbol{Q}_{ab}/\boldsymbol{Q}_{ab}$ is unramified under some additional conditions. We need the following

---

1) Use the equivalence

$$\frac{(c+2)(c-2)}{c+1}=\frac{\mu(\mu^3+2^3)}{\mu^3-1}\Longleftrightarrow\{\mu^2-c\mu+(c+2)\}\left(\mu^2+\frac{c+4}{c+1}\mu+\frac{c-2}{c+1}\right)=0$$

and put

$$c=-\frac{1}{3(\varepsilon p)^n}-1.$$

LEMMA 2 (Y. Ihara). *Let k be an algebraic number field of finite degree over $\boldsymbol{Q}$, k_{ab} be the maximum abelian extension of k, and K be a finite Galois extension of k. Then, Kk_{ab}/k_{ab} is unramified if and only if, for any prime divisor of K its decomposition group in K/k is commutative.*

This lemma was communicated to the author by Y. Ihara. For the proof, see [1].

PROPOSITION 1. *Let K' be as before. Assume that n is odd and $p^r \mid n$. Then, $K'\boldsymbol{Q}_{ab}/\boldsymbol{Q}_{ab}$ is an unramified Galois extension.*

PROOF. By Lemma 2, it suffices to show that

(C_l) $\quad K'\boldsymbol{Q}_l/\boldsymbol{Q}_l$ is an abelian extension

for every rational prime l. (We consider K' is contained in $\overline{\boldsymbol{Q}}_l$.) If l is unramified in K', the extension $K'\boldsymbol{Q}_l/\boldsymbol{Q}_l$ is cyclic, hence abelian. Therefore, we only have to verify the condition (C_l) for the primes which are ramified in K'. Such primes are, by the criterion of Néron-Ogg-Šafarevič, contained in the set $\{p\} \cup \{\text{the bad primes of } E_j\}$.

(i) $l=p$. By Lemma 1, $E_j \underset{\boldsymbol{Q}}{\otimes} \boldsymbol{Q}_p \simeq \underset{k}{E(q)}$, where k is the unramified quadratic extension of $\boldsymbol{Q}_p$ and $E(q)=\boldsymbol{G}_m/q^{\boldsymbol{Z}}$ $(q \in p\boldsymbol{Z}_p)$ is a Tate curve over $\boldsymbol{Q}_p$. The invariants j and q are related by the well-known formula

$$j=1/q+744+196884\,q+\cdots. \tag{3}$$

Therefore, if the field obtained by adjoining to $\boldsymbol{Q}_p$ all coordinates of the p^r-division points on $E(q)$ is an abelian extension of $\boldsymbol{Q}_p$, then, Kk is also an abelian extension of $\boldsymbol{Q}_p$. Especially the extension $K'\boldsymbol{Q}_p/\boldsymbol{Q}_p$ is abelian. So we may assume that $E_j \underset{\boldsymbol{Q}}{\otimes} \boldsymbol{Q}_p$ is a Tate curve over $\boldsymbol{Q}_p$.

As n is odd, it follows from (1) that $j\cdot(-\varepsilon p)^{3n} \equiv 1 \bmod p^n$. Therefore, $j\cdot(-\varepsilon p)^{3n} \in (\boldsymbol{Z}_p^*)^{p^{n-1}}$. By the assumption that $p^r \mid n$, it follows easily that

$$j \in (\boldsymbol{Q}_p^*)^{p^r}. \tag{*}$$

On the other hand, put $u=j\cdot q$. Then, $u \equiv 1 \bmod q$, by (3). As $v_p(q)=-v_p(j)=3n$, $u \in (\boldsymbol{Z}_p^*)^{p^{3n-1}}$, especially

$$u \in (\boldsymbol{Z}_p^*)^{p^r}. \tag{**}$$

By (*) and (**), it follows that $q \in (\boldsymbol{Q}_p^*)^{p^r}$.
Therefore, we see that $K\boldsymbol{Q}_p=\boldsymbol{Q}_p(\zeta_{p^r})$, where ζ_{p^r} is a primitive p^r-th root of

unity. Hence, KQ_p/Q_p is an abelian extension and especially the condition (C_l) is satisfied for $l=p$.

(ii) l: a bad prime of E_j $(l\neq p)$. By Lemma 1, $l\neq 3$ and E_j has potential good reduction at l. Let $(E_j)_{p^\infty}$ denote the group of all points of p-power order on E_j. Then, $\mathrm{Gal}(\bar{Q}_l/Q_l^{ur})$ acts naturally on $(E_j)_{p^\infty}$ and we get a representation ρ_I;

$$\rho_I:\ \mathrm{Gal}(\bar{Q}_l/Q_l^{ur})\longrightarrow \mathrm{Aut}(E_j)_{p^\infty}\simeq \mathrm{GL}_2(Z_p),$$

where Q_l^{ur} denotes the maximum unramified extension of Q_l. Let L be the subextension of $\bar{Q}_l$ over Q_l^{ur} corresponding to the subgroup $\mathrm{Ker}\,\rho_I\subset\mathrm{Gal}(\bar{Q}_l/Q_l^{ur})$. Let K_3 and μ be as in Lemma 1. We may consider K and K_3 are contained in $\bar{Q}_l$. Then, by a result of Ogg ([13] Proposition in II. See also Serre-Tate [16] 2.) and by Lemma 1,

$$L=KQ_l^{ur}=K_3Q_l^{ur}=Q_l^{ur}(\mu,\ \sqrt{2\mu(\mu^3+8)(8+20\mu^3-\mu^6)}).$$

Therefore, if we put

$$L_0=Q_l^{ur}(\mu),$$

which is an abelian extension of Q_l, then, $[L:L_0]=1$ or 2.

Case 1 $[L:L_0]=1$, i.e., $L=L_0$. In this case, L/Q_l is an abelian extension. Therefore, $K'Q_l/Q_l$ is an abelian extension.

Case 2 $[L:L_0]=2$. Let σ denote the generator of $\mathrm{Gal}(L/L_0)$. Then, as $\sigma^2=1$, we have $\rho_I(\sigma)^2=1$. On the other hand, as $\zeta^\sigma=\zeta^{\det\rho_I(\sigma)}$ for any p^m-th root of unity ζ $(m=1,2,\cdots)$, we have $\det\rho_I(\sigma)=1$. It follows that $\rho_I(\sigma)=\pm 1$. Hence, $K'Q_l^{ur}$, which is nothing but the subextension of $\bar{Q}_l$ over Q_l^{ur} corresponding to the subgroup $\rho_I^{-1}(\{\pm 1\})\subset\mathrm{Gal}(\bar{Q}_l/Q_l^{ur})$, is either L_0 or Q_l^{ur}. Therefore, $K'Q_l^{ur}/Q_l$ is an abelian extension and especially the condition (C_l) is satisfied for the bad primes of E_j.

