Sairaiji, F.
Osaka J. Math.
39 (2002), 223–243

FORMAL GROUPS OF CERTAIN Q-CURVES OVER QUADRATIC FIELDS

Fumio SAIRAIJI

(Received March 24, 2000)

1. Introduction

Let E be an elliptic curve over $\mathbf{Q}$. We denote by $\hat{E}(x_1, x_2)$ the formal group associated to the minimal model over $\mathbf{Z}$ for E. Let $L(E/\mathbf{Q}, s) = \sum_{n\geq 1} a_n n^{-s}$ be the L-series attached to the l-adic representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on E. We denote by $\hat{L}(x_1, x_2)$ the formal group of the L-series $L(E/\mathbf{Q}, s)$, that is, the formal group with transformer $\sum_{n\geq 1} a_n n^{-1} x^n$. Then Honda shows:

Theorem 1.1 ([6], [7]). *$\hat{L}(x_1, x_2)$ is defined over $\mathbf{Z}$, and it is strongly isomorphic over $\mathbf{Z}$ to $\hat{E}(x_1, x_2)$.*

He also shows that $\hat{E}(x_1, x_2)$ determines the L-series $L(E/\mathbf{Q}, s)$. Namely, the coefficients of $L(E/\mathbf{Q}, s)$ can be obtained explicitly from the coefficients of the transformer of $\hat{E}(x_1, x_2)$.

We call an elliptic curve E over $\overline{\mathbf{Q}}$ a $\mathbf{Q}$-*curve* if it has an isogeny over $\overline{\mathbf{Q}}$ to E^{σ} for each σ in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ (cf. e.g. [4]). An elliptic curve over $\mathbf{Q}$ is a $\mathbf{Q}$-curve. We attempt to get a similar result of Theorem 1.1 to formal groups of $\mathbf{Q}$-curves over quadratic fields. The problem is to find an L-series whose formal group is strongly isomorphic to the formal group of a fixed Weierstrass model of a $\mathbf{Q}$-curve over a quadratic field.

Let K be a quadratic field with maximal order $\mathcal{O}_K$. We denote by σ a generator of the Galois group $\mathrm{Gal}(K/\mathbf{Q})$ of K over $\mathbf{Q}$. Let E be a $\mathbf{Q}$-curve defined over K. We assume that it has an isogeny φ over K from E to E^{σ} of non-square degree not equal to one. Let A be the restriction of scalars of E from K to $\mathbf{Q}$. Then A is of type F for some quadratic field F. We fix a Weierstrass model over $\mathcal{O}_K$ for E. We denote by $\hat{E}(x_1, x_2)$ its formal group. For the fixed Weierstrass model of E, we define the L-series $L_{\alpha}(s)$ by (3.8) in Section 3. $L_{\alpha}(s)$ is a linear combination of L-series attached to λ-adic representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on A, and it has coefficients in K. Then, for a finite set S satisfying the conditions (4.2) in Section 4, we have:

Theorem 4.1. *$\hat{L}_\alpha(x_1, x_2)$ is defined over the ring $\mathcal{O}_{K,S}$ of S-integers in K, and it is strongly isomorphic over $\mathcal{O}_{K,S}$ to $\hat{E}(x_1, x_2)$.*

As a corollary, we see that $\hat{E}(x_1, x_2)$ determines the p-factors of the L-series attached to λ-adic representations on A for almost all primes p. Since each p-factor of the ordinary L-series is obtained from that of the L-series attached to λ-adic representations, $\hat{E}(x_1, x_2)$ also determines the p-factors of the ordinary L-series.

When K is reduced to $\mathbf{Q}$, λ-adic representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on A is reduced to l-adic representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on E. Thus Theorem 4.1 is a generalization of Theorem 1.1 to the case of a $\mathbf{Q}$-curve E over a quadratic field K in the sense that $\hat{E}(x_1, x_2)$ determines the L-series attached to λ-adic representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on A, though we can not exclude some assumptions on E and on S.

The contents of this paper are as follows. In Section 2, we review the classification theory, studied by Honda, of formal groups over $\mathfrak{p}$-adic integer rings. In Section 3, after some investigations on the L-series of the restriction of scalars of a certain $\mathbf{Q}$-curve which we deal, we define an L-series associated to a certain $\mathbf{Q}$-curve and we discuss its associated formal group. In Section 4, we investigate the formal group structure of a certain $\mathbf{Q}$-curve and we prove Theorem 4.1.

The author would like to express his sincere gratitude to Professor Yoshihiko Yamamoto for his useful suggestion. The author also wishes to thank Professor Hirotada Naito for his warmful encouragement.

2. Formal groups over $\mathfrak{p}$-adic integer rings

We review some results needed in Sections 3 and 4.

2.1. Let R be a commutative ring. We denote by $R[[x_1, x_2, \dots, x_n]]$ the ring of formal power series on n variables $x_1, x_2, \dots, x_n$ with coefficients in R. We say that two power series $\varphi(x_1, \dots, x_n)$ and $\psi(x_1, \dots, x_n)$ in $R[[x_1, \dots, x_n]]$ are *congruent modulo degree r*, if they differ only in terms of total degree greater than or equal to r. Then we write $\varphi(x_1, \dots, x_n) \equiv \psi(x_1, \dots, x_n) \bmod \deg r$. We put

$$R[[x_1, \dots, x_n]]_0 := \{\varphi \in R[[x_1, \dots, x_n]] \mid \varphi \equiv 0 \bmod \deg 1\}.$$

A power series $\varphi(x)$ in $R[[x]]_0$ is said to be *invertible*, if $\psi(\varphi(x)) = x$ holds for some $\psi(x)$ in $R[[x]]_0$. The power series $\psi(x)$ is then uniquely determined by $\varphi(x)$, and is written $\varphi^{-1}(x)$. We note that a power series $\varphi(x)$ in $R[[x]]_0$ is invertible if and only if $\varphi(x) \equiv ax \bmod \deg 2$ holds for some unit a in R.

We define a (*one-dimensional commutative*) *formal group* over R as a power series $F(x_1, x_2)$ in $R[[x_1, x_2]]$ satisfying the following:

(i) $F(x_1, x_2) \equiv x_1 + x_2 \bmod \deg 2$.

