J. Math. Soc. Japan
Vol. 35, No. 2, 1983

The 2-adic representations attached to elliptic curves defined over Q whose points of order 2 are all Q-rational

By Kumiko NISHIOKA

(Received July 10, 1980)
(Revised Dec. 3, 1981)

0. Introduction.

Let E be an elliptic curve defined over the field $\boldsymbol{Q}$ of rational numbers. Throughout the paper, an elliptic curve defined over $\boldsymbol{Q}$ means an abelian variety of dimension one which is defined over $\boldsymbol{Q}$. Let G be the Galois group of extension $\bar{\boldsymbol{Q}}/\boldsymbol{Q}$, where $\bar{\boldsymbol{Q}}$ denotes an algebraic closure of $\boldsymbol{Q}$. Then the group G, with the Krull topology, is compact and totally disconnected. For each positive integer m, we denote by E_m the kernel of multiplication by m. Let p be a prime number. With the multiplication by $p: E_{p^{n+1}} \to E_{p^n}$, the sequence $\{E_{p^n}\}_{n=1,2,\dots}$ forms a projective system. The Tate module $T_p(E)$ is defined as follows:

$$T_p(E) = \operatorname{proj}\lim_{n\to\infty} E_{p^n}\,.$$

The module $T_p(E)$ is a free $\boldsymbol{Z}_p$-module of rank 2, where $\boldsymbol{Z}_p$ denotes a p-adic completion of the ring $\boldsymbol{Z}$ of rational integers, and G acts on $T_p(E)$. Fix a base (ξ_0, ξ_1) of $T_p(E)$ over $\boldsymbol{Z}_p$. If σ is an element of G, then there exists a unique element $\pi_p(\sigma)$ of $GL_2(\boldsymbol{Z}_p)$ such that

$$(\sigma\xi_0, \sigma\xi_1) = (\xi_0, \xi_1)\pi_p(\sigma)\,.$$

The mapping $\pi \to \pi_p(\sigma)$, which will be denoted by π_p, is a continuous representation $G \to GL_2(\boldsymbol{Z}_p)$.

Serre [7] proved that if E has no complex multiplication, then the image group $\pi_p(G)$ is an open subgroup of $GL_2(\boldsymbol{Z}_p)$. He also states that if E is semistable and $p \geqq 11$, then the Galois group $\mathrm{Gal}(\boldsymbol{Q}(E_p)/\boldsymbol{Q})$ is isomorphic to $GL_2(\boldsymbol{Z}/p\boldsymbol{Z})$ (Theorem 5 in [8]), and therefore $\pi_p(G) = GL_2(\boldsymbol{Z}_p)$. Put

$$H^{(n)} = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\boldsymbol{Z}_p) \,\middle|\, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod p^n \right\}.$$

This research was partially supported by Grant-in-Aid for Scientific Research (No. 57540029), Ministry of Education.

Then $\{H^{(n)}\}_{n=0,1,\dots}$ is a fundamental system of neighbourhoods of unity in $GL_2(\boldsymbol{Z}_p)$. Therefore $\pi_p(G)\supset H^{(N)}$, where N is a non-negative integer depending on E and p. Especially if E is semi-stable and $p\geqq 11$, then we can take $N=0$.

In this paper we shall consider the case $p=2$ and prove:

THEOREM 1. *Let the notations be as above. Assume that E has no complex multiplication, and the points of order* 2 *of E are all* $\boldsymbol{Q}$*-rational. Then*

$$\pi_2(G)\supset H^{(7)}.$$

THEOREM 2. *Assume that E satisfies the conditions of Theorem* 1 *and moreover E has a* $\boldsymbol{Q}$*-rational point of order* 8. *Then*

$$\pi_2(G)=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in H^{(1)}\,\middle|\,\begin{pmatrix} a & b \\ c & d \end{pmatrix}\equiv\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \bmod 2^3\right\},$$

with a suitable $\boldsymbol{Z}_2$*-base of* $T_2(E)$. *Especially* $\pi_2(G)\supset H^{(3)}$.

Our Theorem 1 asserts that for $p=2$, we can take $N=7$ independently of E under the hypothesis of Theorem 1, and Theorem 2 asserts that the conjugate class of $\pi_2(G)$ is uniquely determined under the hypothesis of Theorem 2.

The paper is divided into 3 parts as follows. Chapter 1 contains a number of preliminary lemmas. Theorem 1 and Theorem 2 are proved in Chapter 2 and Chapter 3 respectively.

1. Preliminary lemmas.

Let k be a field, the characteristic of k be not 2, and K be a field extension of k which is algebraically closed. Let E be the curve defined by:

$$Y^2Z=X^3+AXZ^2+BZ^3, \qquad A,\ B\in k,\ 4A^3+27B^2\neq 0, \tag{1.1}$$

in 2-dimensional projective space $P^2(K)$. Then E has the structure of an abelian variety with $(X, Y, Z)=(0, 1, 0)$ as zero element. We denote this curve in the affine form:

$$Y^2=X^3+AX+B, \tag{1.2}$$

and denote $(0, 1, 0)$ by (∞, ∞). Then the addition formulas are expressed as follows (cf. Cassels [2]). If $(X_1, Y_1)+(X_2, Y_2)=(X_3, Y_3)$, then

$$\begin{cases} X_3=-X_2-X_1+\left(\dfrac{Y_2-Y_1}{X_2-X_1}\right)^2, \\ Y_3=-\left(\dfrac{Y_1-Y_2}{X_1-X_2}\right)X_3-\dfrac{X_2Y_1-X_1Y_2}{X_2-X_1}. \end{cases} \tag{1.3}$$

If $2(X_1, Y_1)=(X_3, Y_3)$, then

$$\begin{cases} X_3=-2X_1+\left(\dfrac{3X_1^2+A}{2Y_1}\right)^2, \\ Y_3=-\left(\dfrac{3X_1^2+A}{2Y_1}\right)(X_3-X_1)-Y_1. \end{cases} \tag{1.4}$$

The points of order 2 are $(e_0, 0)$, $(e_1, 0)$ and $(e_2, 0)$, where $X^3+AX+B=(X-e_0)\cdot(X-e_1)(X-e_2)$. Let (x_0, y_0) be a point on E, and (x_1, y_1) be a 2-divisional point of (x_0, y_0). Put

$$\begin{cases} (x_2, y_2)=(x_1, y_1)+(e_0, 0), \\ (x_3, y_3)=(x_1, y_1)+(e_1, 0), \\ (x_4, y_4)=(x_1, y_1)+(e_2, 0). \end{cases} \tag{1.5}$$

Then these three points and (x_1, y_1) are the 2-divisional points of (x_0, y_0). From (1.4) we have

$$x_0=-2x_i+\left(\frac{3x_i^2+A}{2y_i}\right)^2=-2x_i+\frac{(3x_i^2+A)^2}{4(x_i^3+Ax_i+B)} \qquad (i=1, 2, 3, 4)$$

and x_1, x_2, x_3, x_4 are the four roots of

$$X^4-4x_0X^3-2AX^2-(4Ax_0-8B)X+(A^2-4Bx_0)=0. \tag{1.6}$$

Since x_1 is a root of this equation and $y_1^2=x_1^3+Ax_1+B$, we get

$$x_0-e_i=\left(\frac{x_1^2-2e_ix_1-A-2e_i^2}{2y_1}\right)^2 \qquad (i=0, 1, 2). \tag{1.7}$$

Put

$$\begin{cases} 4w_0=(x_1+x_2)-(x_3+x_4), \\ 4w_1=(x_1+x_3)-(x_2+x_4), \\ 4w_2=(x_1+x_4)-(x_2+x_3). \end{cases} \tag{1.8}$$

From (1.3) and (1.5), we have

$$\begin{cases} x_2=-x_1-e_0+\left(\dfrac{y_1}{x_1-e_0}\right)^2=-x_1-e_0+\dfrac{(x_1-e_1)(x_1-e_2)}{x_1-e_0}, \\ x_3=-x_1-e_1+\left(\dfrac{y_1}{x_1-e_1}\right)^2=-x_1-e_1+\dfrac{(x_1-e_0)(x_1-e_2)}{x_1-e_1}, \\ x_4=-x_1-e_2+\left(\dfrac{y_1}{x_1-e_2}\right)^2=-x_1-e_2+\dfrac{(x_1-e_0)(x_1-e_1)}{x_1-e_2}. \end{cases} \tag{1.9}$$

Substituting (1.9) to (1.8) and noting $y_1^2=(x_1-e_0)(x_1-e_1)(x_1-e_2)$, we have

$$\begin{cases} w_0=\left(\dfrac{x_1^2-2e_1x_1-A-2e_1^2}{2y_1}\right)\left(\dfrac{x_1^2-2e_2x_1-A-2e_2^2}{2y_1}\right), \\ w_1=\left(\dfrac{x_1^2-2e_2x_1-A-2e_2^2}{2y_1}\right)\left(\dfrac{x_1^2-2e_0x_1-A-2e_0^2}{2y_1}\right), \\ w_2=\left(\dfrac{x_1^2-2e_0x_1-A-2e_0^2}{2y_1}\right)\left(\dfrac{x_1^2-2e_1x_1-A-2e_1^2}{2y_1}\right). \end{cases} \tag{1.10}$$

Comparing (1.7) and (1.10), we get

$$\begin{cases} w_0^2=(x_0-e_1)(x_0-e_2), \\ w_1^2=(x_0-e_2)(x_0-e_0), \\ w_2^2=(x_0-e_0)(x_0-e_1), \\ w_0w_1w_2=(x_0-e_0)(x_0-e_1)(x_0-e_2). \end{cases} \tag{1.11}$$

Since x_1, x_2, x_3, x_4 are the four roots of (1.6), we have $x_1+x_2+x_3+x_4=4x_0$. From this and (1.8),

$$\begin{cases} x_1=x_0+w_0+w_1+w_2, \\ x_2=x_0+w_0-w_1-w_2, \\ x_3=x_0-w_0+w_1-w_2, \\ x_4=x_0-w_0-w_1+w_2. \end{cases} \tag{1.12}$$

From (1.5) and (1.8), we have

LEMMA 1. *Let the notations be as above, and* $e_i\in k$ $(i=0, 1, 2)$. *Suppose that there exists an automorphism* σ *of* K *over* k *such that*

$$(x_1^\sigma, y_1^\sigma)=(x_1, y_1)+(e_i, 0).$$

Then $w_i^\sigma=w_i$ *and* $w_j^\sigma=-w_j$ *for* $j\neq i$.

Let p be a prime number. For any positive integer h, r_h denotes the canonical homomorphism of $GL_2(\boldsymbol{Z}_p)$ to $GL_2(\boldsymbol{Z}/p^h\boldsymbol{Z})$. Let n be a positive integer. For any integer h such that $1\leqq h\leqq n$, $r_{n,h}$ denotes the canonical homomorphism of $GL_2(\boldsymbol{Z}/p^n\boldsymbol{Z})$ to $GL_2(\boldsymbol{Z}/p^h\boldsymbol{Z})$. For any integer h such that $0\leqq h\leqq n$, we define

$$H_n^{(h)}=\left\{\begin{pmatrix} a & b \\ c & d\end{pmatrix}\in GL_2(\boldsymbol{Z}/p^n\boldsymbol{Z})\,\middle|\,\begin{pmatrix} a & b \\ c & d\end{pmatrix}\equiv\begin{pmatrix} 1 & 0 \\ 0 & 1\end{pmatrix} \bmod p^h\right\}.$$

Then we have obviously the following lemma.

LEMMA 2. *Let* V *be a subgroup of* $GL_2(\boldsymbol{Z}/p^n\boldsymbol{Z})$. *Then*

$$|V|=\prod_{h=1}^{n}|r_{n,h}(V)\cap H_h^{(h-1)}|.$$

Let $2 \leqq h \leqq n-2$, and $\sigma \in H_h^{(h)}$. Then there exist elements a, b, c and d of $\boldsymbol{Z}/p^n\boldsymbol{Z}$ such that

$$\sigma \equiv \begin{pmatrix} 1+ap^h & bp^h \\ cp^h & 1+dp^h \end{pmatrix} \bmod p^{h+1}.$$

Then

$$\sigma^p \equiv \begin{pmatrix} 1+ap^{h+1} & bp^{h+1} \\ cp^{h+1} & 1+dp^{h+1} \end{pmatrix} \bmod p^{h+2}.$$

Hence we have:

LEMMA 3. *Let* $2 \leqq h \leqq n-1$.

(1) *If a subgroup* V *of* $GL_2(\boldsymbol{Z}/p^n\boldsymbol{Z})$ *satisfies* $r_{n,h+1}(V) \supset H_{h+1}^{(h)}$, *then* $V \supset H_n^{(h)}$.

(2) *If a subgroup* V *of* $SL_2(\boldsymbol{Z}/p^n\boldsymbol{Z})$ *satisfies* $r_{n,h+1}(V) \supset H_{h+1}^{(h)} \cap SL_2(\boldsymbol{Z}/p^{h+1}\boldsymbol{Z})$, *then* $V \supset H_n^{(h)} \cap SL_2(\boldsymbol{Z}/p^n\boldsymbol{Z})$.

LEMMA 4. *Let* A *be a closed subgroup of* $GL_2(\boldsymbol{Z}_p)$ *and* h *be an integer such that* $h \geqq 2$. *If* $r_{h+1}(A) \supset H_{h+1}^{(h)}$, *then* $A \supset H^{(h)}$.