This completes the proof of Proposition 1.

2.2. The Galois group of $K'Q_{ab}$ over Q_{ab}

In this subsection we shall prove the following

PROPOSITION 2. *Let K' be as before and assume that*

$$\begin{cases} p^r\mid n \\ n:\textit{odd}\ (n\equiv 11\ \textit{mod}\ 16\ \textit{if}\ p=5). \end{cases}$$

Then, $\mathrm{Gal}(K'\boldsymbol{Q}_{ab}/\boldsymbol{Q}_{ab}) \simeq \mathrm{PSL}_2(\boldsymbol{Z}/p^r\boldsymbol{Z})$.

PROOF. Let K_{p^∞} denote the field obtained by adjoining to $\boldsymbol{Q}$ all coordinates of the points of p-power order on E_j. We shall show that

$$(*) \qquad \mathrm{Gal}(K_{p^\infty}\boldsymbol{Q}_{ab}/\boldsymbol{Q}_{ab}) \simeq \mathrm{SL}_2(\boldsymbol{Z}_p).$$

Then, the proposition follows at once from this. Here we quote the following

LEMMA 3 (Serre [14] Ch. IV 3.4. Lemma 3). *Let X be a closed subgroup of $\mathrm{SL}_2(\boldsymbol{Z}_p)$ whose image in $\mathrm{SL}_2(\boldsymbol{F}_p)$ is $\mathrm{SL}_2(\boldsymbol{F}_p)$. Assume $p \geq 5$. Then, $X = \mathrm{SL}_2(\boldsymbol{Z}_p)$.*

By this lemma, to show $(*)$ it suffices to verify

$$(*)' \qquad \mathrm{Gal}(K_p/\boldsymbol{Q}) \simeq \mathrm{GL}_2(\boldsymbol{F}_p),$$

where K_p denotes the field obtained by adjoining to $\boldsymbol{Q}$ all coordinates of the p-division points on E_j.

To verify $(*)'$, we apply general results to $\mathrm{Gal}(K_p/\boldsymbol{Q})$. Here, we briefly summarize them. In general, let E be an arbitrary elliptic curve defined over $\boldsymbol{Q}$, $p \geq 5$ be a prime number, and E_p denote the group of the p-division points on E. Then, $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ acts naturally on E_p and we get a representation ρ_p;

$$\rho_p : \mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}) \longrightarrow \mathrm{Aut}\, E_p \simeq \mathrm{GL}_2(\boldsymbol{F}_p).$$

For the sake of simplicity, fix an isomorphism from $\mathrm{Aut}\, E_p$ to $\mathrm{GL}_2(\boldsymbol{F}_p)$ and identify the former with the latter. The field corresponding to the subgroup $\mathrm{Ker}\,\rho_p \subset \mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ is nothing but the field obtained by adjoining to $\boldsymbol{Q}$ all coordinates of the p-division points on E. Then, it is known that we have the following five cases for $\mathrm{Im}\,\rho_p$, the image of ρ_p (cf. e.g. Mazur [10]).

(i) $\mathrm{Im}\,\rho_p = \mathrm{GL}_2(\boldsymbol{F}_p)$.

(ii) The group $\mathrm{Im}\,\rho_p$ is contained in a Borel subgroup. In this case, if $p = 11$ or ≥ 17, E has potential good reduction at all rational primes except 2 (Mazur [11] Corollary 4.4).

(iii) The group $\mathrm{Im}\,\rho_p$ is contained in the normalizer of a split Cartan subgroup. In this case, if $p = 11$ or ≥ 17, E has potential good reduction at all rational primes except 2 (Momose [12] Proposition 3.1).

(iv) The group $\mathrm{Im}\,\rho_p$ is contained in the normalizer of a non-split Cartan subgroup.

(v) The group $\mathrm{Im}\,\rho_p$ is conjugate to a subgroup of the inverse image of $H \subset \mathrm{PGL}_2(F_p)$ in $\mathrm{GL}_2(F_p)$, where H is isomorphic to S_4, the symmetric group of degree 4.

Now we go back to the proof of Proposition 2. We apply the above results to our special case $E=E_j$.

Case 1 $p=11$ or ≥ 17. As j is not p-integral, E_j does not have potential good reduction at p. Therefore, for our E_j, the cases (ii) and (iii) do not occur. We shall exclude the cases (iv) and (v). We have shown in the proof of Proposition 1 that the invariant q of E_j belongs to $(Q_p^*)^p$. Therefore, $\rho_p(I)$ is conjugate to the subgroup

$$\left\{\begin{pmatrix} x & \\ & 1 \end{pmatrix} \middle| \; x \in F_p^*\right\},$$

where I is the inertia group of an extension of p to $\bar{Q}$ (Serre [15] 1.12. Corollary). Therefore, $\rho_p(I)$ is a cyclic group of order $p-1$ (≥ 10) so that the case (v) does not occur. Assume that the case (iv) occurs. Then, the subgroup $\rho_p(I)$ of $\mathrm{Im}\,\rho_p$ is contained in the normalizer of a non-split Cartan subgroup. Then, by Proposition 14 of Serre [15], $\rho_p(I)$ is contained in a non-split Cartan subgroup, which is impossible. So the case (iv) does not occur. Thus we have verified $(*)'$.

Case 2 $p=5, 7, 13$. We shall exclude the cases (ii)$\sim$(v). By the same argument as in the proof of Case 1, the case (iv) does not occur. To exclude the cases (ii), (iii), and (v), we use the following lemma, which is a part of Proposition 19 in Serre [15].

LEMMA 4 (Serre). *Let $p \geq 5$ be a prime number and $G \subset \mathrm{GL}_2(F_p)$ be a subgroup satisfying the following conditions*:

(1) $\det: G \longrightarrow F_p^*$ *is surjective.*

(2) *G is not contained in the normalizer of any non-split Cartan subgroup.*

Assume that G contains an element s_1 such that $\mathrm{Tr}(s_1)^2 - 4\cdot\det(s_1) \notin (F_p^*)^2$ and $\mathrm{Tr}(s_1) \neq 0$. Then, $G=\mathrm{GL}_2(F_p)$, or the image of G in $\mathrm{PGL}_2(F_p)$ is isomorphic to A_4 or S_4 or A_5. (A_n denotes the alternating group of degree n.)

