Local fields generated by 3-division points of elliptic curves

By Hirotada NAITO

Department of Mathematics, Kagawa University, 1-1, Saiwai-cho, Takamatsu, Kagawa 760-8522

(Communicated by Shokichi IYANAGA, M. J. A., Nov. 12, 2002)

Abstract: We determine all the extensions generated by 3-division points of elliptic curves over the fields of p-adic numbers. As application, we construct $GL_2(\mathbf{F}_3)$-extensions over the field of rational numbers with given finitely many local conditions.

Key words: Elliptic curves; local fields; Galois theory.

1. Introduction. Let E be an elliptic curve defined over the field $\mathbf{Q}$ of rational numbers. We denote by E_l the set of l-division points of E for a prime l. We put $K_{(l)} = \mathbf{Q}(E_l)$. We denote by $G_{(l)} = \mathrm{Gal}(K_{(l)}/\mathbf{Q})$ the Galois group of $K_{(l)}$ over $\mathbf{Q}$. We think that $G_{(l)}$ is a subgroup of the general linear group $GL_2(\mathbf{F}_l)$ of degree 2 over the finite field $\mathbf{F}_l$ of l elements, because E_l is isomorphic to a vector space of dimension 2 over $\mathbf{F}_l$.

We know that the action of $\sigma \in G_{(l)} \subset GL_2(\mathbf{F}_l)$ on an l-th primitive root ζ_l of unity is determined by $\zeta_l^\sigma = \zeta_l^{\det \sigma}$. Thus we see that the fixed field of $G_{(l)} \cap SL_2(\mathbf{F}_l)$ is $\mathbf{Q}(\zeta_l)$, where SL_2 is the special linear group of degree 2.

We denote by $L(s, E/\mathbf{Q}) = \sum_{n=1}^{\infty} a_n n^{-s}$ the Hasse-Weil zeta function of E over $\mathbf{Q}$. We know that a_p mostly describes the decomposition law of a prime p of $K_{(l)}/\mathbf{Q}$ (cf. Shimura [9]).

For example in the case of $l = 2$, Koike [3] proved that $a_p \equiv b_p \bmod 2$ for good primes $p \neq 2$, where $L(s, \rho, K_{(2)}/\mathbf{Q}) = \sum_{n=1}^{\infty} b_n n^{-s}$ is the Artin L-function for the 2-dimensional irreducible representation ρ of $GL_2(\mathbf{F}_2)$. Naito [7] got a similar result in the case of $l = 3$. In the case of $l = 2$, $GL_2(\mathbf{F}_2)$ is isomorphic to the symmetric group $\mathfrak{S}_3$ of degree 3. Let $K/\mathbf{Q}$ be a Galois extension whose Galois group is isomorphic to $\mathfrak{S}_3$. We can find a polynomial $f(X)$ of degree 3 with rational coefficients such that K is the decomposition field over $\mathbf{Q}$ of $f(X) = 0$. Let E be the elliptic curve defined by $y^2 = f(x)$. We see $K = \mathbf{Q}(E_2)$. Therefore the theorem of Koike [3] is regarded as a decomposition law of primes of Galois extensions whose Galois groups are isomorphic to $\mathfrak{S}_3$. Next we consider the case of $l = 3$. Let $K/\mathbf{Q}$ be a Galois extension whose Galois group is isomorphic to $GL_2(\mathbf{F}_3)$. When is there an elliptic curve E defined over $\mathbf{Q}$ such that $K = \mathbf{Q}(E_3)$? We see that a necessary condition for existence of such an elliptic curve is that K contains a certain cubic root by considering the equation of x-coordinates of 3-division points. Lario and Rio [4, 5] got some sufficient conditions.

We consider local cases in this note. Let K_p be a Galois extension over the field $\mathbf{Q}_p$ of p-adic numbers for a prime p whose Galois group $\mathrm{Gal}(K_p/\mathbf{Q}_p)$ is isomorphic to a subgroup G of $GL_2(\mathbf{F}_3)$. From now on, we call such a Galois extension a G-extension, for simplicity. We determine all such K_p which contains ζ_3 with $\zeta_3^\sigma = \zeta_3^{\det \sigma}$ for $\sigma \in \mathrm{Gal}(K_p/\mathbf{Q}_p) \subset GL_2(\mathbf{F}_3)$. Recently Bayer and Rio [1] determined all such extensions over $\mathbf{Q}_2$ without the condition $\zeta_3^\sigma = \zeta_3^{\det \sigma}$. They also computed irreducible equations and the discriminants of those fields.

Next we examine whether there exists an elliptic curve E such that $K_p = \mathbf{Q}_p(E_3)$. We get such curves satisfying some congruence conditions in possible cases. We get two examples K_2 such that there exists no elliptic curve E over $\mathbf{Q}_2$ satisfying $K_2 = \mathbf{Q}_2(E_3)$.