PROOF. Since A and $H^{(h)}$ are closed, it is sufficient to show that $A \cap H^{(h)}$ is dense in $H^{(h)}$. Since $r_{h+1}(A) \supset H_{h+1}^{(h)}$,

$$r_{h+1}(A \cap H^{(h)}) \supset H_{h+1}^{(h)}.$$

Let n be any integer with $n > h$. Then by Lemma 3,

$$r_n(A \cap H^{(h)}) \supset H_n^{(h)}.$$

This shows that $A \cap H^{(h)}$ is dense in $H^{(h)}$.

In the rest of this paper, we consider the case $p=2$.

LEMMA 5. *Let* V *be a subgroup of* $SL_2(\boldsymbol{Z}/2^6\boldsymbol{Z})$. *Suppose that* V *includes* $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *and* $\tau = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$ *such that*

$$a \equiv d \equiv 1, \quad b \equiv 2 \bmod 2^2, \quad c \equiv 0 \bmod 2^3, \tag{1.13}$$

$$\begin{pmatrix} e & f \\ g & h \end{pmatrix} \equiv \begin{pmatrix} 1+4 & 0 \\ 8 & 1-4 \end{pmatrix} \bmod 2^4. \tag{1.14}$$

Then $V \supset SL_2(\boldsymbol{Z}/2^6\boldsymbol{Z}) \cap H_6^{(5)}$.

PROOF. Without loss of generality we may assume

$$c=0, \qquad b=2, \qquad f=0. \tag{1.15}$$

In fact by (1.13) $c \equiv 0$ or $8 \bmod 2^4$. In the latter case we may assume $c \equiv 0 \bmod 2^4$ by adopting $\tau\sigma$ for σ. Then $c \equiv 0$ or $16 \bmod 2^5$. In the latter case we may assume $c \equiv 0 \bmod 2^5$ by adopting $\tau^2\sigma$ for σ. Then $c=0$ or 32. If $c=32$, then we adopt $\tau^4\sigma$ for σ. Consequently we may assume $c=0$. By the same process we see that $(\sigma^2)^m\sigma=\begin{pmatrix} * & 2 \\ 0 & * \end{pmatrix}$ and $(\sigma^8)^n\tau=\begin{pmatrix} * & 0 \\ * & * \end{pmatrix}$ for some integers m and n. $(\sigma^2)^m\sigma$ and $(\sigma^8)^n\tau$ satisfy (1.13) and (1.14) respectively, because $\sigma^2\equiv\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 2^2$ and $\sigma^8\equiv\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 2^4$. Hence we may assume (1.15). We can put $\sigma=\begin{pmatrix} a & 2 \\ 0 & a^{-1} \end{pmatrix}$, and $\tau=\begin{pmatrix} e & 0 \\ 8+16i & e^{-1} \end{pmatrix}$, where $a\equiv a^{-1}\equiv 1 \bmod 2^2$, $e\equiv 1+4$, $e^{-1}\equiv 1-4 \bmod 2^4$ and $i\in \boldsymbol{Z}/2^6\boldsymbol{Z}$. Set $\gamma=\sigma\tau\sigma^{-1}\tau^{-1}$. Then we have

$$\gamma=\begin{pmatrix} v_1 & v_2 \\ v_3 & v_4 \end{pmatrix},$$

where we have set

$$v_1=1+2ae(8+16i)+2a^{-1}e^{-1}(8+16i)(1-a^2),$$

$$v_2=2a(1-e^2)-4(8+16i)e,$$

$$v_3=e^{-1}(8+16i)(a^{-2}-1),$$

$$v_4=1-2a^{-1}e(8+16i).$$

Since a^2, $a^{-2}\equiv 1 \bmod 2^3$ and $e^2\equiv 1-8 \bmod 2^5$, we have

$$\gamma=\begin{pmatrix} 1+16+32i & -16 \\ 0 & 1-16+32i \end{pmatrix}.$$

Since $\sigma^8=\begin{pmatrix} a^8 & 16 \\ 0 & a^{-8} \end{pmatrix}$ and $a^8=a^{-8}=1+32j$, where $j\in \boldsymbol{Z}/2^6\boldsymbol{Z}$, we obtain

$$\sigma^8\gamma=\begin{pmatrix} 1+16+32i+32j & 0 \\ 0 & 1-16+32i+32j \end{pmatrix},$$

and therefore

$$\tau^4\sigma^8\gamma=\begin{pmatrix} 1+32i+32j & 0 \\ 32 & 1+32i+32j \end{pmatrix}.$$

Therefore V includes $\sigma^{16}=\begin{pmatrix} 1 & 32 \\ 0 & 1 \end{pmatrix}$, $\tau^8=\begin{pmatrix} 1+32 & 0 \\ 0 & 1+32 \end{pmatrix}$ and

$$\tau^4\sigma^8\gamma=\begin{pmatrix} 1+32i+32j & 0 \\ 32 & 1+32i+32j \end{pmatrix}.$$

Hence we have

$$V\supset\left\langle\begin{pmatrix} 1 & 0 \\ 32 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 32 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1+32 & 0 \\ 0 & 1+32 \end{pmatrix}\right\rangle=SL_2(\boldsymbol{Z}/2^6\boldsymbol{Z})\cap H_6^{(5)}.$$

LEMMA 6. *Let V be a subgroup of $SL_2(\boldsymbol{Z}/2^6\boldsymbol{Z})$. Suppose that V includes σ and τ such that*

$$\sigma\equiv\begin{pmatrix}1 & 4\\ 0 & 1\end{pmatrix} \quad or \quad \begin{pmatrix}1+4 & 4\\ 0 & 1+4\end{pmatrix} \mod 2^3$$

and

$$\tau\equiv\begin{pmatrix}1 & 0\\ 8 & 1\end{pmatrix} \quad or \quad \begin{pmatrix}1+8 & 0\\ 8 & 1+8\end{pmatrix} \mod 2^4 .$$

Then $V\supset SL_2(\boldsymbol{Z}/2^6\boldsymbol{Z})\cap H_6^{(5)}$.

PROOF. In the same way as in the proof of Lemma 5, we may assume that $\sigma=\begin{pmatrix}a & 4\\ 0 & a^{-1}\end{pmatrix}$, and $\tau=\begin{pmatrix}e & 0\\ 8 & e^{-1}\end{pmatrix}$, where $a\equiv 1 \mod 2^2$ and $e\equiv 1 \mod 2^3$. Then

$$\sigma\tau\sigma^{-1}\tau^{-1}=\begin{pmatrix}1+32a^{-1}e^{-1}+32ae-32ae^{-1} & 4a(1-e^2)\\ 8e^{-1}(a^{-2}-1) & 1-32a^{-1}e\end{pmatrix}.$$

Since $32a^{-1}e^{-1}\equiv 32ae\equiv 32ae^{-1}\equiv 32a^{-1}e\equiv 32 \mod 2^6$, $1-e^2\equiv 0 \mod 2^4$ and $a^{-2}-1\equiv 0 \mod 2^3$, we have

$$\sigma\tau\sigma^{-1}\tau^{-1}=\begin{pmatrix}1+32 & 0\\ 0 & 1+32\end{pmatrix}.$$

From this and the assumption, we have

$$V\supset\left\langle\begin{pmatrix}1 & 0\\ 32 & 1\end{pmatrix}, \begin{pmatrix}1 & 32\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1+32 & 0\\ 0 & 1+32\end{pmatrix}\right\rangle=SL_2(\boldsymbol{Z}/2^6\boldsymbol{Z})\cap H_6^{(5)} .$$

The following lemma is well known (cf. Dickson [3]).

LEMMA 7. *Let $a, b\in\boldsymbol{Q}$.*

(1) *If a and b satisfy one of the following equations:*

$$\pm a^2-b^4=1; \quad -2a^2-b^4=1; \quad \pm a^2-4b^4=1;$$

$$\pm 2a^2-4b^4=1; \quad \pm a^2+4b^4=1; \quad \pm 2a^2+4b^4=1,$$

then $b=0$.

(2) *If a and b satisfy one of the following equations:*

$$2a^2-b^4=1; \quad \pm 2a^2+b^4=1,$$

then $b^4=1$.

(3) *If a and b satisfy one of the following equations:*

$$\pm a^2+b^4=1,$$

then $b=0$ or $b^4=1$.

LEMMA 8. (1) *The $\boldsymbol{Q}$-rational points on the curve $Y^2=X^3-X$ are $(X, Y)=(\infty, \infty)$, $(0, 0)$, $(1, 0)$ and $(-1, 0)$.*

(2) *The $\boldsymbol{Q}$-rational points on the curve $Y^2=X^3-4X$ are $(X, Y)=(\infty, \infty)$, $(0, 0)$, $(2, 0)$ and $(-2, 0)$.*

(3) *The $\boldsymbol{Q}$-rational points on the curve $Y^2=X^3+X$ are $(X, Y)=(\infty, \infty)$ and $(0, 0)$.*

(4) *The $\boldsymbol{Q}$-rational points on the curve $Y^2=X^3+4X$ are $(X, Y)=(\infty, \infty)$, $(0, 0)$, $(2, 4)$ and $(2, -4)$.*

PROOF. From Table 3 and Table 4 in Birch and Swinnerton-Dyer [**1**], it follows that free rank of the group of the $\boldsymbol{Q}$-rational points on each one of curves $Y^2=X^3-X$, $Y^2=X^3-4X$, $Y^2=X^3+X$ and $Y^2=X^3+4X$ is zero. Therefore $\boldsymbol{Q}$-rational points on these curves are of finite order. Here we use Theorem 22.1 in Cassels [**2**]: If (x, y) is a point of finite order defined over $\boldsymbol{Q}$ on $Y^2=X^3+AX+B$ $(A, B\in\boldsymbol{Z})$, then $x, y\in\boldsymbol{Z}$ and either $y=0$ or $y^2|(4A^3+27B^2)$. Let (x, y) be a $\boldsymbol{Q}$-rational point on $Y^2=X^3-X$, and $y\neq 0$. Then $x, y\in\boldsymbol{Z}$ and $y^2|4$. Therefore y is prime to 3, and $x^3-x=y^2\equiv 1 \bmod 3$. This is a contradiction, and (1) is proved. In the same way, (2) is proved. Let (x, y) be a $\boldsymbol{Q}$-rational point on $Y^2=X^3+X$, and $y\neq 0$. Then $x, y\in\boldsymbol{Z}$, and $y^2|4$. Therefore y is prime to 5, and $x^3+x=y^2\equiv 1 \bmod 5$. This is a contradiction, and (3) is proved. Let (x, y) be a $\boldsymbol{Q}$-rational point on $Y^2=X^3+4X$, and $y\neq 0$. Then $x, y\in\boldsymbol{Z}$, and $y^2|4^4$. Therefore y^2 is one of $1, 2^2, 2^4, 2^6$ and 2^8. But $x^3+4x \bmod 13$ is not any of $1, 2^2, 2^6$ and 2^8. Hence $y^2=2^4$, and (4) is proved.

LEMMA 9. *Let x be transcendental over $\boldsymbol{Q}$, and $f(x), g(x)\in\boldsymbol{Q}(x)$. Let n be an integer $\geqq 3$, and ζ_{2^n} be a primitive 2^n-th root of 1. Let $a=\sqrt{2}$ or $\sqrt{-2}$. Then*

$$\boldsymbol{Q}(x, \zeta_{2^n}, \sqrt{f(x)})\neq\boldsymbol{Q}(x, \zeta_{2^n}, \sqrt{ag(x)}).$$

PROOF. Assume that

$$\boldsymbol{Q}(x, \zeta_{2^n}, \sqrt{f(x)})=\boldsymbol{Q}(x, \zeta_{2^n}, \sqrt{ag(x)}).$$

We may assume that $f(x), g(x)\in\boldsymbol{Q}[x]$, and they have no multiple roots as polynomials in x. Then there is an element c of $\boldsymbol{Q}(x, \zeta_{2^n})^\times$ such that $c^2f(x)=ag(x)$. Since $f(x)$ and $g(x)$ do not have multiple roots, $c\in\boldsymbol{Q}(\zeta_{2^n})^\times$. Comparing the coefficients of the highest terms, we have $c^2=ac'$, where $c'\in\boldsymbol{Q}^\times$. This contradicts that $\sqrt{ac'}\notin\boldsymbol{Q}(\zeta_{2^n})$.

2. Proof of Theorem 1.

Let E be an elliptic curve defined over $\boldsymbol{Q}$, and $\underline{0}$ be the zero element of E. We assume that E is the elliptic curve:

$$Y^2=X^3+AX+B\,, \qquad A, B\in\boldsymbol{Q}\,, \qquad 4A^3+27B^2\neq 0\,,$$

and $\underline{0}=(\infty, \infty)$ (cf. Cassels [**2**]). Assume that E has no complex multiplication.

Then $j=12^3(4A^3)/(4A^3+27B^2)$ is neither 0 nor 12^3, and $AB\neq 0$. Put $a=27j/4(j-12^3)$. Then the invariant of the elliptic curve E':

$$Y^2=X^3-aX-a$$

is j. Therefore there is an isomorphism λ of E to E' defined over $\bar{\boldsymbol{Q}}$. From Theorem 7.1 in Cassels [2], there is an element $\mu\in\bar{\boldsymbol{Q}}$ such that $-a=\mu^4A$, $-a=\mu^6B$, and

$$\lambda(x, y)=(\mu^2x, \mu^3y)$$

for $(x, y)\in E$. Since $ABa\neq 0$, $\mu^2\in\boldsymbol{Q}^\times$. Hence the points of order 2 on E' are all $\boldsymbol{Q}$-rational, if and only if the points of order 2 on E are all $\boldsymbol{Q}$-rational. Let N be a positive integer, and (u_0, u_1) be a base of E_N over $\boldsymbol{Z}/N\boldsymbol{Z}$, where E_N denotes the kernel of the multiplication by N on E. Then $(\lambda u_0, \lambda u_1)$ is a base of E'_N. By $\boldsymbol{Q}(E_N)$ and $\boldsymbol{Q}(E'_N)$ we denote the fields which are generated by the coordinates of all elements of E_N and E'_N respectively. We identify $\mathrm{Gal}(\boldsymbol{Q}(E_N)/\boldsymbol{Q})$ and $\mathrm{Gal}(\boldsymbol{Q}(E'_N)/\boldsymbol{Q})$ with subgroups of $GL_2(\boldsymbol{Z}/N\boldsymbol{Z})$ having (u_0, u_1) and $(\lambda u_0, \lambda u_1)$ as bases respectively.