Assume further that G contains an element s_2 such that

$$u = \frac{\mathrm{Tr}(s_2)^2}{\det(s_2)} \neq 0, 1, 2, 4 \text{ and } u^2 - 3u + 1 \neq 0.$$

Then, $G=\mathrm{GL}_2(F_p)$.

We apply this lemma to $\mathrm{Im}\,\rho_p$. (Note that $\mathrm{Im}\,\rho_p$ satisfies the condition (1), because E_j is defined over $\boldsymbol{Q}$.) In general, for a good prime l of E_j, let σ_l be the Frobenius automorphism of an extension of l to $\bar{\boldsymbol{Q}}$ and put $\pi_l=\rho_p(\sigma_l)\in \mathrm{GL}_2(\boldsymbol{F}_p)$. Up to conjugacy, π_l is uniquely determined by l.

(a) $p=5$. It is easily verified that $l=17$ is a good prime of E_j. Then, by simple calculations,

$$(\text{the number of } \boldsymbol{F}_{17}\text{-rational points on } E_j \bmod 17)=12.$$

So we have

$$\begin{aligned}
&\mathrm{Tr}(\pi_{17})=1+17-12=1,\\
&\det(\pi_{17})=17=2,\\
&\mathrm{Tr}(\pi_{17})^2-4\det(\pi_{17})=3\notin(\boldsymbol{F}_5^*)^2,\\
&u=\frac{\mathrm{Tr}(\pi_{17})^2}{\det(\pi_{17})}=3,\quad u^2-3u+1\neq 0.
\end{aligned}$$

Put $s_1=s_2=\pi_{17}$. Then, they satisfy the conditions in Lemma 4. Thus, $\mathrm{Im}\,\rho_5=\mathrm{GL}_2(\boldsymbol{F}_5)$ and $(*)'$ is verified.

(b) $p=7, 13$. By the same argument as in the proof of Case 1, the case (v) does not occur. Therefore, to exclude the cases (ii) and (iii), it suffices to show the existence of $s_1\in \mathrm{Im}\,\rho_p$ satisfying the condition in Lemma 4. (Note that by the general results on $\mathrm{Im}\,\rho_p$ summarized before, the image of $\mathrm{Im}\,\rho_p$ in $\mathrm{PGL}_2(\boldsymbol{F}_p)$ is isomorphic neither to A_4 nor to A_5.)

By Lemma 1 (ii), $l=3$ is a good prime of E_j. Then, by simple calculations,

$$(\text{the number of } \boldsymbol{F}_3\text{-rational points on } E_j \bmod 3)=\begin{cases} 3 & \cdots\ p=7\\ 6 & \cdots\ p=13.\end{cases}$$

So we have

$$\begin{aligned}
&\mathrm{Tr}(\pi_3)=\begin{cases}1+3-3=1 & \cdots\ p=7\\ 1+3-6=-2 & \cdots\ p=13,\end{cases}\\
&\det(\pi_3)=3 \qquad\qquad p=7, 13,\\
&\mathrm{Tr}(\pi_3)^2-4\det(\pi_3)=\begin{cases}3\notin(\boldsymbol{F}_7^*)^2 & \cdots\ p=7\\ 5\notin(\boldsymbol{F}_{13}^*)^2 & \cdots\ p=13.\end{cases}
\end{aligned}$$

Therefore, $s_1=\pi_3$ satisfies the condition in Lemma 4. Thus $\mathrm{Im}\,\rho_p=\mathrm{GL}_2(\boldsymbol{F}_p)$ and $(*)'$ is verified.

This completes the proof of Proposition 2.

2.3. Proof of Theorem 1

Let n be a positive integer satisfying the conditions in Proposition 2. Let K' be as before and put $F=K'Q_{ab}$. Then, by Propositions 1 and 2, F is an unramified Galois extension of Q_{ab} having $\mathrm{PSL}_2(Z/p^rZ)$ as the Galois group over Q_{ab}.

§ 3. Construction of unramified extensions over M_0

As before, let M^t be the maximum unramified Galois extension of Q_{ab}^t and $M_0=M^tQ_{ab}$. Our aim in this section is to prove the following

THEOREM 2. *There exists an unramified Galois extension E of M_0 such that* $\mathrm{Gal}(E/M_0)\simeq\mathrm{PSL}_2(Z/p^rZ)$.

In this section, let n be a positive integer satisfying the conditions in Proposition 2, namely,

$$\text{(C)}\qquad \begin{cases} p^r \mid n \\ n:\ \text{odd}\ (n\equiv 11 \bmod 16 \text{ if } p=5), \end{cases}$$

and $E_j=E_{j(n)}$ be the elliptic curve defined in § 1. Let K and K' be the Galois extensions of Q defined in § 2. In § 2 we have proved that $K'Q_{ab}$ is an unramified Galois extension of Q_{ab} having $\mathrm{PSL}_2(Z/p^rZ)$ as the Galois group over Q_{ab}. The field E in Theorem 2 shall be obtained as the composite of K' and M_0.

3.1. Some lemmas

In this subsection we shall prove some lemmas, which we need to prove Theorem 2.

LEMMA 5. *Let K_3 be the field obtained by adjoining to Q all coordinates of the 3-division points on E_j. Then, there exists only one prime divisor of K_3 lying above 2, and its inertia group is a cyclic group of order 4.*

PROOF. By Lemma 1,

$$K_3=Q\left(\sqrt{-3},\ \mu,\ \sqrt{2\mu(\mu^3+8)(8+20\mu^3-\mu^6)}\right),$$

where μ is a root of the equation (2). First, we shall show that K_3/Q is a Galois extension such that $\mathrm{Gal}(K_3/Q)\simeq D_4$, the dihedral group of order 8, and that $K_3/Q(\sqrt{-3})$ is a cyclic extension of degree 4. In fact, as

$$Q(\mu)=Q(\sqrt{a}),\quad a=1+18(\varepsilon p)^n-27(\varepsilon p)^{2n},$$

$Q(\mu)$ is an imaginary quadratic field in which the prime 3 is unramified. Therefore, $Q(\mu)\cap Q(\sqrt{-3})=Q$. Let σ_0 denote the generator of $\mathrm{Gal}(Q(\mu)/Q)$ and put