As application of these results, we can construct infinitely many $GL_2(\mathbf{F}_3)$-extensions over $\mathbf{Q}$ satisfying decomposing conditions for given finitely many primes by using these results in local cases.

2. Results in local cases. We list all subgroups G of $GL_2(\mathbf{F}_3)$ up to conjugacy. The order of G is divisible by 3 in (1), …, (4-2) and (5). That in other cases is not divisible by 3. We remark that the order of $GL_2(\mathbf{F}_3)$ is $48 = 2^4 \cdot 3$. We denote by C_n (resp. D_n) the cyclic group (resp. the dihedral group) of order n. In each case, we list all Galois extensions

2000 Mathematics Subject Classification. 11F85, 11G05, 11G07.

K_p containing ζ_3 whose Galois group $\mathrm{Gal}(K_p/\mathbf{Q}_p)$ is isomorphic to G satisfying $\zeta_3^\sigma = \zeta_3^{\det\sigma}$ for $\sigma \in \mathrm{Gal}(K_p/\mathbf{Q}_p)$. At last we give elliptic curves E such that $K_p = \mathbf{Q}_p(E_3)$ in the possible cases. In only two extensions for $p = 2$ in (6), there exists no such elliptic curve.

Let $K/\mathbf{Q}_p$ be a Galois extension. We put F the maximal unramified extension in $K/\mathbf{Q}_p$. We see that $F/\mathbf{Q}_p$ is a cyclic extension. We put $e = [K : F]$ and $f = [F : \mathbf{Q}_p]$. If $K/\mathbf{Q}_p$ is tamely ramified, K/F is a cyclic extension and e divides $p^f - 1$. Therefore it is easy to list all G-extensions in the cases of $p \neq 2, 3$. We see by $\zeta_3 \in K$ and $\zeta_3^\sigma = \zeta_3^{\det\sigma}$ that G is contained in $SL_2(\mathbf{F}_3)$ if and only if $p \equiv 1 \bmod 3$.

We define an elliptic curve E by the equation

$$dy^2 = 4x^3 - g_2x - g_3, \quad (d, g_2, g_3 \in \mathbf{Z}_p),$$

where $\mathbf{Z}_p$ is the ring of p-adic integers. The equation of x-coordinates of E_3 is as follows:

$$\begin{aligned} f(x) &= x^4 - \frac{g_2}{2}x^2 - g_3x - \frac{{g_2}^2}{48} \\ &= \left(x^2 - \sqrt{\frac{g_2-\Delta^{1/3}}{3}}x - \frac{2\Delta^{1/3}+g_2}{12} - \frac{g_3}{2\sqrt{\frac{g_2-\Delta^{1/3}}{3}}}\right) \\ &\times \left(x^2 + \sqrt{\frac{g_2-\Delta^{1/3}}{3}}x - \frac{2\Delta^{1/3}+g_2}{12} + \frac{g_3}{2\sqrt{\frac{g_2-\Delta^{1/3}}{3}}}\right) \\ &= 0, \end{aligned}$$

where $\Delta = {g_2}^3 - 27{g_3}^2$.

Therefore x-coordinates of 3-division points are independent on d. Moreover we see that $\Delta^{1/3}$ is contained in the field generated by all the x-coordinates of E_3.

Now we describe data. We use α and β as p-adic units in this section.

(1) $G = GL_2(\mathbf{F}_3)$. We see that this case occurs in only $p = 2$ by considering a ramification. Weil [10] proved that there exist three Galois extensions $M/\mathbf{Q}_2$ whose Galois groups are isomorphic to the symmetric group $\mathfrak{S}_4$ of degree 4, which is isomorphic to $GL_2(\mathbf{F}_3)/\{\pm 1\}$. Such fields are

$$M_1 = \mathbf{Q}_2\left(\zeta_3, \sqrt[3]{2}, \sqrt{3(1+\sqrt[3]{2})}\right),$$

$$M_2 = \mathbf{Q}_2\left(\zeta_3, \sqrt[3]{2}, \sqrt{1+\sqrt[3]{2}^2}\right)$$

and

$$M_3 = \mathbf{Q}_2\left(\zeta_3, \sqrt[3]{2}, \sqrt{3(3+\sqrt[3]{2}+\sqrt[3]{2}^2)}\right).$$

M_1 and M_2 have four quadratic extensions K whose Galois group over $\mathbf{Q}_2$ are isomorphic to $GL_2(\mathbf{F}_3)$ respectively. But M_3 has no such extension. Furthermore he gave elliptic curves E satisfying $K = \mathbf{Q}_2(E_3)$. We give another elliptic curves in this note. We see that M_1 is generated by the x-coordinates of 3-division points of the elliptic curve with $g_2 = 2\alpha$ ($\alpha \equiv 3 \bmod 4$) and $g_3 = 2\beta$, and M_2 is similarly generated with $g_2 = 2^2\alpha$ ($\alpha \equiv 3 \bmod 4$) and $g_3 = 2^2\beta$. We can construct four K by taking d as $d \equiv 1, 3 \bmod 2^3$ and $d \equiv 2, 6 \bmod 2^4$, respectively.