(ii) $F(x_1, F(x_2, x_3)) = F(F(x_1, x_2), x_3)$.

(iii) $F(x_1, x_2) = F(x_2, x_1)$.

For example, the additive group $\hat{\mathbf{G}}_a(x_1, x_2) := x_1 + x_2$ and the multiplicative group $\hat{\mathbf{G}}_m(x_1, x_2) := x_1 + x_2 + x_1x_2$ are formal groups over R.

Let $F(x_1, x_2)$ and $G(x_1, x_2)$ be formal groups over R, and let $\varphi(x)$ be a power series in $R[[x]]_0$. We call $\varphi(x)$ a *homomorphism* over R from $F(x_1, x_2)$ to $G(x_1, x_2)$, if it satisfies

$$\varphi(F(x_1, x_2)) = G(\varphi(x_1), \varphi(x_2)).$$

Moreover, if $\varphi(x)$ is invertible, we call $\varphi(x)$ a (*weak*) *isomorphism*. The power series $\varphi^{-1}(x)$ is then an isomorphism from $G(x_1, x_2)$ to $F(x_1, x_2)$. We call an isomorphism $\varphi(x)$ a *strong isomorphism*, if $\varphi(x) \equiv x \bmod \deg 2$ holds. We see that a strong isomorphism from $F(x_1, x_2)$ to $G(x_1, x_2)$ is uniquely determined by $F(x_1, x_2)$ and $G(x_1, x_2)$ if it exists. We say that two formal groups are (*weakly*) *isomorphic* (resp. *strongly isomorphic*) if there exists an isomorphism (resp. a strong isomorphism) between them.

The set $\mathrm{Hom}_R(F, G)$ of all homomorphisms over R from $F(x_1, x_2)$ to $G(x_1, x_2)$ forms an additive group by the addition law: $(\varphi_1 + \varphi_2)(x) := G(\varphi_1(x), \varphi_2(x))$. We put $\mathrm{End}_R(F) := \mathrm{Hom}_R(F, F)$. Then the additive group $\mathrm{End}_R(F)$ forms a ring by the multiplication law: $(\varphi_1\varphi_2)(x) := \varphi_1(\varphi_2(x))$. We denote by $[n]_F(x)$ the image of an integer n under the canonical ring homomorphism from $\mathbf{Z}$ to $\mathrm{End}_R(F)$.

We suppose that R is an integral domain of characteristic zero. Then, for every formal group $F(x_1, x_2)$ over R, there exists an unique strong isomorphism $f(x)$ over its quotient field from $F(x_1, x_2)$ to $\hat{\mathbf{G}}_a(x_1, x_2)$ (cf. e.g. [7]; Theorem 1). We call $f(x)$ the *transformer* of $F(x_1, x_2)$. We see that $F(x_1, x_2) = f^{-1}(f(x_1) + f(x_2))$.

Now we suppose that R is a field of characteristic $p > 0$. Then the endomorphism $[p]_F(x)$ of $F(x_1, x_2)$ satisfies either $[p]_F(x) \equiv ax^{p^h} \bmod \deg(p^h + 1)$ with non-zero element a for some integer h or $[p]_F(x) = 0$ (cf. e.g. [6]; Lemma 1). We say that the *height* of $F(x_1, x_2)$ is h or infinity, according as in the former case or in the latter case.

2.2. We review the classification theory of formal groups over $\mathfrak{p}$-adic integer rings, which is studied by Honda [7].

Let K be a finite Galois extension of the p-adic number field $\mathbf{Q}_p$. We denote by $\mathcal{O}$ and $\mathfrak{p}$ its maximal order and its maximal ideal, respectively. We fix a Frobenius endomorphism σ for $\mathfrak{p}$ in $\mathrm{Gal}(K/\mathbf{Q}_p)$. We also fix a prime element π in $\mathcal{O}$.

Let $K_\sigma[[T]]$ (resp. $\mathcal{O}_\sigma[[T]]$) be the non-commutative power series ring in T with the multiplication law: $Ta = a^\sigma T$ for $a \in K$ (resp. $a \in \mathcal{O}$). We define the action of

$K_\sigma[[T]]$ on $K[[x]]_0$ from left hand side by the following:

$$(u * f)(x) := \sum_{\nu=0}^{\infty} a_\nu f^{\sigma^\nu}\left(x^{p^\nu}\right) \quad \text{for} \quad u := \sum_{\nu=0}^{\infty} a_\nu T^\nu \in K_\sigma[[T]].$$

An element u in $\mathcal{O}_\sigma[[T]]$ is said to be *special*, if $u \equiv \pi \bmod \deg 1$. A power series $f(x)$ in $K[[x]]_0$ is said to be of *type* u, if $f(x) \equiv x \bmod \deg 2$ and $(u * f)(x) \equiv 0 \bmod \mathfrak{p}$. For example, $(u^{-1}\pi) * x$ is of type u. A formal group over K is said to be of *type* u, if its transformer is of type u.

Let $F(x_1, x_2)$ and $G(x_1, x_2)$ be formal groups over K with transformer $f(x)$ and $g(x)$, respectively.

Proposition 2.1 ([7, Theorem 2 and 3]). *Suppose that $F(x_1, x_2)$ is of type u for some special element u. Then $F(x_1, x_2)$ is defined over $\mathcal{O}$. In addition, suppose that $G(x_1, x_2)$ is of type v for some special element v. Then the mapping*:

$$\{c \in \mathcal{O} \mid vc = tu \text{ for some } t \in \mathcal{O}_\sigma[[T]]\} \to \mathrm{Hom}_{\mathcal{O}}(F, G) : \ c \mapsto g^{-1}(cf(x))$$

is a group isomorphism. In particular, $F(x_1, x_2)$ and $G(x_1, x_2)$ are strongly isomorphic over $\mathcal{O}$ if and only if $v = tu$ for some t in $\mathcal{O}_\sigma[[T]]$.

As below in this section, we assume that we take p as fixed prime π when $\mathfrak{p}$ is unramified. In the case where $\mathfrak{p}$ is unramified, the converse of the former part of Proposition 2.1 holds.