$$\alpha=2\mu(\mu^3+8)(8+20\mu^3-\mu^6).$$

Then, by simple calculations, we can show

$$\alpha^{\sigma_0}=\frac{(-3)^5}{(\mu-1)^{10}}\alpha.$$

(Using that $\mu^{\sigma_0}=(\mu+2)(\mu-1)^{-1}$, we obtain easily that $(\mu^3+8)^{\sigma_0}=3^2\mu(\mu^2-2\mu+4)(\mu-1)^{-3}$ and $(8+20\mu^3-\mu^6)^{\sigma_0}=-3^3(8+20\mu^3-\mu^6)(\mu-1)^{-6}$.) From this, it follows that K_3 is the Galois closure of $Q(\mu,\sqrt{\alpha})$ over Q. Therefore, $[K_3:Q]=8$ and $[K_3:Q(\sqrt{-3})]=4$. Let τ denote the generator of $\mathrm{Gal}(K_3/Q(\mu,\sqrt{\alpha}))$ and $\sigma\in\mathrm{Gal}(K_3/Q(\sqrt{-3}))$ be an extension of the generator of $\mathrm{Gal}(Q(\sqrt{-3},\mu)/Q(\sqrt{-3}))$. Then, it can be easily shown that

$$\tau^2=1,\quad \sigma^4=1,\quad \tau\sigma\tau^{-1}=\sigma^{-1},$$

which means $\mathrm{Gal}(K_3/Q)\simeq D_4$ and $K_3/Q(\sqrt{-3})$ is a cyclic extension of degree 4.

Now, since $\varepsilon p\equiv 1 \bmod 4$, $(\varepsilon p)^n\equiv 1$ or 5 or 9 or 13 mod 16. In any case, it is easily verified that $a\equiv 8 \bmod 16$. Therefore, the rational prime 2 ramifies in $Q(\mu)$. Thus, the prime $\mathfrak{p}=(2)$ of $Q(\sqrt{-3})$ ramifies in $Q(\mu,\sqrt{-3})$. Since $K_3/Q(\sqrt{-3})$ is cyclic, $\mathfrak{p}$ is totally ramified in $K_3/Q(\sqrt{-3})$. This completes the proof of Lemma 5.

COROLLARY. *The prime 2 is wildly ramified in K'/Q.*

PROOF. We may consider K, K', and K_3 are all contained in $\bar{Q}_2$. Then, by a result of Ogg quoted in the proof of Proposition 1,

$$KQ_2^{ur}=K_3Q_2^{ur}=Q_2^{ur}(\mu,\sqrt{2\mu(\mu^3+8)(8+20\mu^3-\mu^6)}).$$

By Lemma 5, KQ_2^{ur}/Q_2^{ur} is a cyclic extension of degree 4. As K/K' is at most a quadratic extension, the corollary follows at once.

Let K_p' denote the field obtained by adjoining to Q the "x-coordinates"

of the p-division points on E_j. The field K'_p is nothing but the field K' in the case that $r=1$.

LEMMA 6. $\mathrm{Gal}(K'_pM_0/M_0)\simeq \mathrm{PSL}_2(\boldsymbol{F}_p)$.

PROOF. In the proof of Proposition 2, we have already seen that $\mathrm{Gal}(K'_p/\boldsymbol{Q})\simeq \mathrm{GL}_2(\boldsymbol{F}_p)/\{\pm 1\}$. Since $\boldsymbol{Q}(\zeta_p)$ is the maximum abelian subextension of K'_p over $\boldsymbol{Q}$, it follows that $\mathrm{Gal}(K'_p\boldsymbol{Q}^t_{ab}/\boldsymbol{Q}^t_{ab})\simeq \mathrm{PSL}_2(\boldsymbol{F}_p)$. Thus, we see that $K'_p\boldsymbol{Q}^t_{ab}\cap M^t=\boldsymbol{Q}^t_{ab}$. This follows from the facts that $\mathrm{PSL}_2(\boldsymbol{F}_p)$ is a simple group, 2 is wildly ramified in $K'_p\boldsymbol{Q}^t_{ab}$ (Corollary to Lemma 5), and $M^t/\boldsymbol{Q}$ is only tamely ramified. Therefore, $\mathrm{Gal}(K'_pM^t/M^t)\simeq \mathrm{PSL}_2(\boldsymbol{F}_p)$. As M_0/M^t is abelian, the lemma follows at once.

3.2. Proof of Theorem 2

Put $E=K'M_0$. Then, by Proposition 1, E/M_0 is an unramified Galois extension. We shall show that

$$(*)\qquad \mathrm{Gal}(E/M_0)\simeq \mathrm{PSL}_2(\boldsymbol{Z}/p^r\boldsymbol{Z}).$$

We have already seen that $\mathrm{Gal}(K_{p^\infty}\boldsymbol{Q}_{ab}/\boldsymbol{Q}_{ab})\simeq \mathrm{SL}_2(\boldsymbol{Z}_p)$, where K_{p^∞} denotes the field obtained by adjoining to $\boldsymbol{Q}$ all coordinates of the points of p-power order on E_j. (Refer to the proof of Proposition 2.) Therefore, to verify $(*)$, it is enough to show that $K_{p^\infty}\boldsymbol{Q}_{ab}\cap M_0=\boldsymbol{Q}_{ab}$. Fix a p-adic coordinate system of E_j and identify $\mathrm{Gal}(K_{p^\infty}\boldsymbol{Q}_{ab}/\boldsymbol{Q}_{ab})$ with $\mathrm{SL}_2(\boldsymbol{Z}_p)$. Let N be the normal subgroup of $\mathrm{SL}_2(\boldsymbol{Z}_p)$ corresponding to the Galois subextension $K_{p^\infty}\boldsymbol{Q}_{ab}\cap M_0$ of $K_{p^\infty}\boldsymbol{Q}_{ab}$ over $\boldsymbol{Q}_{ab}$. We shall show that $N=\mathrm{SL}_2(\boldsymbol{Z}_p)$.

Put $\tilde{N}=N\Gamma(p)$, where

$$\Gamma(p)=\left\{\begin{pmatrix} a & b\\ c & d\end{pmatrix}\in \mathrm{SL}_2(\boldsymbol{Z}_p)\;\middle|\; \begin{matrix} a\equiv d\equiv 1 \bmod p\\ b\equiv c\equiv 0 \bmod p\end{matrix}\right\}.$$

Then, $\tilde{N}/\Gamma(p)$ is a normal subgroup of $\mathrm{SL}_2(\boldsymbol{Z}_p)/\Gamma(p)=\mathrm{SL}_2(\boldsymbol{F}_p)$. Therefore, it follows easily that $\tilde{N}/\Gamma(p)=\{1\}$ or $\{\pm 1\}$ or $\mathrm{SL}_2(\boldsymbol{F}_p)$. If $\tilde{N}/\Gamma(p)=\{1\}$ or $\{\pm 1\}$, $N\subset\Gamma(p)\{\pm 1\}$. This means that $K_{p^\infty}\boldsymbol{Q}_{ab}\cap M_0\supset K'_p\boldsymbol{Q}_{ab}$, i.e., $M_0\supset K'_p\boldsymbol{Q}_{ab}$. This contradicts Lemma 6. So, $\tilde{N}/\Gamma(p)=\mathrm{SL}_2(\boldsymbol{F}_p)$. Hence, $N=\mathrm{SL}_2(\boldsymbol{Z}_p)$ by Lemma 3 and the proof is completed.