(2) $G = SL_2(\mathbf{F}_3)$. It must be $p \equiv 1 \bmod 3$. But we see that this case occurs in the case of $p = 2$ by considering a ramification. So it never occurs.

(3) $G = B = \left\{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \in GL_2(\mathbf{F}_3)\right\}$. B is isomorphic to the dihedral group D_{12} of order 12. It must be $p \not\equiv 1 \bmod 3$. In $p \neq 2, 3$, $K = \mathbf{Q}_p(\zeta_3, \sqrt[6]{p})$ is the only one D_{12}-extension. We get an elliptic curve E by putting $g_2 = p^2\alpha$, $g_3 = p\beta$ and $d \not\equiv 0 \bmod p$ satisfying $K = \mathbf{Q}_p(E_3)$. We remark that a D_{12}-extension is the compositum of an $\mathfrak{S}_3$-extension and a quadratic extension. Hence we simultaneously deal the case of $p = 2, 3$ in (4-1).

(4-1) $G = \left\{\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbf{F}_3)\right\}$ or $\left\{\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \in GL_2(\mathbf{F}_3)\right\}$. Both of them are isomorphic to $\mathfrak{S}_3$. It must be $p \not\equiv 1 \bmod 3$. In $p \neq 2, 3$, $K = \mathbf{Q}_p(\zeta_3, \sqrt[3]{p})$ is the only one $\mathfrak{S}_3$-extension. We get an elliptic curve E satisfying $K = \mathbf{Q}_p(E_3)$ by putting $g_2 = p^3\alpha$, $g_3 = p^2\beta$ and $d \not\equiv 0 \bmod p$, where $-\beta \bmod p$ is a quadratic residue. If $d \bmod p$ is a quadratic residue, the Galois group of $\mathbf{Q}_p(E_3)/\mathbf{Q}_p$ is $\left\{\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}\right\}$. Otherwise it is $\left\{\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}\right\}$.

In $p = 3$, there exist four $\mathfrak{S}_3$-extensions K containing ζ_3. They are $K = \mathbf{Q}_3(\zeta_3, \sqrt[3]{2})$, $\mathbf{Q}_3(\zeta_3, \sqrt[3]{3})$, $\mathbf{Q}_3(\zeta_3, \sqrt[3]{6})$ and $\mathbf{Q}_3(\zeta_3, \sqrt[3]{12})$. Each $\mathfrak{S}_3$-extension over $\mathbf{Q}_3$ is extended to only one D_{12}-extension. By putting $g_2 = 3^3\alpha$ and $g_3 \equiv 2 \bmod 3^2$, we get a $\left\{\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}\right\}$-extension (resp. $\left\{\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}\right\}$-extension, D_{12}-extension), if $d \equiv 1 \bmod 3$ (resp. $d \equiv -1 \bmod 3$, $d \equiv 3 \bmod 3^2$). These extensions contain $\mathbf{Q}_3(\zeta_3, \sqrt[3]{2})$. By putting $g_2 = 3^4\alpha$ and $g_3 = 3\beta$, we get a $\left\{\begin{pmatrix}1 & *\\ 0 & *\end{pmatrix}\right\}$-extension (resp. $\left\{\begin{pmatrix}* & *\\ 0 & 1\end{pmatrix}\right\}$-extension, D_{12}-extension), if $d \equiv 0 \bmod 3$, $d \not\equiv 0 \bmod 3^2$ and $-3\beta/d \equiv 1 \bmod 3$ (resp. $d \equiv 0 \bmod 3$, $d \not\equiv 0 \bmod 3^2$ and $-3\beta/d \equiv -1 \bmod 3$, $d \equiv -\beta \bmod 3$). We see that these extensions contain $\mathbf{Q}_3(\zeta_3, \sqrt[3]{3})$ (resp. $\mathbf{Q}_3(\zeta_3, \sqrt[3]{6})$, $\mathbf{Q}_3(\zeta_3, \sqrt[3]{12})$) if $\beta \equiv 1 \bmod 3^2$ (resp. $\beta \equiv 2 \bmod 3^2$, $\beta \equiv 4 \bmod 3^2$).