Proposition 2.2 ([7, Propositions 2.6 and 3.3]). *Assume that $\mathfrak{p}$ is unramified. If $F(x_1, x_2)$ is a formal group defined over $\mathcal{O}$ with transformer $f(x)$, then the ideal $\{u' \in \mathcal{O}_\sigma[[T]] \mid u' * f \equiv 0 \bmod \mathfrak{p}\}$ is a left principal ideal generated by some special element u. In particular, $F(x_1, x_2)$ is of type u.*

Let u' and v' be elements in $\mathcal{O}_\sigma[[T]]$. We say that v' is *left associate* with u', if $v' = tu'$ holds for some unit t in $\mathcal{O}_\sigma[[T]]$. A formal group over $\mathcal{O}$ is said to be of *height* h, if its reduction modulo $\mathfrak{p}$ is of height h. In the case where $\mathfrak{p}$ is unramified, it follows from Propositions 2.1 and 2.2 that the strong isomorphism classes of formal groups over $\mathcal{O}$ correspond bijectively to the left associate classes of the special elements.

Proposition 2.3 ([7, Proposition 3.5]). *Assume that $\mathfrak{p}$ is unramified. The strong isomorphism classes of formal groups over $\mathcal{O}$, of height h $(1 \le h \le \infty)$, correspond* *bijectively to the special elements of the following form*:

$$\begin{cases} p & \text{if } h = \infty \\ p + \displaystyle\sum_{\nu=1}^{h} a_\nu T^\nu \text{ with } a_1, \ldots, a_{h-1} \in \mathfrak{p} \text{ and } a_h \in \mathcal{O}^* & \text{if } 1 \leq h < \infty. \end{cases}$$

The following propositions are needed in Section 4.

Proposition 2.4 ([7, Lemma 4.2]). *Let $f(x)$ be a power series in $K[[x]]_0$ of type u for some special element u. Let $\psi_1(x)$ be a power series in $K[[x]]_0$ and let $\psi_2(x)$ be a power series in $\mathcal{O}[[x]]_0$. Then, $f(\psi_1(x)) \equiv f(\psi_2(x)) \bmod \mathfrak{p}$ if and only if $\psi_1(x) \equiv \psi_2(x) \bmod \mathfrak{p}$.*

Proposition 2.5. *Let $u = \sum_{\nu=0}^{m} a_\nu T^\nu$ and $v = \sum_{\nu=0}^{n} b_\nu T^\nu$ be elements of $\mathcal{O}_\sigma[[T]]$. Assume that $v = tu$ for some $t = \sum_{\nu=0}^{\infty} c_\nu T^\nu$ in $\mathcal{O}_\sigma[[T]]$. If $n \geq m$, $a_0, \ldots, a_{m-1} \in \mathfrak{p}$, and $a_m \in \mathcal{O}^*$, then $c_\nu = 0$ holds for each $\nu > n - m$.*

Proof. Since

$$tu = \left(\sum_{\nu=0}^{\infty} c_\nu T^\nu\right)\left(\sum_{\nu=0}^{m} a_\nu T^\nu\right) = \sum_{\nu=0}^{\infty}\left(\sum_{\mu=0}^{\nu} c_\mu a_{\nu-\mu}^{\sigma^\mu}\right)T^\nu,$$

where we put $a_\nu = 0$ for $\nu > m$, it follows from $v = tu$ that

$$c_{\nu-m}a_m^{\sigma^{\nu-m}} = -\left(c_{\nu-m+1}a_{m-1}^{\sigma^{\nu-m+1}} + \cdots + c_\nu a_0^{\sigma^\nu}\right) \tag{2.1}$$

holds for each $\nu > n$. Since $a_0, \ldots, a_{m-1} \in \mathfrak{p}$ and $a_n \in \mathcal{O}^*$, it follows from (2.1) that $c_{\nu-m} \in \mathfrak{p}$ for $\nu > n$, that is, $c_\nu \in \mathfrak{p}$ for $\nu > n - m$. Thus by using (2.1) again, we have $c_\nu \in \mathfrak{p}^2$ for $\nu > n - m$. In the same way, we inductively get $c_\nu \in \mathfrak{p}^\mu$ for each positive integer μ and $\nu > n - m$. Hence we have $c^\nu = 0$ for $\nu > n - m$. □

2.3. We give certain formal groups over $\mathcal{O}$ in the case of $\sigma^2 = 1$. They are related to the formal groups, over quadratic fields, which we deal with in Sections 3 and 4.

We fix an integer $\chi(p)$ in the set $\{-1, 0, 1\}$. For each commutative ring R, we define the linear action $T_{p,\chi}$ on $R[[x]]_0$ from right hand side by

$$\sum_{n\geq 1} a_n x^n \mid T_{p,\chi} := \sum_{n\geq 1} a_{np} x^n + \chi(p) p \sum_{n\geq 1} a_n x^{np}. \tag{2.2}$$

Let $\sum_{n\geq 1} a_n x^n$ be a power series in $\mathcal{O}[[x]]_0$ with $a_1 = 1$.

Proposition 2.6. *Assume that* $\mathfrak{p}$ *is unramified. If*

$$\sum_{n\geq 1} a_n x^n \mid T_{p,\chi} = a_p \sum_{n\geq 1} a_n^\sigma x^n, \tag{2.3}$$

then $\sum_{n\geq 1} a_n n^{-1} x^n$ *is of type* $p - a_p T + \chi(p) T^2$.