§ 4. Infinite existence

Our purpose in this section is to prove the following

THEOREM 3. *There exist infinitely many lineary independent Galois*

extensions of Q_{ab} *(resp.* M_0*) contained in* M *having* $\mathrm{PSL}_2(Z/p^rZ)$ *as the Galois group over* Q_{ab} *(resp.* M_0*).*

We have already shown that there exists at least one Galois extension of Q_{ab} (or M_0) satisfying the condition of Theorem 3. To show the infinite existence, we need some more technical preliminaries.

In this section, let n_α $(\alpha=1, 2, \cdots)$ be positive integers satisfying the condition (C) in § 3. For such n_α, let $E_{j(n_\alpha)}$ be the elliptic curve defined in § 1. For the sake of simplicity, we write E_{j_α} in place of $E_{j(n_\alpha)}$. Let $K'^{(\alpha)}$ denote the field obtained by adjoining to Q the "x-coordinates" of the p^r-division points on E_{j_α} $(\alpha=1, 2, \cdots)$. In (the proof of) Theorem 1 (resp. Theorem 2), we have seen that $K'^{(\alpha)}Q_{ab}/Q_{ab}$ (resp. $K'^{(\alpha)}M_0/M_0$) is an unramified Galois extension having $\mathrm{PSL}_2(Z/p^rZ)$ as the Galois group over Q_{ab} (resp. M_0). To prove Theorem 3, we choose n_α $(\alpha=1, 2, \cdots)$ suitably so that $K'^{(\alpha)}Q_{ab} \cap K'^{(\beta)}Q_{ab}=Q_{ab}$ and $K'^{(\alpha)}M_0 \cap K'^{(\beta)}M_0=M_0$ holds if $\alpha \neq \beta$.

4.1. Preliminaries for proving Theorem 3

In this subsection, we shall show that we can choose n_1 and n_2 suitably so that $K'^{(1)}Q_{ab} \cap K'^{(2)}Q_{ab}=Q_{ab}$ and $K'^{(1)}M_0 \cap K'^{(2)}M_0=M_0$ holds (Proposition 3).

For each $\alpha \geq 1$, let $K_p^{(\alpha)}$ (resp. $K_p'^{(\alpha)}$) denote the field obtained by adjoining to Q all coordinates (resp. the "x-coordinates") of the p-division points on E_{j_α}. The field $K_p'^{(\alpha)}$ is nothing but the field $K'^{(\alpha)}$ in the case that $r=1$. Let k_α denote the subextension of $K_p^{(\alpha)}$ over Q corresponding to the center F_p^* of $\mathrm{GL}_2(F_p) \simeq \mathrm{Gal}(K_p^{(\alpha)}/Q)$. (See the proof of Proposition 2.)

LEMMA 7. *Let* l *be a good prime of* E_{j_1}*, and*

$$x^2-a_lx+l \quad (a_l \in Z)$$

be the characteristic polynomial of the l*-th power Frobenius endomorphism of the reduction of* E_{j_1} *at* l*. Assume that* $a_l \equiv 0 \bmod p$*. Then, the residue extension degree of* l *in* k_1/Q *is at most* 2.

PROOF. Let $\mathfrak{l}$ be any prime divisor of $K_p^{(1)}$ lying above l, and $\sigma_\mathfrak{l}$ denote the Frobenius automorphism of $\mathfrak{l}$. Then,

$$\rho_p(\sigma_\mathfrak{l})^2+l \cdot 1_2=0 \quad \text{in } \mathrm{GL}_2(F_p) \simeq \mathrm{Gal}(K_p^{(1)}/Q),$$

where ρ_p is as before. (See the proof of Proposition 2.) Therefore, $\rho_p(\sigma_\mathfrak{l})^2 \in F_p^*$. This means that $\sigma_\mathfrak{l}^2$ is the identity on k_1. From this the lemma follows at once.

LEMMA 8. *There exist infinitely many prime numbers l satisfying the following conditions*:

(i) *The residue extension degree of l in k_1/Q is neither one nor two.*

(ii) *The prime l remains prime in $Q(\sqrt{-11})$ and $Q(\sqrt{-2})$.*

(iii) *$l\equiv 3 \bmod 4$, i.e., l remains prime in $Q(\sqrt{-1})$.*

PROOF. First, assume that $p\neq 11$. Let L be the composite of the fields $Q(\sqrt{-11})$, $Q(\sqrt{-2})$, $Q(\sqrt{-1})$, and k_1. Since $Q(\sqrt{\pm p})$ ($\pm p\equiv 1 \bmod 4$) is the maximum abelian subextension of k_1 over Q, L/Q is a Galois extension such that $\mathrm{Gal}(L/Q)\simeq Z/2Z\times Z/2Z\times Z/2Z\times \mathrm{GL}_2(F_p)/F_p^*$. Let N_1, N_2, N_3 and N_4 be the normal subgroups of $\mathrm{Gal}(L/Q)$ corresponding to the fields $Q(\sqrt{-11})$, $Q(\sqrt{-2})$, $Q(\sqrt{-1})$, and k_1 respectively. Then, it is easy to see that there exists an element σ of $\mathrm{Gal}(L/Q)$ such that $\sigma\notin N_i$ ($1\leq i\leq 3$) and $\sigma^2\notin N_4$. Let C be the conjugacy class of σ in $\mathrm{Gal}(L/Q)$. Then, by Čebotarev's density theorem, there exist infinitely many prime numbers (in fact, with positive density) whose Frobenius automorphisms (up to conjugacy) belong to C. These primes satisfy the conditions (i), (ii), and (iii). In the case of $p=11$, the lemma is proved similarly.