In $p = 2$, $\mathbf{Q}_2(\zeta_3, \sqrt[3]{2})$ is the only one $\mathfrak{S}_3$-extension. Then all D_{12}-extensions are $\mathbf{Q}_2(\zeta_3, \sqrt[3]{2}, \sqrt{-1})$, $\mathbf{Q}_2(\zeta_3, \sqrt[3]{2}, \sqrt{2})$ and $\mathbf{Q}_2(\zeta_3, \sqrt[3]{2}, \sqrt{-2})$. We put $g_2 = 2^4\alpha$ and $g_3 = 2\beta$. We see that $\mathbf{Q}_2(E_3)$ is a D_{12}-extension $\mathbf{Q}_2(\zeta_3, \sqrt[3]{2}, \sqrt{-1})$ (resp. a $\left\{\begin{pmatrix}1 & *\\ 0 & *\end{pmatrix}\right\}$-extension, $\left\{\begin{pmatrix}* & *\\ 0 & 1\end{pmatrix}\right\}$-extension) for $d \equiv 2\beta \bmod 2^4$ (resp. $d \equiv -2\beta \bmod 2^4$, $d \equiv 6\beta \bmod 2^4$). We see $\mathbf{Q}_2(E_3) = \mathbf{Q}_2(\zeta_3, \sqrt[3]{2}, \sqrt{2})$ (resp. $\mathbf{Q}_2(\zeta_3, \sqrt[3]{2}, \sqrt{-2})$) for $d \equiv -\beta \bmod 2^3$ (resp. $d \equiv \beta \bmod 2^3$).

(4-2) $G = \left\langle \begin{pmatrix}-1 & -1\\ 0 & -1\end{pmatrix} \right\rangle$. It is isomorphic to C_6.

(5) $G = \left\langle \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \right\rangle$. It is isomorphic to C_3.

These two cases occur in $p \equiv 1 \bmod 3$. There are four C_3-extensions. They are $\mathbf{Q}_p(\sqrt[3]{\delta})$, $\mathbf{Q}_p(\sqrt[3]{p})$, $\mathbf{Q}_p(\sqrt[3]{\delta p})$ and $\mathbf{Q}_p(\sqrt[3]{\delta^2 p})$, where δ is a p-adic unit such that $\delta \bmod p$ is not a cubic residue. Each C_6-extension is the compositum of a C_3-extension and a quadratic extension. There are three quadratic extensions, $\mathbf{Q}_p(\sqrt{\gamma})$, $\mathbf{Q}_p(\sqrt{p})$ and $\mathbf{Q}_p(\sqrt{\gamma p})$, where γ is a p-adic unit such that $\gamma \bmod p$ is not a quadratic residue. We put $g_2 = p\alpha$ and $g_3 = \beta$, where $\beta \bmod p$ is not a cubic residue. We see that $\mathbf{Q}_p(\sqrt[3]{\delta})$ coincides with the field generated by x-coordinates of E_3. We see that $\mathbf{Q}_p(E_3)$ is a C_3-extension $\mathbf{Q}_p(\sqrt[3]{\delta})$, if $-\beta/d \bmod p$ is a quadratic residue. We also see that $\mathbf{Q}_p(E_3)$ is a C_6-extension containing $\mathbf{Q}_p(\sqrt{\gamma})$ (resp. $\mathbf{Q}_p(\sqrt{p})$, $\mathbf{Q}_p(\sqrt{\gamma p})$), if $-\beta/d \bmod p$ is not a quadratic residue (resp. $-\beta/d \equiv p \bmod p^2$, $-\beta/d \equiv \gamma p \bmod p^2$). We put $g_2 = p^3\alpha$ and $g_3 = p^2\beta$. We see that the extension generated by x-coordinates of E_3 is $\mathbf{Q}_p(\sqrt[3]{p})$ (resp. $\mathbf{Q}_p(\sqrt[3]{\delta p})$, $\mathbf{Q}_p(\sqrt[3]{\delta^2 p})$), for $\beta \equiv 1 \bmod p$ (resp. $\beta \equiv \delta \bmod p$, $\beta \equiv \delta^2 \bmod p$). If $-\beta/d \bmod p$ is a quadratic residue, $\mathbf{Q}_p(E_3)$ is a C_3-extension. If $-\beta/d \bmod p$ is not a quadratic residue, $\mathbf{Q}_p(E_3)$ is a C_6-extension containing $\mathbf{Q}_p(\sqrt{\gamma})$. If $-d/\beta \equiv p \bmod p^2$ (resp. $-d/\beta \equiv p\gamma \bmod p^2$), $\mathbf{Q}_p(E_3)$ is a C_6-extension containing $\mathbf{Q}_p(\sqrt{p})$ (resp. $\mathbf{Q}_p(\sqrt{\gamma p})$).