PROPOSITION 1. *Let the notations be as above. Then*

$$\mathrm{Gal}(\boldsymbol{Q}(E_N)/\boldsymbol{Q})\{\pm 1_2\}=\mathrm{Gal}(\boldsymbol{Q}(E'_N)/\boldsymbol{Q})\{\pm 1_2\},$$

where $1_2=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\in GL_2(\boldsymbol{Z}/N\boldsymbol{Z})$.

PROOF. Let $\sigma_0\in\mathrm{Gal}(\boldsymbol{Q}(E'_N)/\boldsymbol{Q})$ $(\subset GL_2(\boldsymbol{Z}/N\boldsymbol{Z}))$, and σ an extension of σ_0 to an automorphism of $\bar{\boldsymbol{Q}}$. By σ_1 we denote the restriction of σ on $\boldsymbol{Q}(E_N)$. Then $\sigma_1\in\mathrm{Gal}(\boldsymbol{Q}(E_N)/\boldsymbol{Q})$ $(\subset GL_2(\boldsymbol{Z}/N\boldsymbol{Z}))$. We view σ_0 and σ_1 as automorphisms of E'_N and E_N respectively. For $(x, y)\in E_N$,

$$\begin{aligned}\lambda^{-1}\circ\sigma_0\circ\lambda(x, y)&=\lambda^{-1}\circ\sigma_0(\mu^2x, \mu^3y)\\ &=\lambda^{-1}(\mu^2x^\sigma, (\mu^3)^\sigma y^\sigma)\\ &=(x^\sigma, \mu^{-3}(\mu^3)^\sigma y^\sigma),\end{aligned}$$

since $\mu^2\in\boldsymbol{Q}^\times$. Then $\lambda^{-1}\circ\sigma_0\circ\lambda=\pm\sigma_1$. Therefore $\sigma_0\in\mathrm{Gal}(\boldsymbol{Q}(E_N)/\boldsymbol{Q})\{\pm 1_2\}$, and

$$\mathrm{Gal}(\boldsymbol{Q}(E'_N)/\boldsymbol{Q})\{\pm 1_2\}\subset\mathrm{Gal}(\boldsymbol{Q}(E_N)/\boldsymbol{Q})\{\pm 1_2\}.$$

In the same way, we have

$$\mathrm{Gal}(\boldsymbol{Q}(E_N)/\boldsymbol{Q})\{\pm 1_2\}\subset\mathrm{Gal}(\boldsymbol{Q}(E'_N)/\boldsymbol{Q})\{\pm 1_2\}.$$

PROPOSITION 2. *Let n be an integer $\geqq 6$. Let V be a subgroup of $GL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})$ such that*

$$\det(V)=\{\textit{the determinant of } \sigma \mid \sigma\in V\}=(\boldsymbol{Z}/2^n\boldsymbol{Z})^\times, \tag{2.1}$$

$$-1_2 \in V \subset H_n^{(1)}, \tag{2.2}$$

$$V \not\supset H_n^{(5)} \cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}). \tag{2.3}$$

Then V is conjugate to a subgroup of a group A, where $A \subset H_n^{(1)}$, $\det(A) = (\boldsymbol{Z}/2^n\boldsymbol{Z})^\times$, *and A satisfies one of the following:*

(1) $A \supset H_n^{(3)} \cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})$,

$$r_{n,3}(A \cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})) = \left\langle \begin{pmatrix} 1+4 & 0 \\ 0 & 1+4 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 4 & 1 \end{pmatrix} \right\rangle \{\pm 1_2\};$$

(2) $A \supset H_n^{(4)} \cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})$,

$$r_{n,4}(A \cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\boldsymbol{Z}/2^4\boldsymbol{Z}) \cap H_4^{(1)} \,\middle|\, c = 0 \right\};$$

(3) $A \supset H_n^{(3)} \cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})$,

$$r_{n,3}(A \cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})) = \left\langle \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}, \begin{pmatrix} 1+4 & 0 \\ 0 & 1+4 \end{pmatrix} \right\rangle \{\pm 1_2\}.$$

PROOF. By (2.3) and Lemma 3 it follows that

$$r_{n,6}(V \cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})) \not\supset H_6^{(5)} \cap SL_2(\boldsymbol{Z}/2^6\boldsymbol{Z}). \tag{2.4}$$

By (2.2) we get $2 \leqq |r_{n,2}(V \cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))| \leqq 2^3$. We show that

$$|r_{n,2}(V \cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))| = 2^2 \quad \text{or} \quad 2. \tag{2.5}$$

Indeed, suppose $|r_{n,2}(V \cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))| = 2^3$. Then $r_{n,2}(V \cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})) = H_2^{(1)} \cap SL_2(\boldsymbol{Z}/2^2\boldsymbol{Z})$. There are two elements σ and τ of $V \cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})$ such that $\sigma \equiv \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \bmod 2^2$ and $\tau \equiv \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \bmod 2^2$. Then $\sigma^2 \equiv \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix} \bmod 2^3$ and $\tau^4 \equiv \begin{pmatrix} 1 & 0 \\ 8 & 1 \end{pmatrix} \bmod 2^4$. This contradicts (2.4) by Lemma 6. Hence (2.5) is proved.

(I) Suppose $|r_{n,2}(V \cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))| = 2^2$. In this case, we see that $r_{n,2}(V \cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))$ is one of the groups:

$$\left\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \right\rangle; \left\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\rangle; \left\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \right\rangle$$

by (2.2). The second group and the third group are conjugate to the first one by the inner automorphisms given by $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ respectively. Therefore we may assume that

$$r_{n,2}(V \cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})) = \left\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \right\rangle. \tag{2.6}$$

Here we have two cases:

(I. I) There is an element σ of $V \cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})$ such that

$$\sigma\equiv\begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix} \bmod 2^2 \quad\text{and}\quad \sigma\equiv\begin{pmatrix}* & *\\ 4 & *\end{pmatrix} \bmod 2^3; \tag{2.7}$$

(I. II) There is an element σ of $V\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})$ such that

$$\sigma\equiv\begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix} \bmod 2^2 \quad\text{and}\quad \sigma\equiv\begin{pmatrix}* & *\\ 0 & *\end{pmatrix} \bmod 2^3. \tag{2.8}$$

Let us consider the case (I. I). Let γ_0 be an element of $SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})$ such that $\gamma_0\equiv\begin{pmatrix}1+4 & 0\\ 0 & 1+4\end{pmatrix} \bmod 2^3$ and N_{γ_0} denote the normal subgroup of $H_n^{(1)}$ generated by $\bigcup_{\tau\in H_n^{(1)}}\tau^{-1}\gamma_0\tau$. We show that

$$r_{n,3}(V\cdot N_{\gamma_0}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\not\supset H_3^{(2)}\cap SL_2(\boldsymbol{Z}/2^3\boldsymbol{Z}). \tag{2.9}$$

Indeed conversely let us suppose $r_{n,3}(V\cdot N_{\gamma_0}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\supset H_3^{(2)}\cap SL_2(\boldsymbol{Z}/2^3\boldsymbol{Z})$. Then there are $\tau\in V$ and $\gamma\in N_{\gamma_0}$ such that $\tau\gamma\in SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})$ and $\tau\gamma\equiv\begin{pmatrix}1 & 0\\ 4 & 1\end{pmatrix} \bmod 2^3$. Since $N_{\gamma_0}\subset SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})$ and $r_{n,3}(N_{\gamma_0})=\left\langle\begin{pmatrix}1+4 & 0\\ 0 & 1+4\end{pmatrix}\right\rangle$, we have that $\tau\in V\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})$ and

$$\tau\equiv\begin{pmatrix}1 & 0\\ 4 & 1\end{pmatrix} \text{ or } \begin{pmatrix}1+4 & 0\\ 4 & 1+4\end{pmatrix} \bmod 2^3.$$

Therefore $r_{n,6}(V\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))$ includes σ^2 and τ^2 and satisfies the assumption of Lemma 6. This contradicts (2.4). Hence (2.9) is proved. (2.9) implies that

$$r_{n,3}(V\cdot N_{\gamma_0}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\cap H_3^{(2)}=\left\langle\begin{pmatrix}1+4 & 0\\ 0 & 1+4\end{pmatrix}, \begin{pmatrix}1 & 4\\ 0 & 1\end{pmatrix}\right\rangle.$$

Therefore

$$r_{n,3}(V\cdot N_{\gamma_0}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))=\left\langle\begin{pmatrix}1+4 & 0\\ 0 & 1+4\end{pmatrix}, \begin{pmatrix}1 & 2\\ 4 & 1\end{pmatrix}\right\rangle\{\pm 1_2\}.$$

Put $A=V\cdot N_{\gamma_0}\cdot(H_n^{(3)}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))$. Then $\det(A)=\det(V)=(\boldsymbol{Z}/2^n\boldsymbol{Z})^\times$, $H_n^{(1)}\supset A\supset V$, $A\supset H_n^{(3)}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})$, and $r_{n,3}(A\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))=r_{n,3}(V\cdot N_{\gamma_0}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))$ $=\left\langle\begin{pmatrix}1+4 & 0\\ 0 & 1+4\end{pmatrix}, \begin{pmatrix}1 & 2\\ 4 & 1\end{pmatrix}\right\rangle\{\pm 1_2\}$. Hence A satisfies (1) and A is a required group. Next let us consider the case (I. II). Let $\sigma\in V\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})$, and σ satisfy (2.8). If $\sigma\not\equiv\begin{pmatrix}* & *\\ 0 & *\end{pmatrix} \bmod 2^4$, then $\sigma\equiv\begin{pmatrix}1+4a & 2+4b\\ 8 & 1+4d\end{pmatrix} \bmod 2^4$. Since $\det\sigma=1$, we have $4a+4d\equiv 0 \bmod 2^4$, so that $\begin{pmatrix}1 & 0\\ 2 & 1\end{pmatrix}^{-1}\sigma\begin{pmatrix}1 & 0\\ 2 & 1\end{pmatrix}\equiv\begin{pmatrix}* & *\\ 0 & *\end{pmatrix} \bmod 2^4$. Therefore, by taking $\begin{pmatrix}1 & 0\\ 2 & 1\end{pmatrix}^{-1}V\begin{pmatrix}1 & 0\\ 2 & 1\end{pmatrix}$ in place of V we may assume that $\sigma\equiv\begin{pmatrix}* & *\\ 0 & *\end{pmatrix} \bmod 2^4$. Let γ_1 be an element of $SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})$ such that $\gamma_1\equiv\begin{pmatrix}1+4 & 0\\ 0 & 1-4\end{pmatrix} \bmod 2^4$, and N_{γ_1}

denote the normal subgroup of $H_n^{(1)}$ generated by $\bigcup_{\tau\in H_n^{(1)}}\tau^{-1}\gamma_1\tau$. We show that

$$r_{n,4}(V\cdot N_{\gamma_1}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\not\supset H_4^{(3)}\cap SL_2(\boldsymbol{Z}/2^4\boldsymbol{Z}). \tag{2.10}$$

In fact, conversely let us suppose $r_{n,4}(V\cdot N_{\gamma_1}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\supset H_4^{(3)}\cap SL_2(\boldsymbol{Z}/2^4\boldsymbol{Z})$. Then there exist $\tau\in V\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})$ and $\gamma\in N_{\gamma_1}$ such that $\tau\gamma\equiv\begin{pmatrix}1&0\\8&1\end{pmatrix}$ mod 2^4. We see that $r_{n,4}(N_{\gamma_1})=\left\langle\begin{pmatrix}1+4&0\\0&1-4\end{pmatrix}\right\rangle$. Therefore $\tau\equiv\tau_0 \bmod 2^4$, where τ_0 is one of

$$\begin{pmatrix}1+4&0\\8&1-4\end{pmatrix},\ \begin{pmatrix}1-4&0\\8&1+4\end{pmatrix},\ \begin{pmatrix}1&0\\8&1\end{pmatrix}\ \text{and}\ \begin{pmatrix}1+8&0\\8&1+8\end{pmatrix}.$$

In any case, we see that $r_{n,6}(V\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))$ satisfies the assumption of Lemma 5 or the assumption of Lemma 6. This contradicts (2.4). Hence (2.10) is proved. Since $r_{n,4}(\sigma^4)=\begin{pmatrix}1&8\\0&1\end{pmatrix}$ and $r_{n,4}(\gamma_1^2)=\begin{pmatrix}1+8&0\\0&1+8\end{pmatrix}$, (2.10) implies

$$r_{n,4}(V\cdot N_{\gamma_1}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\cap H_4^{(3)}=\left\langle\begin{pmatrix}1&8\\0&1\end{pmatrix},\ \begin{pmatrix}1+8&0\\0&1+8\end{pmatrix}\right\rangle.$$

Since

$$r_{n,3}(\sigma^2)=\begin{pmatrix}1&4\\0&1\end{pmatrix}\quad\text{and}\quad r_{n,3}(\gamma_1)=\begin{pmatrix}1+4&0\\0&1+4\end{pmatrix}\in r_{n,3}(V\cdot N_{\gamma_1}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\cap H_3^{(2)},$$

we have

$$r_{n,3}(V\cdot N_{\gamma_1}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\cap H_3^{(2)}=\left\langle\begin{pmatrix}1&4\\0&1\end{pmatrix},\ \begin{pmatrix}1+4&0\\0&1+4\end{pmatrix}\right\rangle.$$

Therefore

$$\begin{aligned}r_{n,4}(V\cdot N_{\gamma_1}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))&=\langle r_{n,4}(\sigma),\ r_{n,4}(\gamma_1)\rangle\{\pm 1_2\}\\&=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\in SL_2(\boldsymbol{Z}/2^4\boldsymbol{Z})\cap H_4^{(1)}\,\middle|\,c=0\right\}.\end{aligned}$$

Put $A=V\cdot N_{\gamma_1}\cdot(H_n^{(4)}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))$. Then we see that A satisfies (2) and A is a required group.