LEMMA 9. *Let $l\geq 13$ be a good prime of E_{j_1} satisfying the conditions* (i), (ii), *and* (iii) *of Lemma* 8. *Let n_1 and n_2 be positive integers satisfying the condition* (C) *in* § 3. *Choose n_2 such that $(l-1)/2 \mid n_2$. (This is possible, for $l\equiv 3 \bmod 4$.) Then, $K_p^{(1)}\cap K_p^{(2)}=Q(\zeta_p)$.*

PROOF. We first show that the residue extension degree of l in k_2/Q is at most 2. Consider the reduction of E_{j_2} at l. By the assumption that $(l-1)/2 \mid n_2$, $(\varepsilon p)^{n_2}\equiv \pm 1 \bmod l$. So, we get $j_2=j(n_2)\equiv -2^{15}$ or $20^3 \bmod l$. As $l\geq 13$, $j_2\neq 0$, $12^3 \bmod l$, so that l is a good prime of E_{j_2}. It is known that -2^{15} (resp. 20^3) is the modular invariant of the elliptic curve with complex multiplication whose endomorphism ring is isomorphic to the integer ring of $Q(\sqrt{-11})$ (resp. $Q(\sqrt{-2})$ (cf. e. g. Fricke [5] p. 396, 443). By this and the condition (ii), the reduction of E_{j_2} at l is a supersingular elliptic curve (cf. e. g. Lang [8] Ch. 13 § 2). Therefore, the characteristic polynomial of the l-th power Frobenius endomorphism of the reduction of E_{j_2} at l is x^2+l (cf. e. g. Lang [8] Ch. 13 § 2). Hence, by Lemma 7, the residue extension degree of l in k_2/Q is at most 2.

Now, assume that the lemma does not hold, i. e., $K_p^{(1)}\cap K_p^{(2)}\supsetneq Q(\zeta_p)$. The field $K_p^{(1)}\cap K_p^{(2)}$ is a Galois extension of $Q(\zeta_p)$, and $\mathrm{Gal}(K_p^{(\alpha)}/Q(\zeta_p))\simeq \mathrm{SL}_2(F_p)$ ($\alpha=1, 2$). Since $\{\pm 1\}$ is the unique non-trivial normal subgroup of $\mathrm{SL}_2(F_p)$,

it follows that $K_p'^{(1)}=K_p'^{(2)}$ and $k_1=k_2$. This is a contradiction, for the residue extension degrees of l in k_1/Q and k_2/Q are different. Therefore, $K_p^{(1)}\cap K_p^{(2)}=Q(\zeta_p)$.

PROPOSITION 3. *Let l, n_1, and n_2 be as in Lemma 9. Then, $K'^{(1)}Q_{ab}\cap K'^{(2)}Q_{ab}=Q_{ab}$ and $K'^{(1)}M_0\cap K'^{(2)}M_0=M_0$.*

PROOF. Let $K_\infty^{(\alpha)}$ denote the field obtained by adjoining to Q all coordinates of the points of p-power order on E_{j_α} $(\alpha=1, 2)$. Then, it suffices to show that $K_\infty^{(1)}Q_{ab}\cap K_\infty^{(2)}Q_{ab}=Q_{ab}$ and $K_\infty^{(1)}M_0\cap K_\infty^{(2)}M_0=M_0$, namely, the canonical injections

$$\mathrm{Gal}(K_\infty^{(1)}K_\infty^{(2)}Q_{ab}/Q_{ab})\longrightarrow\mathrm{Gal}(K_\infty^{(1)}Q_{ab}/Q_{ab})\times\mathrm{Gal}(K_\infty^{(2)}Q_{ab}/Q_{ab})$$

and

$$\mathrm{Gal}(K_\infty^{(1)}K_\infty^{(2)}M_0/M_0)\longrightarrow\mathrm{Gal}(K_\infty^{(1)}M_0/M_0)\times\mathrm{Gal}(K_\infty^{(2)}M_0/M_0)$$

are both surjective. The groups $\mathrm{Gal}(K_\infty^{(\alpha)}Q_{ab}/Q_{ab})$ and $\mathrm{Gal}(K_\infty^{(\alpha)}M_0/M_0)$ $(\alpha=1, 2)$ are all isomorphic to $\mathrm{SL}_2(Z_p)$. (See the proof of Proposition 2 and 3.2.) Therefore, by Lemma 10 of Serre [15], it suffices to verify that $\mathrm{Gal}(K_p^{(1)}K_p^{(2)}Q_{ab}/Q_{ab})\simeq\mathrm{SL}_2(F_p)\times\mathrm{SL}_2(F_p)$ and $\mathrm{Gal}(K_p^{(1)}K_p^{(2)}M_0/M_0)\simeq\mathrm{SL}_2(F_p)\times\mathrm{SL}_2(F_p)$.

By Lemma 9, $\mathrm{Gal}(K_p^{(1)}K_p^{(2)}/Q(\zeta_p))\simeq\mathrm{SL}_2(F_p)\times\mathrm{SL}_2(F_p)$. Since the abelianized group of $\mathrm{SL}_2(F_p)\times\mathrm{SL}_2(F_p)$ is trivial, $\mathrm{Gal}(K_p^{(1)}K_p^{(2)}Q_{ab}/Q_{ab})\simeq\mathrm{SL}_2(F_p)\times\mathrm{SL}_2(F_p)$. Let N be the normal subgroup of $\mathrm{SL}_2(F_p)\times\mathrm{SL}_2(F_p)$ corresponding to the Galois subextension $K_p^{(1)}K_p^{(2)}Q_{ab}\cap M_0$ of $K_p^{(1)}K_p^{(2)}Q_{ab}$ over Q_{ab}. By Lemma 6, N satisfies the condition of Lemma 10 below. Thus, $N=\mathrm{SL}_2(F_p)\times\mathrm{SL}_2(F_p)$, so that $K_p^{(1)}K_p^{(2)}Q_{ab}\cap M_0=Q_{ab}$. Therefore, $\mathrm{Gal}(K_p^{(1)}K_p^{(2)}M_0/M_0)\simeq\mathrm{SL}_2(F_p)\times\mathrm{SL}_2(F_p)$, and the proof is completed.