Proof. It follows from (2.3) that

$$\begin{cases} a_{np} = a_p a_n^\sigma & \text{for each positive integer } n \text{ coprime to } p \\ a_{np^2} - a_p a_{np}^\sigma + \chi(p) p a_n = 0 & \text{for each positive integer } n. \end{cases}$$

Together with $\sigma^2 = 1$, we have

$$\begin{aligned} &\left(p - a_p T + \chi(p) T^2\right) * \sum_{n\geq 1} \frac{a_n}{n} x^n \\ &\quad = p \sum_{n\geq 1} \frac{a_n}{n} x^n - a_p \sum_{n\geq 1} \frac{a_n^\sigma}{n} x^{np} + \chi(p) \sum_{n\geq 1} \frac{a_n}{n} x^{np^2} \\ &\quad = p \left(\sum_{\substack{n\geq 1 \\ (n,p)=1}} + \sum_{\substack{n\geq 1 \\ p\mid n}} \right) \frac{a_n}{n} x^n - a_p \sum_{n\geq 1} \frac{a_n^\sigma}{n} x^{np} + \chi(p) \sum_{n\geq 1} \frac{a_n}{n} x^{np^2} \\ &\quad \equiv \sum_{n\geq 1} \frac{a_{np}}{n} x^{np} - a_p \sum_{n\geq 1} \frac{a_n^\sigma}{n} x^{np} + \chi(p) \sum_{n\geq 1} \frac{a_n}{n} x^{np^2} \bmod \mathfrak{p} \\ &\quad \equiv \sum_{\substack{n\geq 1 \\ (n,p)=1}} \frac{a_{np} - a_p a_n^\sigma}{n} x^{np} + \sum_{n\geq 1} \frac{a_{np^2} - a_p a_{np}^\sigma + \chi(p) p a_n}{np} x^{np^2} \bmod \mathfrak{p} \\ &\quad \equiv 0 \bmod \mathfrak{p}. \end{aligned}$$

□

Proposition 2.7. *Assume that* $\mathfrak{p}$ *is ramified and* $\chi(p) = 0$. *If* $\sum_{n\geq 1} a_n x^n \mid T_{p,\chi} = 0$, *then* $\sum_{n\geq 1} a_n n^{-1} x^n$ *is of type* π.

Proof. It follows from our assumption that $a_{np} = 0$ for $n \geq 1$. Thus we have

$$\pi * \sum_{n\geq 1} \frac{a_n}{n} x^n = \pi \sum_{\substack{n\geq 1 \\ (n,p)=1}} \frac{a_n}{n} x^n \equiv 0 \bmod \mathfrak{p}.$$

□

3. Formal groups associated to L-series of Q-curves over quadratic fields

Let K be a quadratic field with maximal order $\mathcal{O}_K$ and discriminant D_K. We denote by σ the generator of $\mathrm{Gal}(K/\mathbf{Q})$. Let E be an elliptic curve over K such that it has an isogeny φ over K from E to E^σ of non-square degree. Then E is a **Q**-curve.

By taking bases, conjugate over **Q**, of one-dimensional K-vector spaces of differentials of E over K and of E^σ over K and by looking at the actions of the pull-backs of φ and φ^σ, we see that

$$\left[m^2 d\right]_E = \varphi^\sigma \circ \varphi \quad \text{and} \quad m^2 d = \alpha\alpha^\sigma \tag{3.1}$$

for some square-free integer d, some natural number m, and some α in K, where $[n]_E$ is the multiplication-by-n map of E. The integer d is positive or negative according as the dual isogeny of φ is equal to φ^σ or $-\varphi^\sigma$. The degree of φ is the absolute value of $m^2 d$. Since the degree of φ is not square, d is not equal to ± 1.

3.1. Let (A, η) be the restriction of scalars of E from K to **Q**. By definition, A is an abelian variety over **Q** of dimension two and η is a homomorphism over K from A to E such that the homomorphism (η, η^σ) is an isomorphism over K from A to $E \times E^\sigma$. We denote by N_E and N_A the conductors of E over K and of A over **Q**, respectively (cf. e.g. [9]).

Proposition 3.1 ([9, Proposition 1]). *$N_A = (\mathbf{N}_{K/\mathbf{Q}} N_E)|D_K|^2$, where $\mathbf{N}_{K/\mathbf{Q}}$ is the norm.*

Let $L(E/K, s)$ and $L(A/\mathbf{Q}, s)$ be the L-series attached to the l-adic representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/K)$ on E and of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on A, respectively.

Proposition 3.2 ([9, Proposition 3]). *$L(E/K, s) = L(A/\mathbf{Q}, s)$.*

Now we discuss endomorphisms defined over **Q** of A.

We put $F := \mathbf{Q}(\sqrt{d})$. Since d is a square-free integer not equal to ± 1, F is a quadratic field not equal to $\mathbf{Q}(\sqrt{-1})$. Furthermore F is real or imaginary according as the dual isogeny of φ is equal to φ^σ or $-\varphi^\sigma$. We denote by τ the generator of $\mathrm{Gal}(F/\mathbf{Q})$.

The isogeny φ induces the endomorphism $[\varphi \times \varphi^\sigma]_A$ satisfying the following commutative diagram:

$$\begin{tikzcd} A \arrow[r, "{[\varphi\times\varphi^\sigma]_A}"] \arrow[d, "{(\eta,\eta^\sigma)}"'] & A \arrow[d, "{(\eta^\sigma,\eta)}"'] \\ E \times E^\sigma \arrow[r, "\varphi\times\varphi^\sigma"] & E^\sigma \times E. \end{tikzcd}$$

We note that $\varphi^\sigma \circ \varphi$ is the multiplication-by-$m^2 d$ map of E. We can check that

$$([\varphi \times \varphi^\sigma]_A)^\sigma = [\varphi \times \varphi^\sigma]_A \text{ and } ([\varphi \times \varphi^\sigma]_A)^2 = [m^2 d]_A.$$

Thus we have isomorphisms from F into the **Q**-algebra $\mathrm{End}^0(A)$ of endomorphisms defined over $\mathbf{Q}$ of A.

We take an isomorphism ι from F to $\mathrm{End}^0(A)$ satisfying $\iota\big(\sqrt{m^2d}\big) = [\pm 1]_A \circ [\varphi \times \varphi^\sigma]_A$. Then (A, ι) is of type F, and so is $(A, \iota \circ \tau)$.

We recall the definition of the L-series attached to the λ-adic representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on (A, ι).