(II) Suppose that $|r_{n,2}(V\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))|=2$. The assumption (2.2) yields $r_{n,2}(V\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))=\{\pm 1_2\}$. If $r_{n,3}(V\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\supset H_3^{(2)}\cap SL_2(\boldsymbol{Z}/2^3\boldsymbol{Z})$, then $r_{n,6}(V\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\supset H_6^{(5)}\cap SL_2(\boldsymbol{Z}/2^6\boldsymbol{Z})$ by Lemma 3, and this contradicts (2.4). Therefore $r_{n,3}(V\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\not\supset H_3^{(2)}\cap SL_2(\boldsymbol{Z}/2^3\boldsymbol{Z})$, so that $|r_{n,3}(V\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\cap H_3^{(2)}|\leqq 2^2$. If $|r_{n,3}(V\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\cap H_3^{(2)}|=2^2$, then $r_{n,3}(V\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\cap H_3^{(2)}$ is one of the following 7 groups:

$$U_1=\left\langle\begin{pmatrix}1&0\\4&1\end{pmatrix},\ \begin{pmatrix}1&4\\0&1\end{pmatrix}\right\rangle;\quad U_2=\left\langle\begin{pmatrix}1&0\\4&1\end{pmatrix},\ \begin{pmatrix}1+4&4\\0&1+4\end{pmatrix}\right\rangle;$$

$$U_3=\left\langle\begin{pmatrix}1 & 4\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1+4 & 0\\ 4 & 1+4\end{pmatrix}\right\rangle;\quad U_4=\left\langle\begin{pmatrix}1+4 & 0\\ 4 & 1+4\end{pmatrix}, \begin{pmatrix}1+4 & 4\\ 0 & 1+4\end{pmatrix}\right\rangle;$$

$$W_1=\left\langle\begin{pmatrix}1 & 0\\ 4 & 1\end{pmatrix}, \begin{pmatrix}1+4 & 0\\ 0 & 1+4\end{pmatrix}\right\rangle;\quad W_2=\left\langle\begin{pmatrix}1 & 4\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1+4 & 0\\ 0 & 1+4\end{pmatrix}\right\rangle;$$

$$W_3=\left\langle\begin{pmatrix}1 & 4\\ 4 & 1\end{pmatrix}, \begin{pmatrix}1+4 & 0\\ 0 & 1+4\end{pmatrix}\right\rangle.$$

If $r_{n,3}(V\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\cap H_3^{(2)}$ is one of U_i $(i=1, 2, 3, 4)$, then $r_{n,6}(V\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\supset H_6^{(5)}\cap SL_2(\boldsymbol{Z}/2^6\boldsymbol{Z})$ by Lemma 6. This is a contradiction to (2.4). Therefore $r_{n,3}(V\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\cap H_3^{(2)}$ is one of W_i $(i=1, 2, 3)$. If $|r_{n,3}(V\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\cap H_3^{(2)}|\leqq 2$, then $r_{n,3}(V\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\cap H_3^{(2)}$ is included in one of the groups W_1, W_2 and W_3. Since W_2 and W_3 are conjugate to W_1 by $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$ and $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ respectively, we may assume that

$$r_{n,3}(V\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\cap H_3^{(2)}\subset W_1.$$

Then

$$r_{n,3}(V\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\subset W_1\cdot\{\pm 1_2\}.$$

Let γ_2 and γ_3 be elements of $SL_2(\boldsymbol{Z}/2^2\boldsymbol{Z})$ such that $\gamma_2\equiv\begin{pmatrix}1+4 & 0\\ 0 & 1+4\end{pmatrix}$ mod 2^3 and $\gamma_3\equiv\begin{pmatrix}1 & 0\\ 4 & 1\end{pmatrix}$ mod 2^3. By N_{γ_i} $(i=2, 3)$ we denote the normal subgroup of $H_n^{(1)}$ which is generated by $\bigcup_{\tau\in H_n^{(1)}}\tau^{-1}\gamma_i\tau$. Then we have

$$\begin{aligned} &r_{n,3}(V\cdot N_{\gamma_2}\cdot N_{\gamma_3}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\\ &\quad=r_{n,3}((V\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\cdot N_{\gamma_2}\cdot N_{\gamma_3})=W_1\cdot\{\pm 1_2\}.\end{aligned}$$

Put $A=V\cdot N_{\gamma_2}\cdot N_{\gamma_3}\cdot(H_n^{(3)}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))$. Then we see that A satisfies (3), and A is a required group.

PROPOSITION 3. *Let E be an elliptic curve defined over $\boldsymbol{Q}$. Assume that E has no complex multiplication and the points of order 2 of E are all $\boldsymbol{Q}$-rational. Identify* $\mathrm{Gal}(\boldsymbol{Q}(E_{2^n})/\boldsymbol{Q})$ *with a subgroup of $GL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})$ by taking a base of E_{2^n} over $\boldsymbol{Z}/2^n\boldsymbol{Z}$. Then*

$$\mathrm{Gal}(\boldsymbol{Q}(E_{2^n})/\boldsymbol{Q})\{\pm 1_2\}\supset H_n^{(5)}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}),$$

for any integer $n\geqq 6$.

PROOF. By Proposition 1, we may assume that E is the curve $E(a)$: $Y^2=X^3-aX-a$, where $a\in\boldsymbol{Q}$ and $a(4a-27)\neq 0$. Let $\boldsymbol{Q}(\alpha)$ be a rational function field of one variable α over $\boldsymbol{Q}$. Let $E(\alpha): Y^2=X^3-\alpha X-\alpha$ be an elliptic curve defined over $\boldsymbol{Q}(\alpha)$ with zero element $\underline{0}=(\infty, \infty)$. By $\mathfrak{O}$ we denote the specialization ring of the specialization $\alpha\to a$ over $\boldsymbol{Q}$ and $\mathfrak{p}$ denotes the maximal ideal of $\mathfrak{O}$. Since

$a\in\boldsymbol{Q}$, $\mathfrak{O}/\mathfrak{p}\cong\boldsymbol{Q}$. We denote by $\boldsymbol{Q}(\alpha, E(\alpha)_{2^n})$ the field which is generated by α and the coordinates of all elements of $E(\alpha)_{2^n}$. Let $\mathfrak{S}$ be the integral closure of $\mathfrak{O}$ in $\boldsymbol{Q}(\alpha, E(\alpha)_{2^n})$, and $\mathfrak{P}$ a maximal ideal of $\mathfrak{S}$ lying above $\mathfrak{p}$. Then we regard $\mathfrak{O}/\mathfrak{p}$ as $\boldsymbol{Q}$ and $\mathfrak{S}/\mathfrak{P}$ as a subfield of $\bar{\boldsymbol{Q}}$; $\boldsymbol{Q}=\mathfrak{O}/\mathfrak{p}\subset\mathfrak{S}/\mathfrak{P}\subset\bar{\boldsymbol{Q}}$. If $(x, y)\in E(\alpha)_{2^n}$ and $(x, y)\neq(\infty, \infty)$, then $x, y\in S$, $(\bar{x}, \bar{y})\in E(a)_{2^n}$ and $(\bar{x}, \bar{y})\neq(\infty, \infty)$, where "$-$" indicates the reduction mod $\mathfrak{P}$. Therefore the reduction mod $\mathfrak{P}$ induces the homomorphism: $E(\alpha)_{2^n}\to E(a)_{2^n}$ whose kernel is trivial. Since $|E(\alpha)_{2^n}|=|E(a)_{2^n}|$, this homomorphism is an isomorphism. Let $V_{\mathfrak{P}}$ be the decomposition group of $\mathfrak{P}$: $V_{\mathfrak{P}}=\{\sigma\in\mathrm{Gal}(\boldsymbol{Q}(\alpha, E(\alpha)_{2^n})/\boldsymbol{Q}(\alpha))\mid\mathfrak{P}^{\sigma}=\mathfrak{P}\}$. Then for each $\sigma\in V_{\mathfrak{P}}$, we can associate an automorphism $\bar{\sigma}$ of $\mathfrak{S}/\mathfrak{P}$ over $\mathfrak{O}/\mathfrak{p}$ in the natural way, and the map given by $\sigma\to\bar{\sigma}$ induces a homomorphism $\phi: V_{\mathfrak{P}}\to\mathrm{Gal}((\mathfrak{S}/\mathfrak{P})/(\mathfrak{O}/\mathfrak{p}))$. We know that ϕ is surjective (cf. Lang [5], Chapter 1). Assume that (u_0, u_1) is a base of $E(\alpha)_{2^n}$ over $\boldsymbol{Z}/2^n\boldsymbol{Z}$. Let $\sigma\in V_{\mathfrak{P}}$, and

$$(\sigma u_0, \sigma u_1)=(u_0, u_1)\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

where $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in GL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})$. Then

$$(\bar{\sigma}\bar{u}_0, \bar{\sigma}\bar{u}_1)=(\bar{u}_0, \bar{u}_1)\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Therefore ϕ is an isomorphism and $\mathfrak{S}/\mathfrak{P}=\boldsymbol{Q}(E(a)_{2^n})$. If we denote by L the fixed subfield of $\boldsymbol{Q}(\alpha, E(\alpha)_{2^n})$ under $V_{\mathfrak{P}}$, then $(L\cap\mathfrak{S})/(L\cap\mathfrak{P})=\mathfrak{O}/\mathfrak{p}=\boldsymbol{Q}$ (cf. Lang [5], Chapter 1). Identify $\mathrm{Gal}(\boldsymbol{Q}(\alpha, E(\alpha)_{2^n})/\boldsymbol{Q}(\alpha))$ (respectively $\mathrm{Gal}(\boldsymbol{Q}(E(a)_{2^n})/\boldsymbol{Q})$) with a subgroup of $GL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})$ by taking the base (u_0, u_1) (respectively $(\bar{u}_0, \bar{u}_1)$). Then $V_{\mathfrak{P}}=\mathrm{Gal}(\boldsymbol{Q}(E(a)_{2^n})/\boldsymbol{Q})$. Let ζ_{2^n} be a primitive 2^n-th root of 1. It is well known (cf. Shimura [9], Chapter 6) that

$$\mathrm{Gal}(\boldsymbol{Q}(\alpha, E(\alpha)_{2^n})/\boldsymbol{Q}(\alpha))=GL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}),$$

$$\boldsymbol{Q}(\alpha, E(\alpha)_{2^n})\cap\bar{\boldsymbol{Q}}=\boldsymbol{Q}(\zeta_{2^n})=\mathrm{fix}(SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})),$$

$$\mathrm{fix}(\{\pm1_2\})=\boldsymbol{Q}(\alpha, \{x\}_{(x,y)\in E(\alpha)_{2^n}}),$$

where $\mathrm{fix}(*)$ denotes the fixed field of $\boldsymbol{Q}(\alpha, E(\alpha)_{2^n})$ under $*$. We denote $V_{\mathfrak{P}}\{\pm1_2\}$ by V. Since $\zeta_{2^n}\in\boldsymbol{Q}(E(a)_{2^n})$ and $\zeta_{2^n}^{\sigma}=\zeta_{2^n}^{\det(\sigma)}$ for $\sigma\in\mathrm{Gal}(\boldsymbol{Q}(E(a)_{2^n})/\boldsymbol{Q})$ $(=V_{\mathfrak{P}})$, we have $\det(V)=(\boldsymbol{Z}/2^n\boldsymbol{Z})^{\times}$. Since the points of order 2 of $E(a)$ are all $\boldsymbol{Q}$-rational, we have $V\subset H_n^{(1)}$. Assume that the consequence of Proposition 3 is false, namely

$$V=\mathrm{Gal}(\boldsymbol{Q}(E(a)_{2^n})/\boldsymbol{Q})\{\pm1_2\}\not\supset H_n^{(5)}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}).$$

We shall prove that this assumption derives a contradiction. By Proposition 2, V is conjugate to a subgroup of a group A in $GL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})$, where $A\subset H_n^{(1)}$, $\det(A)=(\boldsymbol{Z}/2^n\boldsymbol{Z})^{\times}$, and A satisfies one of (1), (2) and (3) in Proposition 2. Then we may assume $V \subset A$ by selecting a suitable base (u_0, u_1). It follows that

$$L=\mathrm{fix}(V_{\mathfrak{P}}) \supset \mathrm{fix}(V) \supset \mathrm{fix}(A)=F \supset \boldsymbol{Q}(\alpha).$$