LEMMA 10. *Let N be a normal subgroup of $\mathrm{SL}_2(F_p)\times\mathrm{SL}_2(F_p)$ which is contained neither in $\{\pm1\}\times\mathrm{SL}_2(F_p)$ nor in $\mathrm{SL}_2(F_p)\times\{\pm1\}$. Then, $N=\mathrm{SL}_2(F_p)\times\mathrm{SL}_2(F_p)$.*

PROOF. First, let $\overline{N}$ be the image of N under the canonical projection from $\mathrm{SL}_2(F_p)\times\mathrm{SL}_2(F_p)$ to $\mathrm{PSL}_2(F_p)\times\mathrm{PSL}_2(F_p)$. By the assumption on N and the well-known fact that $\mathrm{PSL}_2(F_p)$ is a simple group, it follows easily that either $\overline{N}=\mathrm{PSL}_2(F_p)\times\mathrm{PSL}_2(F_p)$ or the projections to the first and the second components (of $\mathrm{PSL}_2(F_p)\times\mathrm{PSL}_2(F_p)$) are both bijective on $\overline{N}$. But the latter is impossible. In fact, assume that the latter occurs. Choose an element $(\sigma_1, \sigma_2)\in\overline{N}$ such that $\sigma_1\neq1$. Then, $(\tau, \sigma_2)(\sigma_1, \sigma_2)(\tau, \sigma_2)^{-1}$

$=(\tau\sigma_1\tau^{-1}, \sigma_2) \in \bar{N}$ for any $\tau \in \mathrm{PSL}_2(F_p)$. Hence, by the bijectivity of the projection to the second component, $\tau\sigma_1\tau^{-1}=\sigma_1$ for any $\tau \in \mathrm{PSL}_2(F_p)$. Therefore, σ_1 is contained in the center of $\mathrm{PSL}_2(F_p)$, a contradiction. So, $\bar{N}=\mathrm{PSL}_2(F_p)\times\mathrm{PSL}_2(F_p)$. Then, $\mathrm{SL}_2(F_p)\times\mathrm{SL}_2(F_p)=N\cdot\{\pm 1\}\times\{\pm 1\}$. In particular, $\mathrm{SL}_2(F_p)\times\mathrm{SL}_2(F_p)/N$ is abelian. Since the abelianized group of $\mathrm{SL}_2(F_p)\times\mathrm{SL}_2(F_p)$ is trivial, $N=\mathrm{SL}_2(F_p)\times\mathrm{SL}_2(F_p)$.

4.2. Proof of Theorem 3

We determine a sequence of positive integers n_α $(\alpha=1, 2, \cdots)$ in the following manner. First, let n_1 be any positive integer satisfying the condition (C) in § 3. Let $l_1 \geq 13$ be a good prime of E_{j_1} satisfying the conditions in Lemma 8. Let n_2 be a positive integer satisfying the condition (C) in § 3 and $(l_1-1)/2 \mid n_2$. Suppose that $n_1, \cdots, n_\alpha$ and $l_1, \cdots, l_{\alpha-1}$ have been already chosen. Then, let $l_\alpha \geq 13$ be a good prime of E_{j_α} satisfying the conditions in Lemma 8. (The field k_1 in condition (i) should be replaced by k_α.) Let $n_{\alpha+1}$ be a positive integer satisfying the condition (C) in § 3 and

$$\frac{l_1-1}{2}\,\frac{l_2-1}{2}\cdots\frac{l_\alpha-1}{2} \,\Big|\, n_{\alpha+1}.$$

Then, by Proposition 3, $K'^{(\alpha)}Q_{ab} \cap K'^{(\beta)}Q_{ab}=Q_{ab}$ and $K'^{(\alpha)}M_0 \cap K'^{(\beta)}M_0=M_0$ $(\alpha \neq \beta)$. Thus, $K'^{(\alpha)}Q_{ab}$ $(\alpha=1, 2, \cdots)$ (resp. $K'^{(\alpha)}M_0$ $(\alpha=1, 2, \cdots)$) is a sequence of infinitely many lineary independent Galois extensions of Q_{ab} (resp. M_0) contained in M having $\mathrm{PSL}_2(Z/p^rZ)$ as the Galois group over Q_{ab} (resp. M_0). This completes the proof of Theorem 3.

§ 5. Remarks

5.1. Let γ be any element of $\mathrm{Gal}(M_0/M^t)$ and $\tilde{\gamma}$ be any extension of γ to M. Then, if F is a subextension of M over M_0, $\tilde{\gamma}(F)$ is also a subextension of M over M_0, possibly $\tilde{\gamma}(F) \neq F$. But the subextensions $K'^{(\alpha)}M_0$ $(\alpha=1, 2, \cdots)$ of M over M_0 we have constructed in (the proof of) Theorem 3 are Galois extensions over M_0 (in fact, Galois over Q). Therefore, $\tilde{\gamma}(K'^{(\alpha)}M_0)=K'^{(\alpha)}M_0$ $(\alpha=1, 2, \cdots)$. Thus, we have constructed infinitely many, in a sense, "$\mathrm{Gal}(M_0/M^t)$-independent" Galois subextensions of M over M_0 having $\mathrm{PSL}_2(Z/p^rZ)$ as the Galois group over M_0.

5.2. Let E be an elliptic curve over Q, p be a prime number, and K_{p^∞} denote the field obtained by adjoining to Q all coordinates of the points

of p-power order on E. In our previous paper [1], we have shown that $K_{p^\infty}F_{ab}/F_{ab}$ is unramified if E has good and supersingular reduction at p, under some additional conditions. Here, F is a certain algebraic number field of finite degree over $\boldsymbol{Q}$. If E does not have complex multiplication, it is known that $\mathrm{Gal}(K_{p^\infty}/\boldsymbol{Q})$ is isomorphic to an open subgroup of $\mathrm{GL}_2(\boldsymbol{Z}_p)$ (Serre [14]). Especially, $K_{p^\infty}F_{ab}/F_{ab}$ is an infinite extension (cf. Supplement). But we can not take $F=\boldsymbol{Q}$ ([1] § 4). In this paper, we can take the field $F=\boldsymbol{Q}$ by using a prime p such that $E\underset{\boldsymbol{Q}}{\otimes}\boldsymbol{Q}_p$ is isomorphic to a Tate curve over $\boldsymbol{Q}_p$.

Supplement

Here, we shall give an explicit example of an unramified Galois extension over an abelian extension of an algebraic number field of finite degree over $\boldsymbol{Q}$, by using the points of p-power order on an elliptic curve, where p is a "supersingular" prime. This is an example of our previous result ([1] § 4).