(6) $G = \left\langle a = \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix},\ b = \begin{pmatrix}-1 & 0\\ 1 & 1\end{pmatrix} \right\rangle$ with $a^8 = b^2 = 1$, $b^{-1}ab = a^3$. It is isomorphic to the semi-dihedral group SD_{16} of order 16. We see that this case occurs in only $p = 2$ by considering a ramification. Let K be an SD_{16}-extension. Let M be the $\langle a^4 \rangle$-fixed subfield of $K/\mathbf{Q}_p$. We see that M is a D_8-extension over $\mathbf{Q}_2$. Naito [6] determined all such extensions. By the action of the Galois group on ζ_3, K must be a cyclic extension of degree 8 over a quadratic field other than $\mathbf{Q}_2(\zeta_3)$. We see that M is a cyclic extension over k. We see $k = \mathbf{Q}_2(\sqrt{-1})$ or $\mathbf{Q}_2(\sqrt{-5})$ by Naito [6].

By local class field theory and computation of $k^\times/(k^\times)^8$, where $k = \mathbf{Q}_2(\sqrt{-1})$ or $\mathbf{Q}_2(\sqrt{-5})$, we can determine all D_8-extensions M which have quadratic extensions K which are cyclic of degree 8 over $\mathbf{Q}_2(\sqrt{-1})$ (resp. $\mathbf{Q}_2(\sqrt{-5})$) such that $\mathrm{Gal}(K/\mathbf{Q}_2) \cong SD_{16}$. These are $M = \mathbf{Q}_2\left(\sqrt{3+2\sqrt{-5}}, \sqrt{5}\right)$, $\mathbf{Q}_2\left(\sqrt{4+\sqrt{-5}}, \sqrt{5}\right)$ (resp. $\mathbf{Q}_2\left(\sqrt{3+2\sqrt{-1}}, \sqrt{5}\right)$, $\mathbf{Q}_2\left(\sqrt{2+\sqrt{-1}}, \sqrt{5}\right)$).

The compositum of two SD_{16}-extensions whose intersection is a D_8-extension is an $SD_{16} \times C_2$-extension. If there exists an SD_{16}-extension containing M, we find another SD_{16}-extension in the compositum of it and a quadratic extension over $\mathbf{Q}_2$.

If $K = \mathbf{Q}_2(E_3)$ for an elliptic curve E, we see that M is the field generated by all the x-coordinates of E_3. We put $g_2 = 2^a\alpha$ and $g_3 = 2^b\beta$.

In the first place, we consider the case of $3a < 2b$. We get SD_{16}-extensions K which are cyclic over $\mathbf{Q}_2(\sqrt{-1})$ in the case of $2b - 3a \geq 3$. We get $M = \mathbf{Q}_2\left(\sqrt{3+2\sqrt{-5}}, \sqrt{5}\right)$ (resp. $M = \mathbf{Q}_2\left(\sqrt{4+\sqrt{-5}}, \sqrt{5}\right)$) by putting $a = 2$, $b = 5$ and $\alpha \equiv 1 \bmod 2^3$ (resp. $a = 1$, $b = 4$ and $\alpha \equiv \pm 1 \bmod 2^3$). We get two SD_{16}-extensions by putting $d \equiv \pm 1 \bmod 2^2$ or $d \equiv 2 \bmod 2^2$ in each case. We get all SD_{16}-extensions which are cyclic over $\mathbf{Q}_2(\sqrt{-1})$. We get SD_{16}-extensions K which are cyclic over $\mathbf{Q}_2(\sqrt{-5})$ in the case of $2b - 3a = 2$. We get $M = \mathbf{Q}_2\left(\sqrt{3+2\sqrt{-1}}, \sqrt{5}\right)$ for any 2-adic integers α and β. We get two SD_{16}-extensions by putting $d \equiv \pm 1 \bmod 2^2$ or $d \equiv 2 \bmod 2^2$, respectively. We see $[\mathbf{Q}_2(E_3) : \mathbf{Q}_2] \leq 8$ in the case of $2b - 3a = 1$, where we denote by $[\mathbf{Q}_2(E_3) : \mathbf{Q}_2]$ the degree of $\mathbf{Q}_2(E_3)/\mathbf{Q}_2$.

In the second place, we consider the case of $3a > 2b$. We see that b is divisible by 3, if and only if

$\Delta^{1/3} \in \mathbf{Q}_2$. We see $[\mathbf{Q}_2(E_3) : \mathbf{Q}_2] \leq 8$ in the case of $a - (2/3)b \geq 2$. In the case of $a - (2/3)b = 1$, we get SD_{16}-extensions which are cyclic over $\mathbf{Q}_2(\sqrt{-5})$ (resp. $\mathbf{Q}_2(\sqrt{-1})$) for $\alpha \equiv -1 \bmod 2^2$ (resp. $\alpha \equiv 1 \bmod 2^2$). We get $M = \mathbf{Q}_2\left(\sqrt{3+2\sqrt{-1}}, \sqrt{5}\right)$ for $\alpha \equiv -1 \bmod 2^2$.