Since the residue class field $(L \cap \mathfrak{S})/(L \cap \mathfrak{P})$ is equal to $\boldsymbol{Q}$,

$$(F \cap \mathfrak{S})/(F \cap \mathfrak{P})=\boldsymbol{Q}. \tag{2.11}$$

We determine F for A of each type and deduce a contradiction to (2.11). Put

$$\begin{cases} 2^{n-4}u_i=(h_i, \sqrt{h_i^3-\alpha h_i-\alpha}), \\ 2^{n-3}u_i=(g_i, \sqrt{g_i^3-\alpha g_i-\alpha}), \\ 2^{n-2}u_i=(f_i, \sqrt{f_i^3-\alpha f_i-\alpha}), \\ 2^{n-1}u_i=(e_i, 0), \end{cases} \tag{2.12}$$

where $i=0, 1$, and

$$(e_0, 0)+(e_1, 0)=(e_2, 0).$$

By (1.11) and (1.12),

$$\begin{cases} f_0=e_0+\sqrt{(e_0-e_1)(e_0-e_2)}, \\ f_1=e_1+\sqrt{(e_1-e_2)(e_1-e_0)}, \\ g_i=f_i+\sqrt{(f_i-e_1)(f_i-e_2)}+\sqrt{(f_i-e_2)(f_i-e_0)}+\sqrt{(f_i-e_0)(f_i-e_1)}, \\ h_i=g_i+\sqrt{(g_i-e_1)(g_i-e_2)}+\sqrt{(g_i-e_2)(g_i-e_0)}+\sqrt{(g_i-e_0)(g_i-e_1)}, \end{cases} \tag{2.13}$$

where $i=0, 1$. In the following, as a square root of $(e_0-e_1)(e_0-e_2)$, $(e_1-e_2)(e_1-e_0)$, $\cdots$, $(g_i-e_0)(g_i-e_1)$ we use $\sqrt{(e_0-e_1)(e_0-e_2)}$, $\sqrt{(e_1-e_2)(e_1-e_0)}$, $\cdots$, $\sqrt{(g_i-e_0)(g_i-e_1)}$ in (2.13) respectively. Since $A \subset H_n^{(1)}$, we have
$F=\mathrm{fix}(A) \supset \mathrm{fix}(H_n^{(1)})=\boldsymbol{Q}(\alpha, E(\alpha)_2)=\boldsymbol{Q}(\alpha, e_0, e_1, e_2)$. Put $s=1+2e_1/e_0$. Then

$$\begin{cases} e_0=-(s^2+3)/(s^2-1), \\ e_1=-(s^2+3)/2(s+1), \\ e_2=(s^2+3)/2(s-1), \end{cases} \tag{2.14}$$

so that $\boldsymbol{Q}(\alpha, E(\alpha)_2)=\boldsymbol{Q}(s)$. We have

$$\begin{cases} e_0-e_1=(s^2+3)(s-3)/2(s^2-1), \\ e_0-e_2=-(s^2+3)(s+3)/2(s^2-1), \\ e_1-e_2=-(s^2+3)s/(s^2-1). \end{cases} \tag{2.15}$$

We divide the consideration into 3 parts (I), (II), and (III) corresponding to each case that A satisfies (1), (2), or (3).

(I) Suppose that A satisfies (1) in Proposition 2. Put

$$F'=\operatorname{fix}(A\cdot(H_n^{(2)}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))).$$

Then by Lemma 2 we have

$$\begin{aligned}[F':\boldsymbol{Q}(s)]&=[H_n^{(1)}:A\cdot(H_n^{(2)}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))]\\ &=[\det(H_n^{(1)}):\det(A\cdot(H_n^{(2)}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})))]\\ &\quad\times[H_n^{(1)}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}):(A\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\cdot(H_n^{(2)}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))]\\ &=1\times\frac{|H_n^{(1)}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})|}{|(A\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\cdot(H_n^{(2)}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))|}\\ &=1\times\prod_{h=1}^{n}\frac{|r_{n,h}(H_n^{(1)}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\cap H_h^{(h-1)}|}{|r_{n,h}((A\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\cdot(H_n^{(2)}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})))\cap H_n^{(h-1)}|}\\ &=1\times1\times2\times\prod_{h=3}^{n}1=2. \qquad (2.16)\end{aligned}$$

We obtain also

$$\begin{aligned}&[F'(\zeta_{2^n}):\boldsymbol{Q}(s,\zeta_{2^n})]\\ &=[H_n^{(1)}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}):(A\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\cdot(H_n^{(2)}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))]\\ &=2. \qquad (2.17)\end{aligned}$$

For any $\sigma\in(A\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\cdot(H_n^{(2)}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))$,

$$\sigma(2^{n-2}u_0)=2^{n-2}u_0 \quad\text{or}\quad 2^{n-2}u_0+(e_0,0).$$

Therefore by Lemma 1,

$$\begin{aligned}\sqrt{(e_0-e_1)(e_0-e_2)}&\in\operatorname{fix}((A\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\cdot(H_n^{(2)}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})))\\ &=F'(\zeta_{2^n}).\end{aligned}$$

In the following, $\sqrt{\dfrac{e_0-e_1}{e_0-e_2}}$ denotes $\dfrac{\sqrt{(e_0-e_1)(e_0-e_2)}}{e_0-e_2}$. The equations (2.15) give $\dfrac{e_0-e_1}{e_0-e_2}=(-1)(s-3)/(s+3)$ and $F'(\zeta_{2^n})=\boldsymbol{Q}(s,\zeta_{2^n},\sqrt{(-1)(s-3)(s+3)})$, by (2.17). On the other hand, by (2.16) there is an element $f(s)$ of $\boldsymbol{Q}[s]$ with no multiple roots such that $F'=\boldsymbol{Q}(s,\sqrt{f(s)})$. Then

$$\boldsymbol{Q}(s,\zeta_{2^n},\sqrt{f(s)})=\boldsymbol{Q}(s,\zeta_{2^n},\sqrt{(-1)(s+3)(s-3)}).$$

Therefore $f(s)=c^2(-1)(s+3)(s-3)$, where $c\in\boldsymbol{Q}(s,\zeta_{2^n})^\times$. Since neither $f(s)$ nor $(-1)(s+3)(s-3)$ has any multiple root, we see $c\in\boldsymbol{Q}(\zeta_{2^n})^\times$. Since $c^2\in\boldsymbol{Q}$, we may assume that c^2 is one of 1, -1, 2 and -2. Put $t_1=\sqrt{\dfrac{e_0-e_1}{e_0-e_2}}$, $t_2=\sqrt{-1}\,t_1$, $t_3=\sqrt{2}\,t_1$ and $t_4=\sqrt{-2}\,t_1$. Then F' is one of $\boldsymbol{Q}(s,t_i)$ $(i=1,2,3,4)$. By (2.15) we see $\boldsymbol{Q}(s, t_i)=\boldsymbol{Q}(t_i)$. Therefore F' is one of $\boldsymbol{Q}(t_i)$ $(i=1, 2, 3, 4)$. Since A satisfies (1) in Proposition 2, $A\supset H_n^{(3)}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})$ and

$$r_{n,3}(A\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))=\left\langle\begin{pmatrix}1+4 & 0\\ 0 & 1+4\end{pmatrix}, \begin{pmatrix}1 & 2\\ 4 & 1\end{pmatrix}\right\rangle\{\pm 1_2\}.$$

Let $\sigma\in A\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})$ with $r_{n,3}(\sigma)=\begin{pmatrix}1 & 2\\ 4 & 1\end{pmatrix}$, and $\gamma\in A\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})$ with $r_{n,3}(\gamma)=\begin{pmatrix}1+4 & 0\\ 0 & 1+4\end{pmatrix}$. Then we see

$$\begin{cases}\gamma(2^{n-3}u_0)=2^{n-3}u_0+(e_0, 0),\\ \sigma(2^{n-3}u_0)=2^{n-3}u_0+(e_1, 0),\end{cases}$$

$$\begin{cases}\gamma(2^{n-2}u_1)=2^{n-2}u_1,\\ \sigma(2^{n-2}u_1)=2^{n-2}u_1+(e_0, 0).\end{cases}$$

Therefore by Lemma 1,

$$\begin{cases}\sqrt{(f_0-e_1)(f_0-e_2)}^{\gamma}=\sqrt{(f_0-e_1)(f_0-e_2)},\\ \sqrt{(f_0-e_1)(f_0-e_2)}^{\sigma}=-\sqrt{(f_0-e_1)(f_0-e_2)},\end{cases} \tag{2.18}$$

$$\begin{cases}\sqrt{(e_1-e_2)(e_1-e_0)}^{\gamma}=\sqrt{(e_1-e_2)(e_1-e_0)},\\ \sqrt{(e_1-e_2)(e_1-e_0)}^{\sigma}=-\sqrt{(e_1-e_2)(e_1-e_0)}.\end{cases} \tag{2.19}$$

Since $\sqrt{(f_0-e_1)(f_0-e_2)}$, $\sqrt{(e_1-e_2)(e_1-e_0)}\in\boldsymbol{Q}(\alpha, \{x\}_{(x,y)\in E(\alpha)_{2^n}})=\text{fix}(\{\pm 1_2\})$ and $\sqrt{(f_0-e_1)(f_0-e_2)}$, $\sqrt{(e_1-e_2)(e_1-e_0)}\in\boldsymbol{Q}(\alpha, E(\alpha)_{2^3})=\text{fix}(H_n^{(3)})$, (2.18) and (2.19) imply that

$$\sqrt{(f_0-e_1)(f_0-e_2)}\times\sqrt{(e_1-e_2)(e_1-e_0)}\in\text{fix}(A\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))=F(\zeta_{2^n}).$$

In the same way as before, we see

$$[F(\zeta_{2^n}): F'(\zeta_{2^n})]=[F: F']=2. \tag{2.20}$$

We have

$$\frac{f_0-e_1}{f_0-e_2}=\sqrt{\frac{e_0-e_1}{e_0-e_2}}=t_1\in F'(\zeta_{2^n}),$$

$$\frac{e_1-e_2}{e_1-e_0}=\frac{2s}{s-3}=(t_1^2-1)/t_1^2.$$

Then, since f_0-e_2, $e_1-e_0\in F'(\zeta_{2^n})$, we have

$$F(\zeta_{2^n})\supset F'(\zeta_{2^n}, \sqrt{t_1(t_1^2-1)})=\boldsymbol{Q}(t_1, \zeta_{2^n}, \sqrt{t_1(t_1^2-1)}).$$

By (2.20) we have $F(\zeta_{2^n})=\boldsymbol{Q}(t_1, \zeta_{2^n}, \sqrt{t_1(t_1^2-1)})$. On the other hand, by (2.20) there exists an element $f(t_i)$ of $\boldsymbol{Q}[t_i]$ with no multiple root such that $F=$

$\boldsymbol{Q}(t_i, \sqrt{f(t_i)})$, where $F'=\boldsymbol{Q}(t_i)$. In the case $F'=\boldsymbol{Q}(t_1)$, we obtain

$$F(\zeta_{2^n})=\boldsymbol{Q}(t_1, \zeta_{2^n}, \sqrt{t_1(t_1^2-1)})=\boldsymbol{Q}(t_1, \zeta_{2^n}, \sqrt{f(t_1)}).$$

In the same way as before, we may assume that

$$f(t_1)=c^2t_1(t_1^2-1), \qquad \text{where } c^2=\pm 1 \text{ or } \pm 2.$$

Since $E(a)$ is elliptic, t_1 and $\sqrt{f(t_1)}$ are integral over the specialization ring $\mathfrak{O}$, i. e., $t_1, \sqrt{f(t_1)}\in\mathfrak{S}$, so that $t_1, \sqrt{f(t_1)}\in F\cap\mathfrak{S}$. By (2.11) $(X, Y)=(\bar{t}_1, \overline{\sqrt{f(t_1)}})$ is a finite $\boldsymbol{Q}$-rational point on

$$Y^2=c^2X(X^2-1).$$

Then, by Lemma 8 $\bar{t}_1=0$ or $\bar{t}_1^2=1$. If $\bar{t}_1=0$, then $\overline{\left(\frac{e_0-e_1}{e_0-e_2}\right)}=0$. If $\bar{t}_1^2=1$, then $\overline{\left(\frac{e_0-e_1}{e_0-e_2}\right)}=1$, so that $\bar{e}_1=\bar{e}_2$. These contradict that $E(a)$ is elliptic. If $F'=\boldsymbol{Q}(t_2)$, then

$$F(\zeta_{2^n})=\boldsymbol{Q}(t_2, \zeta_{2^n}, \sqrt{t_2(t_2^2+1)})=\boldsymbol{Q}(t_2, \zeta_{2^n}, \sqrt{f(t_2)}).$$

Then we may assume that $f(t_2)=c^2t_2(t_2^2+1)$, where $c^2=\pm 1$ or ± 2. In the same way as above, $(X, Y)=(\bar{t}_2, \overline{\sqrt{f(t_2)}})$ is a finite $\boldsymbol{Q}$-rational point on

$$Y^2=c^2X(X^2+1).$$

Then, by Lemma 8 $\bar{t}_2=0$ or $\bar{t}_2^2=1$. If $\bar{t}_2=0$, then $\bar{t}_1=0$. If $\bar{t}_2^2=1$, then $\bar{t}_1^2=-1$, so that $\bar{e}_0=0$ and $a=0$. These contradict that $E(a)$ is elliptic. If $F'=\boldsymbol{Q}(t_3)$, then

$$F(\zeta_{2^n})=\boldsymbol{Q}(t_3, \zeta_{2^n}, \sqrt{\sqrt{2}\,t_3(t_3^2-2)})=\boldsymbol{Q}(t_3, \zeta_{2^n}, \sqrt{f(t_3)}).$$

This contradicts Lemma 9. If $F'=\boldsymbol{Q}(t_4)$, then

$$F(\zeta_{2^n})=\boldsymbol{Q}(t_4, \zeta_{2^n}, \sqrt{\sqrt{-2}\,t_4(t_4^2+2)})=\boldsymbol{Q}(t_4, \zeta_{2^n}, \sqrt{f(t_4)}).$$

This contradicts Lemma 9.