For each prime integer l, let $T_l(A)$ be the l-adic Tate module attached to A; $T_l(A)$ is a $\mathbf{Z}_l$-free module of rank four. We put $V_l(A) := \mathbf{Q}_l \otimes_{\mathbf{Z}_l} T_l(A)$; $V_l(A)$ is a $\mathbf{Q}_l$-vector space of dimension four. We put $F_l := F \otimes_{\mathbf{Q}} \mathbf{Q}_l$. Then $V_l(A)$ is an F_l-module since $\iota(F)$ operates on $V_l(A)$; in fact, $V_l(A)$ is a free F_l-module of rank two (cf. [10, Theorem (2.1.1)]). Since the actions of $\mathrm{End}^0(A)$ and of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ commute with each other, the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on $V_l(A)$ is F_l-linear. On the other hand F_l is decomposed into the product $\prod_{\lambda|l} F_\lambda$ of the λ-adic completions F_λ of F at the primes λ dividing l. For each λ dividing l, we put $V_\lambda(A) := F_\lambda \otimes_{F_l} V_l(A)$. Then $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts F_λ-linearly on $V_\lambda(A)$. We get a continuous homomorphism

$$\rho_\lambda : \mathrm{Gal}\big(\overline{\mathbf{Q}}/\mathbf{Q}\big) \to \mathrm{GL}_{F_\lambda}(V_\lambda(A)).$$

The homomorphism ρ_λ is called the *λ-adic representation* on (A, ι).

For a prime integer p, let $\mathfrak{P}$ be a prime in $\overline{\mathbf{Q}}$ and $I_{\mathfrak{P}}$ be its inertia group in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Let $\sigma_{\mathfrak{P}}$ be a Frobenius automorphism for $\mathfrak{P}$ in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. We define the local L-series $L_p(A, \iota, s)$ attached to λ-adic representations by

$$L_p(A, \iota, u) := \det(1 - u \cdot \rho_\lambda(\sigma_{\mathfrak{P}}) \mid V_\lambda(A)^{I_{\mathfrak{P}}}),$$

where $V_\lambda(A)^{I_{\mathfrak{P}}}$ is the fixed subspace for the action of $I_{\mathfrak{P}}$. It does not depend on the choice of $\mathfrak{P}$ and $\sigma_{\mathfrak{P}}$.

Proposition 3.3 ([11, Proposition 11.9]). *For each prime p which does not divide N_A, $L_p(A, \iota, u)$ is a polynomial with coefficients in the maximal order $\mathcal{O}_F$ of F, which is independent of $l \neq p$ and λ dividing l.*

We put

$$\chi(p) := \begin{cases} 0 & \text{if } p \text{ divides } N_A \\ 1 & \text{if } p \text{ does not divide } N_A \text{ and } d > 0 \\ (D_K/p) & \text{if } p \text{ does not divide } N_A \text{ and } d < 0, \end{cases}$$

where $(D_K/*)$ is the Kronecker symbol for K.

Proposition 3.4 ([2, Proposition (2.3)]). *Assume that $d > 0$. For each prime p,*

$$L_p(A, \iota, u) = 1 - c_p u + \chi(p) p u^2 \text{ with } c_p \in \mathcal{O}_F, \tag{3.2}$$

which is independent of $l \neq p$ and λ dividing l.

In the following we will see that (3.2) also holds in the case where $d < 0$ and p does not divide N_A.

For each prime $\mathfrak{p}$ in K, we denote by $L_{\mathfrak{p}}(E/K, u)$ the $\mathfrak{p}$-factor of $L(E/K, s)$, and we put

$$\varepsilon_{\mathfrak{p}} := \begin{cases} 0 & \text{if } \mathfrak{p} \text{ divides } N_E \\ 1 & \text{otherwise.} \end{cases}$$

Then we can write

$$L_{\mathfrak{p}}(E/K, u) = 1 - a_{\mathfrak{p}} u^{\deg \mathfrak{p}} + \varepsilon_{\mathfrak{p}} \mathbf{N}\mathfrak{p} u^{2 \deg \mathfrak{p}}$$

for some integer $a_{\mathfrak{p}}$, where $\mathbf{N}\mathfrak{p}$ is the cardinarity of the residue field $\mathcal{O}_K/\mathfrak{p}$ and $\deg \mathfrak{p}$ is the degree of the extension of $\mathcal{O}_K/\mathfrak{p}$ over its prime field.

We identify $V_l(A)$ with $V_l(E) \oplus V_l(E^\sigma)$ through the isomorphism (η, η^σ). Then we have $\iota\big(\sqrt{d}\big) V_l(E) = V_l(E^\sigma)$. Thus each $\mathbf{Q}_l$-basis of $V_l(E)$ can be seen as a F_l-basis of $V_l(A)$. We note that $V_l(A)^{I_{\mathfrak{P}}} = V_l(E)^{I_{\mathfrak{P}}} \oplus V_l(E^\sigma)^{I_{\mathfrak{P}}}$ if p is unramified in K. In the following we put $\mathfrak{p} := \mathfrak{P} \cap K$.

In the case where p splits completely in K we have the following:

Lemma 3.5. *If p splits completely in K, then $L_p(A, \iota, u) = 1 - a_{\mathfrak{p}} u + \chi(p) p u^2$.*

Proof. Since p splits completely in K, $\sigma_{\mathfrak{P}}$ is a Frobenius automorphism for $\mathfrak{P}$ in $\mathrm{Gal}(\overline{\mathbf{Q}}/K)$. Since $\sigma_{\mathfrak{P}}(V_\ell(E)^{I_{\mathfrak{P}}}) = V_\ell(E)^{I_{\mathfrak{P}}}$, we have $L_p(A, \iota, u) = L_{\mathfrak{p}}(E/K, u)$. The assertion follows by the definition of $\chi(p)$. We note that $L_{\mathfrak{p}}(E/K, u) = L_{\mathfrak{p}^\sigma}(E/K, u)$ since E and E^σ are isogenous over K. □

Next we consider the case where p remains prime in K. Then $\sigma_{\mathfrak{P}}(V_\ell(E)^{I_{\mathfrak{P}}}) = V_\ell(E^\sigma)^{I_{\mathfrak{P}}} = \iota\big(\sqrt{d}\big) V_\ell(E)^{I_{\mathfrak{P}}}$. Suppose that either $d > 0$ or $\mathfrak{p}$ does not divide N_E. It follows from Proposition 3.3 or 3.4 that $L_p(A, \iota, u) = 1 - au + bu^2$ with $a \in \mathbf{Z}\sqrt{d}$ and $b \in \mathbf{Z}$. Now $\sigma_{\mathfrak{P}}^2$ is a Frobenius automorphism for $\mathfrak{P}$ in $\mathrm{Gal}(\overline{\mathbf{Q}}/K)$ and $\sigma_{\mathfrak{P}}^2(V_\ell(E)^{I_{\mathfrak{P}}}) = V_\ell(E)^{I_{\mathfrak{P}}}$. Thus we have

$$L_{\mathfrak{p}}(E/K, u) = 1 - \big(a^2 - 2b\big)u + b^2 u^2. \tag{3.3}$$

If $\mathfrak{p}$ divides N_E, then we have $b = 0$ and $a^2 = 0, \pm 1$. Otherwise we have $b^2 = p^2$, that is, $b = \varepsilon p$ with $\varepsilon = \pm 1$.