Let E be the following elliptic curve defined over $k=\boldsymbol{Q}(\sqrt{29})$;

$$E:\ y^2+xy+\varepsilon^2 y=x^3,\quad j=(24\,\varepsilon^2-1)^3\varepsilon^{-10},$$

where $\varepsilon=\dfrac{5+\sqrt{29}}{2}$ is a fundamental unit of k. Then, E has everywhere good reduction over k (an example of Tate cf. Serre [15] 5.10). Let F be the quadratic number field $\boldsymbol{Q}(\sqrt{-1})$ and $p=71$. For each integer $n\geq 1$, let F_n be the ray class field of F with conductor $(p)^n\mathfrak{l}^3$, where (p) and $\mathfrak{l}=(1+\sqrt{-1})$ are prime ideals of F. Let K_n be the composite of F_n and Fk. Let L_n be the field obtained by adjoining to K_n all coordinates of the p^n-division points on E. Put $K_\infty=\bigcup_{n=1}^{\infty}K_n$ and $L_\infty=\bigcup_{n=1}^{\infty}L_n$. Then, we can show the following

PROPOSITION. *The field L_n is an unramified Galois extension of K_n having $\mathrm{SL}_2(\boldsymbol{Z}/p^n\boldsymbol{Z})$ as the Galois group over K_n. The field L_∞ is an unramified Galois extension of K_∞ having $\mathrm{SL}_2(\boldsymbol{Z}_p)$ as the Galois group over K_∞.*

PROOF. As E has everywhere good reduction over k, hence over K_n, every prime ideal of K_n which is prime to p is unramified in L_n. We shall show that every prime ideal $\mathfrak{P}$ of K_n lying above p is unramified in

L_n, so that the extensions L_n/K_n and L_∞/K_∞ are unramified. It is enough to show that $(L_n)_\mathfrak{P}=(K_n)_\mathfrak{P}$ holds. (For a subfield K of L_n, $K_\mathfrak{P}$ denotes the $\mathfrak{P}$-completion of K.)

First, as p splits completely in k and remains prime in F, $(Fk)_\mathfrak{P}=F_\mathfrak{P}=\boldsymbol{Q}_{p^2}$, the unique unramified quadratic extension of $\boldsymbol{Q}_p$. Therefore, $(K_n)_\mathfrak{P}=(F_n)_\mathfrak{P}F_\mathfrak{P}$, and it is easily verified that the abelian extension $(F_n)_\mathfrak{P}F_\mathfrak{P}/F_\mathfrak{P}$ corresponds to the subgroup $(-p)^Z\times U^{(n)}$ of $F_\mathfrak{P}^*$ by local classfield theory. Here, $(-p)^Z$ denotes the infinite cyclic group generated by $-p$ and

$$U^{(n)}=\{a\in F_\mathfrak{P}^* \mid \quad a\equiv 1 \mod (p)^n\}.$$

On the other hand, let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ be the two prime ideals of k lying above p. Then, by simple calculations, we get $\{j \bmod \mathfrak{p}_1, j \bmod \mathfrak{p}_2\}=\{0, 66\}$, so that $E \bmod \mathfrak{p}_1$ and $E \bmod \mathfrak{p}_2$ are both supersingular elliptic curves over $\boldsymbol{F}_p$ (Deuring [4] p. 258). Therefore, by a result of Honda ([6] 2, 5, See also [1] § 4) the formal groups associated to $E\underset{k}{\otimes}k_{\mathfrak{p}_1}$ and $E\underset{k}{\otimes}k_{\mathfrak{p}_2}$ have formal complex multiplication. More precisely, it is easily verified that their special elements are both $p+T^2$, so that they are both isomorphic (over $\boldsymbol{Z}_{p^2}$) to the Lubin-Tate group over $\boldsymbol{Z}_{p^2}$ associated to the prime element $-p$ of $\boldsymbol{Z}_{p^2}$. Here, $\boldsymbol{Z}_{p^2}$ denotes the integer ring of $\boldsymbol{Q}_{p^2}$. Therefore, by a result of Lubin-Tate [9], $(L_n)_\mathfrak{P}/F_\mathfrak{P}$ corresponds to the subgroup $(-p)^Z\times U^{(n)}$ of $F_\mathfrak{P}^*$. Hence, $(L_n)_\mathfrak{P}=(K_n)_\mathfrak{P}$.

It is known that $\mathrm{Gal}(k(E_p)/k)\simeq \mathrm{GL}_2(\boldsymbol{F}_p)$, where $k(E_p)$ denotes the field obtained by adjoining to k all coordinates of the p-division points on E (Serre [15] 5.10). Since K_n contains ζ_{p^n}, it follows that $\mathrm{Gal}(L_n/K_n)\simeq \mathrm{SL}_2(\boldsymbol{Z}/p^n\boldsymbol{Z})$ and $\mathrm{Gal}(L_\infty/K_\infty)\simeq\mathrm{SL}_2(\boldsymbol{Z}_p)$ by Lemma 3, and the proof of Proposition is completed.

References

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

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

[3] Cornell, G., Abhyanker's lemma and the class group, Lecture Notes in Math. Vol. 751, Springer Verlag, Berlin-Heidelberg-New York, 1979, 82-88.

[4] Deuring, M., Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Univ. Hamburg **14** (1941), 197-272.

[5] Fricke, R., Lehrbuch der Algebra Bd. III, Fried. Vieweg and Sohn, Braunschweig, 1928.

[6] Honda, T., On the theory of commutative formal groups, J. Math. Soc. Japan **22-2** (1970), 213-246.

[7] Igusa, J., Fibre systems of Jacobian varieties III, Amer. J. Math. **81** (1959), 453-476.

[8] Lang, S., Elliptic functions, Addison Wesley, Reading, Mass., 1970.
[9] Lubin, J. and J. Tate, Formal complex multiplication in local fields, Ann. of Math. **81** (1965), 380-387.
[10] Mazur, B., Rational points on modular curves, Lecture Notes in Math. Vol. 601, Springer Verlag, Berlin-Heidelberg-New York, 1977, 107-148.
[11] Mazur, B., Rational isogenies of prime degree, Invent. Math. **44** (1978), 129-162.
[12] Momose, F., Rational points on the modular curves $X_{\mathrm{split}}(p)$, Compositio Math. **52** (1984), 115-137.
[13] Ogg, A., Elliptic curves and wild ramification, Amer. J. Math. **89** (1967), 1-21.
[14] Serre, J.-P., Abelian l-adic Representations and Elliptic Curves, Benjamin, New York, 1968.
[15] Serre, J.-P., Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. **15** (1972), 259-331.
[16] Serre, J.-P. and J. Tate, Good reduction of abelian varieties, Ann. of Math. **88** (1968), 492-517.
[17] Tate, J., The arithmetic of elliptic curves, Invent. Math. **23** (1974), 179-206.
[18] Uchida, K., Galois groups of unramified solvable extensions, Tôhoku Math. J. (2) **34** (1982), 311-317.

(Received February 26, 1985)

Department of Mathematics
Faculty of Science
University of Tokyo
Hongo, Tokyo
113 Japan