(II) Suppose that A satisfies (2) in Proposition 2. Put

$$F'=\mathrm{fix}(A\cdot(H_n^{(2)}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))),$$

$$F''=\mathrm{fix}(A\cdot(H_n^{(3)}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))).$$

In the same way as in the first case, we see that F' is one of $\boldsymbol{Q}(t_i)$ $(i=1, 2, 3, 4)$, where t_i $(i=1, 2, 3, 4)$ are the same as t_i $(i=1, 2, 3, 4)$ in the first case. We have

$$[F'':F']=[F''(\zeta_{2^n}):F'(\zeta_{2^n})]=[F:F'']=[F(\zeta_{2^n}):F''(\zeta_{2^n})]=2.$$

Let $\sigma\in A\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})$ with $r_{n,4}(\sigma)=\begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}$, and $\gamma\in A\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})$ with $r_{n,4}(\gamma)=\begin{pmatrix}1+4 & 0\\ 0 & 1-4\end{pmatrix}$. Then

$$\sigma(2^{n-3}u_0)=2^{n-3}u_0\,,$$

$$\gamma(2^{n-3}u_0)=2^{n-3}u_0+(e_0,\ 0)\,.$$

This implies that $\sqrt{(f_0-e_1)(f_0-e_2)}\in \mathrm{fix}((A\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\cdot(H_n^{(3)}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})))=F''(\zeta_{2^n})$, since $r_{n,3}(A\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))=\langle r_{n,3}(\sigma),\ r_{n,3}(\gamma)\rangle\{\pm 1_2\}$. We saw that $\dfrac{f_0-e_1}{f_0-e_2}=t_1$. Put

$$\sqrt{t_1}=\sqrt{\frac{f_0-e_1}{f_0-e_2}}=\frac{\sqrt{(f_0-e_1)(f_0-e_2)}}{f_0-e_2}\,.$$

Then, since $f_0-e_2\in F'(\zeta_{2^n})$, we have

$$F''(\zeta_{2^n})=\boldsymbol{Q}(t_1,\ \zeta_{2^n},\ \sqrt{t_1})\,.$$

If $F'=\boldsymbol{Q}(t_3)$ or $\boldsymbol{Q}(t_4)$, then we have a contradiction to Lemma 9. Therefore $F'=\boldsymbol{Q}(t_1)$ or $\boldsymbol{Q}(t_2)$. Put

$$\sqrt{t_1}=v_{1,1},\ \sqrt{-1}\,v_{1,1}=v_{1,2},\ \sqrt{2}\,v_{1,1}=v_{1,3},\ \sqrt{-2}\,v_{1,1}=v_{1,4}\,,$$

$$\sqrt{t_2}=v_{2,1},\ \sqrt{-1}\,v_{2,1}=v_{2,2},\ \sqrt{2}\,v_{2,1}=v_{2,3},\ \sqrt{-2}\,v_{2,1}=v_{2,4}\,.$$

Then $F''=\boldsymbol{Q}(v_{i,j})$, where i is one of 1 and 2, and j is one of 1, 2, 3 and 4. Next we determine F. The genus of F as a function field of one variable is 1 by an easy computation (cf. Shimura [**9**]). Set

$$B=\left\{\begin{pmatrix} a & b\\ c & d\end{pmatrix}\in SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})\cap H_n^{(1)}\ \middle|\ a\equiv 1 \bmod 2^3,\ c\equiv 0 \bmod 2^4\right\}.$$

We have

$$r_{n,4}(B\{\pm 1_2\})=\left\langle\begin{pmatrix} 1+8 & 0\\ 0 & 1+8\end{pmatrix},\ \begin{pmatrix} 1 & 2\\ 0 & 1\end{pmatrix}\right\rangle\{\pm 1_2\}\,.$$

Then $2=[A\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}):\ B\{\pm 1_2\}]=[\mathrm{fix}(B\{\pm 1_2\}):F(\zeta_{2^n})]$ and $\mathrm{fix}(B\{\pm 1_2\})=F(\zeta_{2^n},\ \sqrt{(f_0-e_2)(f_0-e_0)})$. We have

$$\frac{f_0-e_0}{f_0-e_2}=\frac{\sqrt{(e_0-e_1)(e_0-e_2)}}{e_0-e_2+\sqrt{(e_0-e_1)(e_0-e_2)}}=\frac{t_1}{1+t_1}\,.$$

Put

$$\frac{\sqrt{(f_0-e_2)(f_0-e_0)}}{f_0-e_2}=\sqrt{\frac{f_0-e_0}{f_0-e_2}}=\frac{\sqrt{t_1}}{\sqrt{t_1+1}}\,,$$

where $\sqrt{t_1}=v_{1,1}$. Since $F''(\zeta_{2^n})=\boldsymbol{Q}(\zeta_{2^n},\ \sqrt{t_1})\subset F(\zeta_{2^n})$, we get

$$\mathrm{fix}(B\{\pm 1_2\})=F(\zeta_{2^n},\ \sqrt{(f_0-e_2)(f_0-e_0)})=F(\zeta_{2^n},\ \sqrt{t_1+1})\,.$$

We see $\sqrt{(g_0-e_1)(g_0-e_2)}\in\mathrm{fix}(B\{\pm 1_2\})$. Noting $g_0-e_2\in\mathrm{fix}(B\{\pm 1_2\})$, we have

$$\sqrt{\frac{g_0-e_1}{g_0-e_2}}\in \mathrm{fix}(B\{\pm 1_2\})=F(\zeta_{2n},\ \sqrt{t_1+1}).$$

Therefore, there are two elements q and r of $F(\zeta_{2n})$ such that

$$\frac{g_0-e_1}{g_0-e_2}=(q+r\sqrt{t_1+1})^2. \tag{2.21}$$

We have

$$\frac{g_0-e_1}{g_0-e_2}=\frac{\dfrac{f_0-e_1}{f_0-e_2}+\sqrt{\dfrac{f_0-e_1}{f_0-e_2}}+\sqrt{\dfrac{f_0-e_0}{f_0-e_2}}+\sqrt{\dfrac{f_0-e_0}{f_0-e_2}}\sqrt{\dfrac{f_0-e_1}{f_0-e_2}}}{1+\sqrt{\dfrac{f_0-e_1}{f_0-e_2}}+\sqrt{\dfrac{f_0-e_0}{f_0-e_2}}+\sqrt{\dfrac{f_0-e_0}{f_0-e_2}}\sqrt{\dfrac{f_0-e_1}{f_0-e_2}}}.$$

$$=\sqrt{t_1}-t_1+\sqrt{t_1}\,t_1+(\sqrt{t_1}-t_1)\sqrt{t_1+1}$$

$$=q^2+r^2(t_1+1)+2qr\sqrt{t_1+1}. \tag{2.22}$$

By (2.21) and (2.22),

$$q^2+r^2(t_1+1)=\sqrt{t_1}-t_1+\sqrt{t_1}\,t_1, \qquad 2qr=\sqrt{t_1}-t_1,$$

and so

$$q^2=(\sqrt{t_1}-t_1+\sqrt{t_1}\,t_1\pm t_1)/2.$$

If $q^2=(\sqrt{t_1}-t_1+\sqrt{t_1}\,t_1-t_1)/2=\sqrt{t_1}(\sqrt{t_1}-1)^2/2$, then $F(\zeta_{2n})=\boldsymbol{Q}(\sqrt{t_1}, \zeta_{2n}, \sqrt{\sqrt{t_1}})$, since $F''(\zeta_{2n})=\boldsymbol{Q}(\sqrt{t_1}, \zeta_{2n})$ and $[F(\zeta_{2n}): F''(\zeta_{2n})]=2$. Therefore the genus of $F(\zeta_{2n})$ is 0. This contradicts that the genus of $F(\zeta_{2n})$ is 1. Hence $q^2=\sqrt{t_1}(t_1+1)/2$, so that

$$F(\zeta_{2n})=\boldsymbol{Q}(\sqrt{t_1},\ \zeta_{2n},\ \sqrt{\sqrt{t_1}(t_1+1)})$$

$$=\boldsymbol{Q}(v_{1,1},\ \zeta_{2n},\ \sqrt{v_{1,1}(v_{1,1}{}^2+1)}).$$

Since $[F: F'']=2$ and $F''=\boldsymbol{Q}(v_{i,j})$, where i is one of 1 and 2, and j is one of 1, 2, 3 and 4, there is an element $f(v_{i,j})$ of $\boldsymbol{Q}[v_{i,j}]$ with no multiple root such that

$$F=\boldsymbol{Q}(v_{i,j},\ \sqrt{f(v_{i,j})}).$$

Then

$$F(\zeta_{2n})=\boldsymbol{Q}(v_{i,j},\ \zeta_{2n},\ \sqrt{f(v_{i,j})})$$

$$=\boldsymbol{Q}(v_{i,j},\ \zeta_{2n},\ \sqrt{v_{1,1}(v_{1,1}{}^2+1)}).$$

If $F''=\boldsymbol{Q}(v_{1,j})$ for a certain j, then we have a contradiction in the same way as in the first case. If $F''=\boldsymbol{Q}(v_{2,1})$, then

$$\boldsymbol{Q}(v_{2,1},\ \zeta_{2n},\ \sqrt{f(v_{2,1})})=\boldsymbol{Q}(v_{2,1},\ \zeta_{2n},\ \sqrt{v_{2,1}(v_{2,1}{}^2+\sqrt{-1})}).$$

Since $f(v_{2,1})$ and $v_{2,1}(v_{2,1}{}^2+\sqrt{-1})$ have no multiple roots, there exists $c\in \boldsymbol{Q}(\zeta_{2^n})^\times$ such that

$$f(v_{2,1})=c^2 v_{2,1}(v_{2,1}{}^2+\sqrt{-1}).$$

This contradicts that $f(v_{2,1})\in \boldsymbol{Q}[v_{2,1}]$. In the same way, if $F''=\boldsymbol{Q}(v_{2,j})$ for a certain j, then we have a contradiction.

(III) Suppose that A satisfies (3) in Proposition 2. Let $\gamma=\begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}\in SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})$. By N_γ we denote the normal subgroup of $H_n^{(1)}$ which is generated by $\bigcup_{\tau\in H_n^{(1)}}\tau^{-1}\gamma\tau$. Put

$$F'=\mathrm{fix}\,(A\cdot N_\gamma\cdot(H_n^{(2)}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))),$$

$$F''=\mathrm{fix}\,(A\cdot(H_n^{(2)}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))).$$

Then we see

$$\begin{aligned}[F:F'']=[F'':F']=[F':\boldsymbol{Q}(s)]=[F(\zeta_{2^n}):F''(\zeta_{2^n})]\\ =[F''(\zeta_{2^n}):F'(\zeta_{2^n})]=[F'(\zeta_{2^n}):\boldsymbol{Q}(s,\zeta_{2^n})]=2.\end{aligned}$$

The genus of $F''(\zeta_{2^n})$ is 0 (cf. Shimura [**9**]), and therefore the genus of $F'(\zeta_{2^n})$ is 0. Since $\det(A)=(\boldsymbol{Z}/2^n\boldsymbol{Z})^\times$, $F\cap\bar{\boldsymbol{Q}}=F'\cap\bar{\boldsymbol{Q}}=F''\cap\bar{\boldsymbol{Q}}=\boldsymbol{Q}$. Since

$$\begin{aligned}&r_{n,2}((A\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\cdot N_\gamma\cdot(H_n^{(2)}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})))\\ &=\left\langle\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix},\begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}\right\rangle,\end{aligned}$$

we have

$$F'(\zeta_{2^n})=\boldsymbol{Q}\left(s,\zeta_{2^n},\sqrt{\frac{e_0-e_2}{e_0-e_1}}\right).$$

Put $\dfrac{e_0-e_2}{e_0-e_1}=g(s)\{h(s)\}^2$, where $g(s)$ is an element of $\boldsymbol{Q}[s]$ with no multiple root and $h(s)$ is an element of $\boldsymbol{Q}(s)$. Since $[F':\boldsymbol{Q}(s)]=2$, there is an element $f(s)$ of $\boldsymbol{Q}[s]$ with no multiple root such that $F'=\boldsymbol{Q}(s,\sqrt{f(s)})$. Then we may assume that $c^2f(s)=g(s)$, where $c^2=\pm1$ or ±2. Hence

$$\omega=\sqrt{f(s)}\,h(s)=(1/c)\sqrt{\frac{e_0-e_2}{e_0-e_1}}\in F'\cap\mathfrak{S}.$$

Since the genus of F' is 0 and $(\bar{s},\overline{\sqrt{f(s)}})$ is a $\boldsymbol{Q}$-rational point on the curve $Y^2=f(X)$, there is an element $t\in F'$ such that $F'=\boldsymbol{Q}(t)$. Since

$$r_{n,2}((A\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\cdot(H_n^{(2)}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})))=\{\pm 1_2\},$$

we have

$$F''(\zeta_{2^n})=\boldsymbol{Q}\left(t,\zeta_{2^n},\sqrt{\frac{e_1-e_2}{e_1-e_0}}\right).$$