Lemma 3.6. *Assume that $d > 0$. If p remains prime in K and $\mathfrak{p}$ divides N_E, then $L_p(A, \iota, u) = 1$. Namely E has additive reduction at $\mathfrak{p}$.*

Proof. We recall $F = \mathbf{Q}\big(\sqrt{d}\big)$ is a quadratic field not equal to $\mathbf{Q}\big(\sqrt{-1}\big)$. Since $a \in \mathbf{Z}\sqrt{d}$ and $a^2 = 0, \pm 1$, we have $a = 0$, namely, $L_p(A, \iota, u) = 1$. Furthermore it follows from (3.3) that $L_{\mathfrak{p}}(E/K, u) = 1$. Thus E has additive reduction at $\mathfrak{p}$. □

Lemma 3.7. *If p remains prime in K and it does not divide N_E, then $L_p(A,\iota,u) = 1 - c_p u + \chi(p)pu^2$ for some c_p in $\mathbf{Z}\sqrt{d}$.*

Proof. Since $c_p = a \in \mathbf{Z}\sqrt{d}$ and $b = \varepsilon p$, it is enough to show $\varepsilon = \chi(p)$. Weil's Riemann conjecture asserts that the absolute value of the inverse roots $\bigl(a \pm \sqrt{a^2 - 4\varepsilon p}\bigr)/2$ of the equation $1 - au + \varepsilon pu^2 = 0$ are equal to $\sqrt{p}$. It occurs only if either $\varepsilon d > 0$ or $a = 0$. $\varepsilon d > 0$ implies $\varepsilon = \chi(p)$ by the definition of $\chi(p)$. If $a = 0$, (3.3) implies $a_{\mathfrak{p}} = -2\varepsilon p$ and then $\varepsilon = \chi(p)$ is verified from the following Lemma 3.8. Thus the assertion is verified. □

Lemma 3.8. *Assume that p remains prime in K and it does not divide N_E. If p divides $a_{\mathfrak{p}}$, then $a_{\mathfrak{p}} = -2\chi(p)p$ and $L_p(A,\iota,u) = 1 + \chi(p)pu^2$.*

Proof. Since $|a_{\mathfrak{p}}| \leq 2\sqrt{\mathbf{N}\mathfrak{p}} = 2p$ and p divides $a_{\mathfrak{p}}$, we can write $a_{\mathfrak{p}} = j\varepsilon p$ for an integer j such that $-2 \leq j \leq 2$. Then it follows from (3.3) that $a = \pm\sqrt{(j+2)\varepsilon p}$. Since $a \in \mathbf{Z}\sqrt{d}$ and $F \neq \mathbf{Q}\bigl(\sqrt{-1}\bigr)$, we have $(j,p,\varepsilon) \neq (0,2,\pm1), (1,3,\pm1)$. Thus p divides d unless $\sqrt{(j+2)\varepsilon p} = 0$.

Suppose that p divides d. We note that p remains prime in K. On the one hand, the order of d at $\mathfrak{p}$ is one since d is square-free. On the other hand, it follows from (3.1) that the order of d at $\mathfrak{p}$ is even. This is a contradiction. Thus p does not divide d. We have $a_{\mathfrak{p}} = -2\varepsilon p$ and $a = 0$.

Next we show $\varepsilon = \chi(p)$. Since $L_{\mathfrak{p}}(E/K,u) = 1 + 2\varepsilon pu^2 + p^2u^4$, $\sigma_{\mathfrak{P}}^2 = [-\varepsilon p]_E$ on $V_\ell(E)$. Since $\mathfrak{p}$ does not divide N_E, the reduction of $\varphi^\sigma \circ \sigma_{\mathfrak{P}}$ modulo $\mathfrak{P}$ is an endomorphism of the reduction $E_{\mathfrak{p}}$ of E modulo $\mathfrak{p}$. Furthermore, the $\mathbf{Q}$-algebra of endomorphisms of $E_{\mathfrak{p}}$ is a definite quarternion algebra since p divides $a_{\mathfrak{p}}$. Now $(\varphi^\sigma \circ \sigma_{\mathfrak{P}})^2 = \varphi^\sigma \circ \varphi \circ \sigma_{\mathfrak{P}}^2 = [-\varepsilon pd]_E$ on $V_\ell(E)$. Thus the injectivity of the reduction mapping from the $\mathbf{Q}$-algebra of endomorphisms of E to that of $E_{\mathfrak{p}}$ implies $-\varepsilon pd < 0$. Hence, by the definition of $\chi(p)$, we have $\varepsilon = \chi(p)$. □

Next we consider the case where $\mathfrak{p}$ ramifies over K. Then it follows from Proposition 3.1 that p divides N_A and thus $\chi(p) = 0$ by definition. Thus Poroposition 3.3 implies that $L_p(A,\iota,u) = 1 - c_p u + \chi(p)pu^2$ for some c_p in $\mathcal{O}_F$.