In the last place, we consider the case of $3a = 2b$. We see that $\Delta^{1/3} \in \mathbf{Q}_2$ if and only if $\alpha^3 - 27\beta^2 = 2^{3c}\gamma$ for a positive integer c and a 2-adic unit γ. By calculating $f(x)$, we see that $\sqrt{2+\sqrt{-1}}$ never appear in the field generating by x-coordinates of E_3.

Therefore these two SD_{16}-extensions which contain $\mathbf{Q}_2\left(\sqrt{2+\sqrt{-1}}, \sqrt{5}\right)$ never coincide with $\mathbf{Q}_2(E_3)$ for any elliptic curves E.

(7-1) $G = \left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle$. It is isomorphic to C_8. This case occurs in $p \equiv 2 \bmod 3$. The compositum of two C_8-extensions whose intersection is a C_4-extension is a $C_8 \times C_2$-extension. Therefore we find another C_8-extension containing the same C_4-extension by composing a quadratic extension over $\mathbf{Q}_p$.

For $p \equiv 1 \bmod 4$, there exist four C_8-extensions. We construct two C_4-extensions by adding x-coordinates of E_3. By putting $g_2 = p\alpha$ and $g_3 = p^3\beta$, the field generated by x-coordinates of E_3 is a C_4-extension. We get two C_8-extension by taking d as a p-adic unit and a prime element, respectively. We also get another C_4-extension by putting $g_2 = \alpha$ and $g_3 = p^2\beta$. We see that it is unramified over $\mathbf{Q}_p$. We get an unramified C_8-extension by taking a p-adic unit d such that $d \bmod p$ is a quadratic residue. We also get another C_8-extension by taking d as a prime element.

For $p \equiv 3 \bmod 4$, there exist two C_8-extensions. We can prove that there exist $\alpha, u \in \mathbf{F}_p^\times$ ($\alpha \neq u$) such that $\alpha^3 - u^3$ is a quadratic residue but not $\alpha - u$. By putting $g_2 \equiv \alpha \bmod p$ and $g_3 \equiv \beta \bmod p$, we get two C_8-extensions, where β satisfies $27\beta^2 \equiv \alpha^3 - u^3 \bmod p$. We remark that it is unramified by taking d as $d \bmod p$ is a quadratic residue. We also get another C_8-extension by taking d as a prime element.

For $p = 2$, there are eight C_8-extensions. By putting $g_2 = 2\alpha$ ($\alpha \equiv 1 \bmod 2^3$) and $g_3 = 2^2\beta$, we get a C_4-extension by adding x-coordinates of E_3. We also get the unramified C_4-extension by putting $g_2 = 2^2\alpha$ ($\alpha \equiv 1 \bmod 2^2$) and $g_3 = \beta$ ($\beta \equiv \pm 1 \bmod 2^3$). We get four C_8-extensions $\mathbf{Q}_2(E_3)$ by taking $d \equiv 1 \bmod 2^3$, $d \equiv -1 \bmod 2^3$, $d \equiv 2 \bmod 2^4$ and $d \equiv -2 \bmod 2^4$, respectively in each case.

(7-2) $G = \left\langle a = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}, \ b = \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle$ with $a^4 = b^2 = 1$, $b^{-1}ab = a^{-1}$. It is isomorphic to the dihedral group D_8 of degree 8. This case occurs in $p \equiv 2 \bmod 3$. Moreover we see $p \equiv 3 \bmod 4$ or $p = 2$ by Naito [6]. In $p \neq 2$, by putting $g_2 = p\alpha$, $g_3 = p^3\beta$ and $d \not\equiv 0 \bmod p$, we see that $\mathbf{Q}_p(E_3)$ is a D_8-extension. We know by Naito [6] that there exists only one D_8-extension for $p \equiv 3 \bmod 4$. For $p = 2$, there exist eighteen D_8-extensions. By putting $g_2 = 2\alpha$ ($\alpha \equiv -1 \bmod 2^3$) and $g_3 = 2^2\beta$, we get two D_8-extension $\mathbf{Q}_2(E_3)$ for $d \equiv 1 \bmod 2^3$, $d \equiv -1 \bmod 2^3$, respectively. They are $\mathbf{Q}_2\left(\zeta_3, \sqrt{\sqrt{-2}(1+\sqrt{-2})}\right)$ and $\mathbf{Q}_2\left(\zeta_3, \sqrt{\sqrt{-2}(1+3\sqrt{-2})}\right)$. Other D_8-extentions do not satisfy the condition $\zeta_3^\sigma = \zeta_3^{\det \sigma}$.

(7-3) $G = SD_{16} \cap SL_2(\mathbf{F}_3)$. It is isomorphic to the quaternion group Q_8 of order 8. It occurs in $p \equiv 1 \bmod 3$. Fujisaki [2] proved that p satisfies $p \equiv 3 \bmod 4$ or $p = 2$ and that there exists only one Q_8-extension for odd prime p. He explicitly constructed them. By putting $g_2 = p\alpha$ and $g_3 = p^3\beta$, we see that $\mathbf{Q}_p(E_3)$ is the Q_8-extension.