Hence in the same way as above, we have

$$F''=\boldsymbol{Q}(t,\ \nu_0)=\boldsymbol{Q}(v),$$

where $\nu_0=(1/c')\sqrt{\dfrac{e_1-e_2}{e_1-e_0}}$, and $c'^2=\pm 1$ or ± 2. Since

$$r_{n,3}((A\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}))\cdot(H_n^{(3)}\cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})))$$
$$=\left\langle\begin{pmatrix}1 & 0\\ 4 & 1\end{pmatrix},\ \begin{pmatrix}1+4 & 0\\ 0 & 1+4\end{pmatrix}\right\rangle\{\pm 1_2\},$$

we have

$$F(\zeta_{2^n})=\boldsymbol{Q}\left(v,\ \zeta_{2^n},\ \sqrt{\frac{f_1-e_2}{f_1-e_0}}\right),$$

where $\dfrac{f_1-e_2}{f_1-e_0}=\sqrt{\dfrac{e_1-e_2}{e_1-e_0}}$. On the other hand $\sqrt{\dfrac{e_1-e_2}{e_1-e_0}}=c'\nu_0$, where $\nu_0\in\boldsymbol{Q}(v)$. Noting $[F:\boldsymbol{Q}(v)]=[F:F'']=2$, we obtain $c'^2=\pm 1$ by Lemma 9. Then

$$F(\zeta_{2^n})=\boldsymbol{Q}(v,\ \zeta_{2^n},\ \sqrt{c'\nu_0})=\boldsymbol{Q}(v,\ \zeta_{2^n},\ \sqrt{\nu_0}),$$

so that

$$F=\boldsymbol{Q}(v,\ \nu),$$

where $\nu=(1/c'')\sqrt{\nu_0}$, and $c''^2=\pm 1$ or ± 2. We have

$$\omega^2=c^{-2}\left(\frac{e_0-e_2}{e_0-e_1}\right),$$
$$\nu^4=c''^{-4}\nu_0^2$$
$$=c''^{-4}c'^{-2}\left(\frac{e_1-e_2}{e_1-e_0}\right).$$

Since $\dfrac{e_0-e_2}{e_0-e_1}+\dfrac{e_1-e_2}{e_1-e_0}=1$, we have $c^2\omega^2+c''^4c'^2\nu^4=1$, where $c^2=\pm 1$ or ± 2, $c'^2=\pm 1$ and $c''^4=1$ or 4. Since $\omega,\ \nu\in F\cap\mathfrak{S}$, $(X,\ Y)=(\bar{\omega},\ \bar{\nu})$ is a finite $\boldsymbol{Q}$-rational point on the curve

$$c^2X^2+c''^4c'^2Y^4=1,$$

where $c^2=\pm 1$ or ± 2, and $c''^4c'^2=\pm 1$ or ± 4. If $c''^4c'^2=\pm 4$, then $\bar{\nu}=0$ by Lemma 7, and therefore $\overline{\left(\dfrac{e_1-e_2}{e_1-e_0}\right)}=0$. This contradicts that $E(a)$ is elliptic. If $c''^4c'^2=\pm 1$, then $\bar{\nu}=0$ or $\bar{\nu}^4=1$ by Lemma 7, and therefore $\overline{\left(\dfrac{e_1-e_2}{e_1-e_0}\right)}=0$ or 1. This contradicts that $E(a)$ is elliptic. We deduced a contradiction in any case of (I), (II), (III), and so complete the proof of Proposition 3.

By Proposition 3, we have obviously the following proposition.

PROPOSITION 4. *Let E satisfy the hypothesis of Theorem* 1, *and notations be* *as above. Then*

$$\mathrm{Gal}(\boldsymbol{Q}(E_{2^n})/\boldsymbol{Q}) \supset SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}) \cap H_n^{(6)},$$

for any integer $n \geqq 7$.

PROPOSITION 5. *Let* E *satisfy the hypothesis of Theorem* 1, *and notations be as above. Then*

$$\mathrm{Gal}(\boldsymbol{Q}(E_{2^n})/\boldsymbol{Q}) \supset H_n^{(7)},$$

for any integer $n \geqq 8$.

PROOF. Let n be an integer $\geqq 8$. Put $V = \mathrm{Gal}(\boldsymbol{Q}(E_{2^n})/\boldsymbol{Q})$. Assume that $V \not\supset H_n^{(n-1)}$. By Proposition 4,

$$V \cap H_n^{(6)} \supset H_n^{(6)} \cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}).$$

By Lemma 3, $r_{n,h+1}(V) \not\supset H_{h+1}^{(h)}$, for any h such that $2 \leqq h \leqq n-1$. For any integer h such that $6 \leqq h \leqq n-1$, since $r_{n,h+1}(V) \supset H_{h+1}^{(h)} \cap SL_2(\boldsymbol{Z}/2^{h+1}\boldsymbol{Z})$, we have

$$r_{n,h+1}(V \cap H_n^{(6)}) \cap H_{h+1}^{(h)} = H_{h+1}^{(h)} \cap SL_2(\boldsymbol{Z}/2^{h+1}\boldsymbol{Z}).$$

Therefore by Lemma 2,

$$|V \cap H_n^{(6)}| = |H_n^{(6)} \cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})|.$$

Hence

$$V \cap H_n^{(6)} = H_n^{(6)} \cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z}).$$

On the other hand, $V \cap H_n^{(6)} = \mathrm{Gal}(\boldsymbol{Q}(E_{2^n})/\boldsymbol{Q}(E_{2^6}))$. Let $\sigma \in V \cap H_n^{(6)} = H_n^{(6)} \cap SL_2(\boldsymbol{Z}/2^n\boldsymbol{Z})$. Then $\zeta_{2^n}^{\sigma} = \zeta_{2^n}^{\det(\sigma)} = \zeta_{2^n}$. So $\zeta_{2^n} \in \boldsymbol{Q}(E_{2^6})$. We have $\mathrm{Gal}(\boldsymbol{Q}(\zeta_{2^n})/\boldsymbol{Q}) \cong \mathrm{Gal}(\boldsymbol{Q}(E_{2^6})/\boldsymbol{Q})/\mathrm{Gal}(\boldsymbol{Q}(E_{2^6})/\boldsymbol{Q}(\zeta_{2^n}))$. If $\sigma \in \mathrm{Gal}(\boldsymbol{Q}(E_{2^6})/\boldsymbol{Q})/\mathrm{Gal}(\boldsymbol{Q}(E_{2^6})/\boldsymbol{Q}(\zeta_{2^n}))$, then $\sigma^{2^5} = 1$, since $\mathrm{Gal}(\boldsymbol{Q}(E_{2^6})/\boldsymbol{Q}) \subset H_6^{(1)}$. Since $\mathrm{Gal}((\boldsymbol{Q}(\zeta_{2^n})/\boldsymbol{Q}) \cong \boldsymbol{Z}/2\boldsymbol{Z} \oplus \boldsymbol{Z}/2^{n-2}\boldsymbol{Z}$, we have $n-2 \leqq 5$. Therefore if $n \geqq 8$, then $\mathrm{Gal}(\boldsymbol{Q}(E_{2^n})/\boldsymbol{Q}) \supset H_n^{(n-1)}$. Let $n \geqq 8$. Then

$$r_{n,8}(\mathrm{Gal}(\boldsymbol{Q}(E_{2^n})/\boldsymbol{Q})) = \mathrm{Gal}(\boldsymbol{Q}(E_{2^8})/\boldsymbol{Q}) \supset H_8^{(7)}.$$

Hence, by Lemma 3,

$$\mathrm{Gal}(\boldsymbol{Q}(E_{2^n})/\boldsymbol{Q}) \supset H_n^{(7)}.$$

We can now complete the proof of our Theorem. We have

$$\begin{aligned} r_8(\pi_2(G)) &= \pi_2(G)/(H^{(8)} \cap \pi_2(G)) \\ &= \mathrm{Gal}(\boldsymbol{Q}(E_{2^8})/\boldsymbol{Q}) \\ &\supset H_8^{(7)}, \end{aligned}$$

by Proposition 5, where G is the Galois group of $\bar{\boldsymbol{Q}}/\boldsymbol{Q}$, π_2 is the 2-adic representation attached to E, and r_8 is the natural homomorphism from $GL_2(\boldsymbol{Z}_2)$ to $GL_2(\boldsymbol{Z}/2^8\boldsymbol{Z})$. Since $\pi_2(G)$ is a closed subgroup of $GL_2(\boldsymbol{Z}_2)$, we obtain $\pi_2(G) \supset H^{(7)}$, by Lemma 4.

3. Proof of Theorem 2.

Let E be an elliptic curve defined over $\boldsymbol{Q}$, and $\underline{0}$ be the zero element of E. Assume that the points of order 2 are all $\boldsymbol{Q}$-rational, and E has a $\boldsymbol{Q}$-rational point of order 8. From Kubert [4], such elliptic curves are parametrized in the following way by variable α:

$$E(\alpha):\ y^2+(1-c)xy-by=x^3-bx^2,$$

where

$$b=(2d-1)(d-1),$$

$$c=(2d-1)(d-1)/d=b/d,$$

$$d=\alpha(8\alpha+2)/(8\alpha^2-1),$$

and

$$d(d-1)(2d-1)(8d^2-8d+1)$$
$$(=2\alpha(4\alpha+1)(2\alpha+1)(8\alpha^2+4\alpha+1)(8\alpha^2+8\alpha+1)^2/(8\alpha^2-1)^5)$$
$$\neq 0.$$

We consider $E(\alpha)$ as an elliptic curve with the zero element (∞, ∞), defined over the rational function field $\boldsymbol{Q}(\alpha)$ of one variable α over $\boldsymbol{Q}$. Then we may consider that $E=E(a)$ and $\underline{0}=(\infty, \infty)$, where $a\in\boldsymbol{Q}$, $\Delta=2a(4a+1)(2a+1)(8a^2+4a+1)(8a^2+8a+1)^2/(8a^2-1)^5\neq 0$, i.e., $E(a)$ is the elliptic curve obtained through the specialization $\alpha\to a$. We see that $(0, 0)$ is of order 8, $-2(0, 0)=(b, 0)$ and $-2(b, 0)=(d(d-1),\ d(d-1)^2)$ on $E(\alpha)$. Put

$$e_0=d(d-1)=2\alpha(4\alpha+1)(2\alpha+1)/(8\alpha^2-1)^2,$$

$$e_1=(4\alpha+1)(8\alpha^2+4\alpha+1)/16\alpha^2(8\alpha^2-1),$$

$$e_2=-2\alpha(2\alpha+1)(8\alpha^2+4\alpha+1)/(4\alpha+1)^2(8\alpha^2-1).$$

Then the points of order 2 on $E(\alpha)$ are

$$(e_i,\ -((1-c)e_i-b)/2) \qquad i=1, 2, 3.$$

Let $2u_0=(0, 0)$ and $8u_1=(e_1,\ -((1-c)e_1-b)/2)$. Then (u_0, u_1) is a base of $E(\alpha)_{2^4}$ over $\boldsymbol{Z}/2^4\boldsymbol{Z}$. Let identify $\mathrm{Gal}(\boldsymbol{Q}(\alpha, E(\alpha)_{2^4})/\boldsymbol{Q}(\alpha))$ with a subgroup of $GL_2(\boldsymbol{Z}/2^4\boldsymbol{Z})$ by taking the base (u_0, u_1). Then we can see easily that

$$\mathrm{Gal}(\boldsymbol{Q}(\alpha, E(\alpha)_{2^4})/\boldsymbol{Q}(\alpha))=\left\{\begin{pmatrix} a & b \\ c & d\end{pmatrix}\in H_4^{(1)}\ \middle|\ a\equiv 1,\ c\equiv 0 \bmod 2^3\right\},$$

$$\bar{\boldsymbol{Q}}\cap\boldsymbol{Q}(\alpha, E(\alpha)_{2^4})=\boldsymbol{Q}(\zeta_{2^4}).$$

Put

$$B=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in H_4^{(1)} \middle| a\equiv 1,\ c\equiv 0 \bmod 2^3\right\}.$$

PROPOSITION 6. *Let E be an elliptic curve defined over $\boldsymbol{Q}$. Let the points of order 2 on E be all $\boldsymbol{Q}$-rational, and E have a $\boldsymbol{Q}$-rational point of order 8. Then we have*

$$\mathrm{Gal}\,(\boldsymbol{Q}(E_{2^4})/\boldsymbol{Q})=B$$

with a suitable base of E_{2^4}.