Lemma 3.9. *Assume that $d > 0$. If $\mathfrak{p}$ is ramified in K, then $L(A,\iota,s) = 1$. Namely, E has additive reduction at $\mathfrak{p}$.*

Proof. By the definition of $L_p(A,\iota,u)$, we have $L_p(A,\iota,u)L_p(A,\iota,u)^\tau = L_p(A/\mathbf{Q},s)$. Together with Proposition 3.2, we see that

$$(1 - c_p u)\bigl(1 - c_p^\tau u\bigr) = 1 - a_{\mathfrak{p}} u + \varepsilon_{\mathfrak{p}} pu^2. \tag{3.4}$$

Suppose that $\varepsilon_{\mathfrak{p}} = 1$. Then c_p must be an imaginary quadratic integer with $|c_p| = \sqrt{p}$

by (3.4). Since F is a real quadratic field, this contradicts Proposition 3.3. Thus $\varepsilon_{\mathfrak{p}} = 0$, and consequently we get $c_p = a_{\mathfrak{p}} = 0$ from (3.4). □

We define the L-series $L(A, \iota, s)$ attached to λ-adic representations on (A, ι) by the Euler product:

$$L(A, \iota, s) := \prod_{p} L_p(A, \iota, p^{-s})^{-1}, \tag{3.5}$$

where the product is taken for all primes p (resp. primes p which does not divide N_A) in the case of $d > 0$ (resp. $d < 0$).

We define $\{c_n\}_{n\geq 1}$ by $L(A, \iota, s) = \sum_{n\geq 1} c_n n^{-s}$. We note c_p is well-defined for each prime p. Since $L_p(A, \iota, u) = 1 - c_p u + \chi(p)pu^2$ from Lemmas 3.5–3.9, the Euler product (3.5) implies the following equations:

$$\begin{cases} c_{nn'} = c_n c_{n'} & \text{for } n, n' \geq 1 \text{ with } (n, n') = 1 \\ c_{p^{n+2}} - c_p c_{p^{n+1}} + \chi(p) p c_{p^n} = 0 & \text{for each prime } p \text{ and } n \geq 0. \end{cases} \tag{3.6}$$

Together with Lemmas 3.5–3.9, we have:

Proposition 3.10. *The coefficient c_n has the following properties*:

$$\begin{cases} c_n \in \mathbf{Z} & \textit{if } (D_K/n) = 1 \\ c_n \in \mathbf{Z}\sqrt{d} & \textit{if } (D_K/n) = -1 \\ c_n = 0 & \textit{if } (D_K/n) = 0. \end{cases} \tag{3.7}$$

We note that $c_{np} = 0$ for each n by the definition of $L(A, \iota, s)$, if $d < 0$ and $\mathfrak{p}$ divides N_E.

3.2. We take an invariant differential ω_E on E. The invariant differential ω_E defines the module homomorphism α from $\mathrm{Hom}_K(E, E^\sigma)$ to K by

$$\psi^*\left((\omega_E)^\sigma\right) = \alpha(\psi)\omega_E,$$

where $\psi^*((\omega_E)^\sigma)$ is the pull-back of the conjugate differential $(\omega_E)^\sigma$ on E^σ by ψ. We define the L-series $L_\alpha(s)$ by

$$\begin{aligned} L_\alpha(s) := {} & \frac{1}{2}(L(A, \iota, s) + L(A, \iota\circ\tau, s)) \\ & + \frac{\varepsilon\alpha(\varphi)^\sigma}{2\iota^{-1}([\varphi\times\varphi^\sigma]_A)}(L(A, \iota, s) - L(A, \iota\circ\tau, s)), \end{aligned} \tag{3.8}$$

where ε is 1 or -1 according as $d > 0$ or $d < 0$. We note that $\iota^{-1}([\varphi\times\varphi^\sigma]_A) = \pm\sqrt{m^2 d}$. The L-series $L_\alpha(s)$ does not depend on the choice of ι, since $(\iota\circ\tau)^{-1}([\varphi\times$

$\varphi^\sigma]_A) = -\iota^{-1}([\varphi \times \varphi^\sigma]_A)$. The L-series $L_\alpha(s)$ has coefficients in K, and it does not generally have Euler product. We define $\{\tilde{c}_n\}_{n\geq 1}$ by $\sum_{n\geq 1}\tilde{c}_n n^{-s} = L_\alpha(s)$. For simplicity, in the rest of this paper, we assume that $\iota\left(\sqrt{m^2 d}\right) = [\varphi \times \varphi^\sigma]_A$, and we write α instead of $\alpha(\varphi)$.

Proposition 3.11. *The coefficient $\tilde{c}_n$ has the following properties*:

$$\tilde{c}_n = \begin{cases} c_n & \text{if } (D_K/n) = 1 \\ \left(c_n/\sqrt{m^2 d}\right)\varepsilon\alpha^\sigma & \text{if } (D_K/n) = -1 \\ 0 & \text{if } (D_K/n) = 0. \end{cases} \tag{3.9}$$

Proof. We get

$$\tilde{c}_n = \frac{c_n + c_n^\tau}{2} + \frac{c_n - c_n^\tau}{2\sqrt{m^2 d}}\varepsilon\alpha^\sigma \tag{3.10}$$

from the definition of $\tilde{c}_n$. Together with Proposition 3.10, Proposition 3.11 follows. □

We denote the formal group over K with transformer $\sum_{n\geq 1}\tilde{c}_n n^{-1}x^n$ by $\hat{L}_\alpha(x_1, x_2)$. We call $\hat{L}_\alpha(x_1, x_2)$ the *formal group of $L_\alpha(s)$*.

For each prime $\mathfrak{p}$, we denote by $\mathcal{O}_{K,\mathfrak{p}}$ and $K_\mathfrak{p}$ the $\mathfrak{p}$-adic completions of $\mathcal{O}_K$ and of K. We denote by $\sigma_\mathfrak{p}$ the Frobenius automorphism for $\mathfrak{p}$ in $\mathrm{Gal}(K_\mathfrak{p}/\mathbf{Q}_p)$. We take a finite set S of primes in K satisfying the following condition:

$$\text{(i)} \quad \text{If } \alpha/m \notin \mathcal{O}_{K,\mathfrak{p}}, \text{ then } \mathfrak{p} \in S. \tag{3.11}$$

If $\mathfrak{p} \notin S$, then $\tilde{c}_n \in \mathcal{O}_{K,\mathfrak{p}}$ for each n. Let $\mathcal{O}_{K,S}$ be the ring of S-integers in K. Namely,

$$\mathcal{O}_{K,S} = \bigcap_{\mathfrak{p}\notin S}(\mathcal{O}_{K,\mathfrak{p}} \cap K).$$

Then $\tilde{c}_n \in \mathcal{O}_{K,S}$ for each n.