(8-1) $G = \left\langle \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \right\rangle$. It is isomorphic to C_4. It occurs in $p \equiv 1 \bmod 3$. For $p \equiv 3 \bmod 4$, there exist two C_4-extensions. By putting $g_2 = \alpha$ and $g_3 = p^2\beta$ such that $(1 - \zeta_3/3)\alpha \bmod p$ is a quadratic residue, we get an unramified C_4-extension $\mathbf{Q}_p(E_3)$ for a p-adic unit d such that $d \bmod p$ is a quadratic residue. We get another C_4-extension for a prime element d. For $p \equiv 1 \bmod 4$, there exist six C_4-extensions. By putting $g_2 = \alpha$ and $g_3 = p^2\beta$, where $\alpha \bmod p$ is not a quadratic residue, we get an unramified C_4-extension $\mathbf{Q}_p(E_3)$ for a p-adic unit d, which is a quadratic residue of modulo p. We get another C_4-extension for a prime element d. By putting $g_2 = p\alpha$ and $g_3 = p^3\beta$, we get a C_4-extension $\mathbf{Q}_p(E_3)$. We get four such extensions as we take $\alpha \bmod p$ and $d \bmod p$ to be a quadratic residue or not respectively.

(8-2) $G = \left\langle \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle$. It is isomorphic to $C_2 \times C_2$.

(9-1) $G = \left\langle \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle$. It is isomorphic to C_2.

These two cases occur in $p \equiv 2 \bmod 3$ or $p = 3$. For an odd prime $p \equiv 2 \bmod 3$, we put $g_2 = p^2\alpha$ and $g_3 \equiv t^3 \bmod p$ for a p-adic unit t. We see that $\mathbf{Q}_p(E_3)$ is a unique $C_2 \times C_2$-extension for a prime element d. We see $\mathbf{Q}_p(E_3) = \mathbf{Q}_p(\zeta_3)$ for a p-adic unit d. For $p = 2$, we put $g_2 = 2^6\alpha$ and $g_3 = 2^3\beta$ ($\beta \equiv 1 \bmod 2^4$). We see $\mathbf{Q}_2(E_3) = \mathbf{Q}_2(\zeta_3, \sqrt{6})$ (resp. $\mathbf{Q}_2(\zeta_3, \sqrt{2})$, $\mathbf{Q}_2(\zeta_3, \sqrt{-1})$, $\mathbf{Q}_2(\zeta_3)$) for $d \equiv 1 \bmod 2^3$ (resp. $d \equiv 3 \bmod 2^3$, $d \equiv 2 \bmod 2^4$, $d \equiv 6 \bmod 2^4$). For $p = 3$, we put $g_2 = 3^4\alpha$ and $g_3 \equiv t^3 \bmod 3^{10}$ for a 3-adic unit t. We see $\mathbf{Q}_3(E_3) = \mathbf{Q}_3(\zeta_3, \sqrt{3})$ (resp. $\mathbf{Q}_3(\zeta_3)$) for a 3-adic unit d such that $t/d \equiv 1 \bmod 3$ (resp. $t/d \equiv -1 \bmod 3$).

(9-2) $G = \left\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle$. It is isomorphic to C_2.

(10) $G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$. These two cases occur in $p \equiv 1 \bmod 3$. We put $g_2 = p^2\alpha$ and $g_3 \equiv t^3 \bmod p$ for a p-adic unit t. We see $\mathbf{Q}_p(E_3) = \mathbf{Q}_p\big(\sqrt{(\gamma/t)p}\big)$ for $d \equiv \gamma p \bmod p^2$. We see that $\mathbf{Q}_p(E_3)$ is an unramified quadratic extension for a p-adic unit d such that $-t^3/d \bmod p$ is not a quadratic residue. We see $\mathbf{Q}_p(E_3) = \mathbf{Q}_p$, if $-t^3/d \bmod p$ is a quadratic residue.

3. Application. We call $\{G_p, I_p, V_p\}$ a ramification triple of $GL_2(\mathbf{F}_3)$, if it satisfies the following conditions:

1. G_p is a subgroup of $GL_2(\mathbf{F}_3)$, such that $G_p \subset SL_2(\mathbf{F}_3)$ (resp. $G_p \not\subset SL_2(\mathbf{F}_3)$) for $p \equiv 1 \bmod 3$ (resp. $p \not\equiv 1 \bmod 3$),
2. I_p is a normal subgroup such that G_p/I_p is a cyclic group,
3. V_p is a normal subgroup such that I_p/V_p is a cyclic group and the order $\sharp\,|\,I_p/V_p\,|$ divides $p^{\sharp|G_p/I_p|} - 1$,
4. V_p is a p-group.