PROOF. Let the notations be as above. Then we may assume that $E=E(a)$, where $a\in\boldsymbol{Q}$. By $\mathfrak{O}$ we denote the specialization ring of the specialization $\alpha\to a$ over $\boldsymbol{Q}$ and by $\mathfrak{p}$ the maximal ideal of $\mathfrak{O}$. Let $\mathfrak{S}$ be the integral closure of $\mathfrak{O}$ in $\boldsymbol{Q}(\alpha, E(\alpha)_{2^4})$, $\mathfrak{P}$ be a maximal ideal of $\mathfrak{S}$ lying above $\mathfrak{p}$. In what follows we regard $\bar{\boldsymbol{Q}}\supset\mathfrak{S}/\mathfrak{P}\supset\mathfrak{O}/\mathfrak{p}=\boldsymbol{Q}$. Let $V_{\mathfrak{P}}$ be the decomposition group of $\mathfrak{P}$. Then by the same reason as in the proof of Proposition 3 it is sufficient to prove that $V_{\mathfrak{P}}=B$. Assume that $V_{\mathfrak{P}}\neq B$. Since B is a 2-group, there exists a subgroup A of B such that $A\supset V_{\mathfrak{P}}$ and $[B:A]=2$. Put $F=\mathrm{fix}(A)$. Then by the same reason as in the proof of Proposition 3, we have $(F\cap\mathfrak{S})/(F\cap\mathfrak{P})=\boldsymbol{Q}$. Next we determine F. Since $[B:A]=2$, $A\supset B^2$, where B^2 is the group generated by $\{\sigma^2\}_{\sigma\in B}$. We have easily

$$B^2=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in H_4^{(2)} \middle| a=1,\ c=0,\ d\equiv 1 \bmod 2^3\right\}.$$

Put $K=\mathrm{fix}(B^2)$. Then u_0 and 2^2u_1 are K-rational, where $2u_0=(0,0)$ and $2\cdot 2^2u_1=(e_1, -((1-c)e_1-b)/2)$. By the assumption that the points of order 2 on $E(\alpha)$ are all $\boldsymbol{Q}(\alpha)$-rational, we see $\sqrt{0-e_0}$, $\sqrt{0-e_1}$, $\sqrt{e_1-e_0}$ and $\sqrt{e_1-e_2}\in K$, where

$$-e_0=-2\alpha(4\alpha+1)(2\alpha+1)/(8\alpha^2-1)^2,$$

$$-e_1=-(4\alpha+1)(8\alpha^2+4\alpha+1)/16\alpha^2(8\alpha^2-1),$$

$$e_1-e_0=-(4\alpha+1)^2/16\alpha^2(8\alpha^2-1)^2,$$

$$e_1-e_2=(8\alpha^2+4\alpha+1)^2(8\alpha^2+8\alpha+1)/16\alpha^2(4\alpha+1)^2(8\alpha^2-1).$$

Since $\det(B^2)=\langle 1+8\rangle\subset(\boldsymbol{Z}/2^4\boldsymbol{Z})^\times$, $\zeta_{2^3}\in K$. Therefore $\sqrt{-1}, \sqrt{2}\in K$. Since $[K:\boldsymbol{Q}(\alpha)]=[B:B^2]=2^8/2^3=2^5$, we have

$$K=\boldsymbol{Q}(\alpha,\ \sqrt{-1},\ \sqrt{2},\ \sqrt{\alpha(4\alpha+1)(2\alpha+1)},$$

$$\sqrt{(4\alpha+1)(8\alpha^2+4\alpha+1)(8\alpha^2-1)},$$

$$\sqrt{(8\alpha^2+8\alpha+1)(8\alpha^2-1)}).$$

Since $[B:A]=2$ and $A\supset B^2$, we have $[F:\boldsymbol{Q}(\alpha)]=2$ and $F\subset K$. Hence there is an element η of F such that $F=\boldsymbol{Q}(\alpha, \eta)$ and η^2 is one of the following:

(0) $i\ (\neq 1)$;

(1) $i(8\alpha^2-1)(8\alpha^2+8\alpha+1)$;

(2) $i\alpha(4\alpha+1)(2\alpha+1)$;

(3) $i(8\alpha^2-1)(8\alpha^2+4\alpha+1)(4\alpha+1)$;

(4) $i(8\alpha^2-1)(8\alpha^2+4\alpha+1)\alpha(2\alpha+1)$;

(5) $i\alpha(4\alpha+1)(2\alpha+1)(8\alpha^2-1)(8\alpha^2+8\alpha+1)$;

(6) $i(8\alpha^2+8\alpha+1)(8\alpha^2+4\alpha+1)(4\alpha+1)$;

(7) $i(8\alpha^2+8\alpha+1)(8\alpha^2+4\alpha+1)(2\alpha+1)\alpha$,

where i is one of 1, -1, 2 and -2. Since $\det(A)=\det(V_{\mathfrak{P}})=(\boldsymbol{Z}/2^4\boldsymbol{Z})^{\times}$, $\bar{\boldsymbol{Q}}\cap F=\boldsymbol{Q}$, so that η^2 is one of (1), (2), $\cdots$, (7). Let h be the image of η by the canonical map $\mathfrak{S}\to\mathfrak{S}/\mathfrak{P}$. Then (a, h) is $\boldsymbol{Q}$-rational, since $\eta\in F\cap\mathfrak{S}$. Next we shall prove that a is one of 0, $-1/4$ and $-1/2$, i.e., $\Delta=0$, so that we have a contradiction. In what follows, we suppose that a is not zero and it has a description $a=t/s$, where s and t are rational integers prime to each other with $s>0$. We can see easily that a common prime divisor of any two of s, t, $4t+s$, $2t+s$, $8t^2-s^2$, $8t^2+8ts+s^2$ and $8t^2+4ts+s^2$, if any, is 2.

(I) Suppose $\eta^2=(1)$. Then $(x, y)=(a, h)$ is a finite $\boldsymbol{Q}$-rational point of the curve $C(1, i)$:

$$y^2=i(8x^2-1)(8x^2+8x+1).$$

Assume that $i=1$ or -1. By Mordell [6] Chapter 10 Theorem 2, $C(1, 1)$ and $C(1, -1)$ are isomorphic to the curve:

$$Y^2=X^3-X.$$

Then by Lemma 8 we can determine the $\boldsymbol{Q}$-rational points of the curves $C(1, 1)$ and $C(1, -1)$, and we obtain that a is one of $-1/4$ and $-1/2$. Assume that $i=2$. Then $2(64t^4+64t^3s-8ts^3-s^4)$ is a square in $\boldsymbol{Q}$. Since

$$2(64t^4+64t^3s-8ts^3-s^4)\equiv -2s^4 \mod 4,$$

we have $s=2s'$, where s' is a rational integer. Hence $2(4t^4+8t^3s'-4ts'^3-s'^4)$ is a square in $\boldsymbol{Q}$. Since

$$2(4t^4+8t^3s'-4ts'^3-s'^4)\equiv -2s'^4 \mod 4,$$

we have $s'=2s''$, where s'' is a rational integer. Hence $2(t^4+4t^3s''-8ts''^3-4s''^4)$ is a square in $\boldsymbol{Q}$. Since

$$2(t^4+4t^3s''-8ts''^3-4s''^4)\equiv 2t^4 \qquad \mathrm{mod}\ 4\,,$$

we have $2|t$. This contradicts that s and t are prime to each other. By the above method, we have also a contradiction for the case where $i=-2$.

(II) Suppose $\eta^2=(2)$. If $i=1$, then (a, h) satisfies the equation: $h^2=a(4a+1)(2a+1)$. Therefore (a, h) satisfies the equation: $(8h)^2=(8a+2)^3-4(8a+2)$. By Lemma 8, $8a+2$ is one of 0, 2 and -2, so that a is one of $-1/4$ and $-1/2$. This result is also obtained in the same manner when i is one of -1, 2 and -2.

(III) Suppose $\eta^2=(5)$. Then (a, h) satisfies the equation:

$$h^2=ia(4a+1)(2a+1)(8a^2-1)(8a^2+8a+1)\,,$$

where i is one of 1, -1, 2 and -2. Then

$$s^8h^2=ist(4t+s)(2t+s)(8t^2-s^2)(8t^2+8ts+s^2)\,.$$

Hence we have

$$i'st(4t+s)(2t+s)=h'^2\,,$$

where i' is one of 1, -1, 2 and -2, h' is a rational integer. Then

$$h'^2/s^4=i'(t/s)(4t/s+1)(2t/s+1)$$
$$=i'a(4a+1)(2a+1)\,.$$

In the same way as in the case where $\eta^2=(2)$, we obtain that a is one of $-1/4$ and $-1/2$.

(IV) Suppose $\eta^2=(3)$ or (6). Then (a, h) satisfies the equation:

$$h^2=i(8a^2-1)(8a^2+4a+1)(4a+1)\,,$$

or the equation:

$$h^2=i(8a^2+8a+1)(8a^2+4a+1)(4a+1)\,.$$

Then

$$s^6h^2=i(8t^2-s^2)(8t^2+4ts+s^2)(4t+s)s$$

or

$$s^6h^2=i(8t^2+8ts+s^2)(8t^2+4ts+s^2)(4t+s)s\,.$$

Hence $s=q^2$ or $2q^2$, and $4t+s=\pm r^2$ or $\pm 2r^2$, where q and r are rational integers. Since $8t^2+4ts+s^2$ is positive, $8t^2+4ts+s^2=k^2$ or $2k^2$, where k is a rational integer. If $s=q^2$ and $4t+s=\pm r^2$, then $8t^2+4ts+s^2=(1/2)(q^4+r^4)$, so that $q^4+r^4=2k^2$ or $(2k)^2$. Then $2(k/q^2)^2-(r/q)^4=1$ or $(2k/q^2)^2-(r/q)^4=1$. By Lemma 7, $(r/q)^4=1$ or $r/q=0$. Therefore $4(t/s)+1=\pm 1$ or 0, so that $a=-1/2$ or $-1/4$. If $s=q^2$ and $4t+s=\pm 2r^2$, $8t^2+4ts+s^2=(1/2)(4r^4+q^4)$, so that $4r^4+q^4=2k^2$ or $(2k)^2$. Then $2(k/q^2)^2-4(r/q)^4=1$ or $(2k/q^2)^2-4(r/q)^4=1$. By Lemma 7, $r/q=0$. Therefore $a=-1/4$. If $s=2q^2$ and $4t+s=\pm r^2$, $8t^2+4ts+s^2=(1/2)(r^4+4q^4)$, ,so that $r^4+4q^4=2k^2$ or $(2k)^2$. Then $r=0$ or $q/r=0$. Therefore $a=-1/4$. If $s=2q^2$ and $4t+s=\pm 2r^2$, then

$8t^2+4ts+s^2=2q^4+2r^4$, so that $q^4+r^4=2(k/2)^2$ or k^2. Thus $a=-1/2$ or $-1/4$.

(V) Suppose $\eta^2=(4)$ or (7). Then (a, h) satisfies the equation:

$$h^2=i(8a^2-1)(8a^2+4a+1)a(2a+1),$$

or the equation:

$$h^2=i(8a^2+8a+1)(8a^2+4a+1)a(2a+1).$$

Then

$$s^6h^2=i(8t^2-s^2)(8t^2+4ts+s^2)(2t+s)t$$

or

$$s^6h^2=i(8t^2+8ts+s^2)(8t^2+4ts+s^2)(2t+s)t.$$

Hence $t=q^2$ or $2q^2$, and $2t+s=\pm r^2$ or $\pm 2r^2$, where q and r are rational integers. Since $8t^2+4ts+s^2$ is positive, we have $8t^2+4ts+s^2=k^2$ or $2k^2$, where k is a rational integer. If $t=q^2$ and $2t+s=\pm r^2$, then $8t^2+4ts+s^2=r^4+4q^4=k^2$ or $2k^2$. Then $r=0$ or $q/r=0$, by Lemma 7. Therefore $a=-1/2$. If $t=q^2$ and $2t+s=\pm 2r^2$, then $8t^2+4ts+s^2=4q^4+4r^4$, so that $q^4+r^4=(k/2)^2$ or $2(k/2)^2$. Then $(r/q)^4=1$ or $r/q=0$, by Lemma 7. Therefore $a=-1/2$ or $-1/4$. If $t=2q^2$ and $2t+s=\pm r^2$, $8t^2+4ts+s^2=r^4+(2q)^4=k^2$ or $2k^2$. Then $(r/2q)^4=1$ or $r/2q=0$. Therefore $a=-1/4$ or $-1/2$. If $t=2q^2$ and $2t+s=\pm 2r^2$, then $8t^2+4ts+s^2=4r^4+(2q)^4=k^2$ or $2k^2$. We get $a=-1/2$, since $r/2q=0$ by Lemma 7. Hence we have that a is $-1/4$ or $-1/2$. Consequently we obtain Proposition 6.

We can now complete the proof of Theorem 2. Let notations be as above. Let $E=E(a)$, and (ξ_0, ξ_1) be a base of $T_2(E)$ such that the projection of ξ_i to E_{2^4} is $\bar{u}_i$ $(i=0, 1)$. With the base (ξ_0, ξ_1), we identify $\pi_2(G)$ as a subgroup of $GL_2(\boldsymbol{Z}_2)$. By Proposition 7,

$$\begin{aligned} r_4(\pi_2(G)) &= \mathrm{Gal}\,(\boldsymbol{Q}(E_{2^4})/\boldsymbol{Q}) \\ &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H_4^{(1)} \,\middle|\, a\equiv 1,\ c\equiv 0 \mod 2^3 \right\} \\ &\supset H_4^{(3)}. \end{aligned}$$

Then $\pi_2(G)\supset H^{(3)}$, by Lemma 4. These imply Theorem 2.

References

[1] B.J. Birch and H.P.F. Swinnerton-Dyer, Notes on elliptic curves I, J. Reine Angew. Math., **212** (1963), 7-25.

[2] J.W.S. Cassels, Diophantine equations with special reference to elliptic curves, J. London Math. Soc., **41** (1966), 193-291.

[3] L.E. Dickson, History of the theory of numbers II, 1934.

[4] D. Kubert, Universal bounds on the torsion of elliptic curves, Proc. London Math. Soc., (3), **33** (1976), 193-237.

[5] S. Lang, Algebraic number theory, Addison-Wesley, 1970.

[6] L.J. Mordell, Diophantine equations, Academic Press, 1969.
[7] J.-P. Serre, Abelian l-adic representations and elliptic curves, Benjamin, Addison-Wesley, 1968.
[8] J.-P. Serre, Points rationnels des courbes modulaires $X_0(N)$, Séminaire Bourbaki, 30e année, 1977/1978, n°511.
[9] G. Shimura, Introduction to the arithmetic theory of automorphic functions, Iwanami Shoten and Princeton University Press, 1971.

Kumiko NISHIOKA
Department of Mathematics
Nara Women's University
Kita-uoya Nishimachi
Nara 630, Japan