Let G_p be a Galois group of a Galois extension $\mathbf{Q}_p(E_3)/\mathbf{Q}_p$. Let I_p (resp. V_p) be an inertia (resp. wild ramification) group of G_p. We see that $\{G_p, I_p, V_p\}$ is a ramification triple of $GL_2(\mathbf{F}_3)$. We get:

Theorem. *Let S be a finite set of primes. For $p \in S$, let $\{G_p, I_p, V_p\}$ be a ramification triple of $GL_2(\mathbf{F}_3)$. Moreover we assume that $\sharp\,|\,G_p/I_p\,|$ is even for $p \not\equiv 1 \bmod 3$. Then there exist infinitely many Galois extensions $K/\mathbf{Q}$ satisfying the following conditions*:

1. *Galois group of $K/\mathbf{Q}$ is isomorphic to $GL_2(\mathbf{F}_3)$,*
2. *$\zeta_3^\sigma = \zeta_3^{\det\sigma}$ for $\sigma \in \mathrm{Gal}(K/\mathbf{Q})$,*
3. *For $p \in S$, the decomposition (resp. inertia, wild ramification) group is conjugate to G_p (resp. I_p, V_p).*

Proof. We put $K = \mathbf{Q}(E_3)$ for an elliptic curve E defined over $\mathbf{Q}$. We see that the Galois group G of $K/\mathbf{Q}$ is a subgroup of $GL_2(\mathbf{F}_3)$ and $\zeta_3^\sigma = \zeta_3^{\det\sigma}$ for $\sigma \in \mathrm{Gal}(K/\mathbf{Q})$. If $\{G_p, I_p, V_p\}$ is a ramification triple of $GL_2(\mathbf{F}_3)$ satisfying the assumption in the theorem, G_p occurs in one of the case (1), (2), ..., or (10). We remark that every SD_{16}-extention in (7.2) has the same ramification triple whether it is generated by 3-division points of an elliptic curve or not. We take an elliptic curve E satisfying congruence conditions of modulo a suitable power of $p \in S$ as the previous section, for each prime $p \in S$. We see that K satisfies the third condition. Moreover we put $G_{q_1} = C_8$, $G_{q_2} = B$, for primes $q_1, q_2 \notin S$. Consequently G contains a subgroup which is isomorphic to C_8. It also contains a subgroup isomorphic to B. Hence we get $G = GL_2(\mathbf{F}_3)$. Hence we get one extension K in the theorem.

Next we prove that there exist infinitely many such fields. If there exist only finite such extensions, we put them $K_1, \ldots, K_t$. Let p_i be a prime which completely decomposes in $K_i/\mathbf{Q}$. We take S containing $p_1, \ldots, p_t$. We put $G_{p_i} \neq \{1\}$. We take an elliptic curve E as above discussion. We see that $K = \mathbf{Q}(E_3)$ is not $K_1, \ldots, K_t$. Thus we can construct infinitely many K. □

Acknowledgements. The author expresses his appreciation of the hospitality of the Faculty of Science of Osaka University during studying this theme in 1995. The summary of this note was published in [8] in Japanese. He also expresses his heartfelt thanks to the referee.

References

[1] Bayer, P., and Rio, A.: Dyadic exercises for octahedral extensions. J. Reine Angew. Math., **517**, 1–17 (1999).

[2] Fujisaki, G.: A remark on quaternion extensions of the rational p-adic field. Proc. Japan Acad., **66A**, 257–259 (1990).

[3] Koike, M.: Higher reciprocity law, modular forms of weight 1 and elliptic curves. Nagoya Math. J., **98**, 109–115 (1985).

[4] Lario, J.-C., and Rio, A.: An octahedral-elliptic type equality in $Br_2(k)$. C. R. Acad. Sci. Paris Sér. I Math., **321**, 39–44 (1995).

[5] Lario, J.-C., and Rio, A.: Elliptic modularity for octahedral Galois representations. Math. Res. Lett., **3**, 329–342 (1996).

[6] Naito, H.: Dihedral extensions of degree 8 over the rational p-adic fields. Proc. Japan Acad., **71A**, 17–18 (1995).

[7] Naito, H.: A congruence between the coefficients of the L-series which are related to an elliptic curve and the algebraic number field generated by its 3-division points. Mem. Fac. Edu. Kagawa Univ., **37**, 43–45 (1987).

[8] Naito, H.: Local fields generated by 3-division points of elliptic curves. RIMS Kokyuroku, **971**, 153–159 (1996). (in Japanese).

[9] Shimura, G.: A reciprocity law in non-solvable extensions. J. Reine Angew. Math., **221**, 209–220 (1966).

[10] Weil, A.: Exercises dyadiques. Invent. Math., **27**, 1–22 (1974).