Theorem 3.12. *$\hat{L}_\alpha(x_1, x_2)$ over $K_\mathfrak{p}$ is of type $p - \tilde{c}_p T + \chi(p)T^2$ for each prime $\mathfrak{p} \notin S$. In particular, $\hat{L}_\alpha(x_1, x_2)$ is defined over $\mathcal{O}_{K,S}$.*

Proof. The latter part immediately follows from the former part by using Proposition 2.1. By using Propositions 2.6 and 2.7, for the proof of the former part it is enough to show

$$\sum_{n\geq 1}\tilde{c}_n x^n \mid T_{p,\chi} = \tilde{c}_p \sum_{n\geq 1}\tilde{c}_n^\sigma x^n \tag{3.12}$$

for each prime $\mathfrak{p} \notin S$.

We define $f_1(x)$ and $f_2(x)$ in $\mathbf{Q}[[x]]_0$ by

$$f_1(x) + \sqrt{m^2 d}\, f_2(x) = \sum_{n \geq 1} c_n x^n.$$

Then we have

$$f_1(x) + \varepsilon\alpha^\sigma f_2(x) = \sum_{n \geq 1} \tilde{c}_n x^n.$$

It follows from (3.6) that

$$\sum_{n \geq 1} c_n x^n \mid T_{p,\chi} = c_p \sum_{n \geq 1} c_n x^n. \tag{3.13}$$

The equation (3.13) implies the following three lemmas. Theorem 3.12 follows from them. □

Lemma 3.13. *If p splits completely in K and $\mathfrak{p} \notin S$, then $\hat{L}_\alpha(x_1, x_2)$ over $K_\mathfrak{p}$ is of type $p - \tilde{c}_p T + \chi(p)T^2$.*

Proof. We recall that $c_p \in \mathbf{Z}$ and $c_p = \tilde{c}_p$ by Propositions 3.10 and 3.11 in this case. We also recall $\sigma_\mathfrak{p} = 1$. Since $c_p \in \mathbf{Z}$, it follows from (3.13) that

$$f_1(x) \mid T_{p,\chi} = c_p f_1(x) \quad \text{and} \quad f_2(x) \mid T_{p,\chi} = c_p f_2(x).$$

Thus we have

$$\sum_{n \geq 1} \tilde{c}_n x^n \mid T_{p,\chi} = (f_1(x) + \varepsilon\alpha^\sigma f_2(x)) \mid T_{p,\chi} = c_p(f_1(x) + \varepsilon\alpha^\sigma f_2(x)) = \tilde{c}_p \sum_{n \geq 1} \tilde{c}_n^{\sigma_\mathfrak{p}} x^n.$$

Hence Lemma 3.13 follows from Proposition 2.6. □

Lemma 3.14. *If p remains prime in K and $\mathfrak{p} \notin S$, then $\hat{L}_\alpha(x_1, x_2)$ over $K_\mathfrak{p}$ is of type $p - \tilde{c}_p T + \chi(p)T^2$.*

Proof. We recall that $c_p \in \mathbf{Z}\sqrt{d}$ and $\tilde{c}_p = \left(c_p/\sqrt{m^2 d}\right)\varepsilon\alpha^\sigma$ by Propositions 3.10 and 3.11 in this case. We also recall $\sigma_{\mathfrak{p}|K} = \sigma$. Since $c_p \in \mathbf{Z}\sqrt{d}$, it follows from (3.13) that

$$f_1(x) \mid T_{p,\chi} = c_p \sqrt{m^2 d}\, f_2(x) \quad \text{and} \quad f_2(x) \mid T_{p,\chi} = \frac{c_p}{\sqrt{m^2 d}} f_1(x).$$

Thus we have

$$\begin{aligned}\sum_{n\geq 1}\tilde{c}_n x^n \mid T_{p,\chi} &= c_p\sqrt{m^2 d}f_2(x)+\varepsilon\alpha^{\sigma}\frac{c_p}{\sqrt{m^2 d}}f_1(x)\\ &= \frac{c_p}{\sqrt{m^2 d}}\varepsilon\alpha^{\sigma}(f_1(x)+\varepsilon\alpha f_2(x)) = \tilde{c}_p\sum_{n\geq 1}\tilde{c}_n^{\sigma_{\mathfrak{p}}}x^n.\end{aligned}$$

Hence Lemma 3.14 follows from Proposition 2.6. □

Lemma 3.15. *If $\mathfrak{p}$ is ramified in K and $\mathfrak{p}\notin S$, then $\hat{L}_{\alpha}(x_1,x_2)$ over $K_{\mathfrak{p}}$ is of type π, where π is a prime element of $\mathcal{O}_{K,\mathfrak{p}}$.*

Proof. We recall that $c_p=\tilde{c}_p=0$ by Propositions 3.10 and 3.11 (resp. by the definition of $L(A,\iota,s)$ and Proposition 3.11) if $d>0$ (resp. if $d<0$). Since $c_p=0$, it follows from (3.13) that

$$f_1(x)\mid T_{p,\chi}=0 \text{ and } f_2(x)\mid T_{p,\chi}=0.$$

Thus we have

$$\sum_{n\geq 1}\tilde{c}_n x^n \mid T_{p,\chi}=0.$$

Hence Lemma 3.15 follows from Proposition 2.7. □

3.3. Finally we give a geometric interpretation of $\tilde{c}_p$ in the case where p remains prime in K and $\mathfrak{p}$ does not divide N_E. In this case we have

$$\left(\frac{c_p}{\sqrt{m^2 d}}\varphi\right)^*((\omega_E)^{\sigma})=\left(\frac{c_p}{\sqrt{m^2 d}}\right)\alpha\omega_E=\varepsilon\tilde{c}_p^{\sigma}\omega_E=\chi(p)\tilde{c}_p^{\sigma}\omega_E.$$

We consider the reduction of $\left(c_p/\sqrt{m^2 d}\right)\varphi$ modulo $\mathfrak{p}$.

In this case we see that p does not divide N_A by Proposition 3.1. We also see that $\mathfrak{p}$ does not divide $N_{E^{\sigma}}$ since $N_{E^{\sigma}}=(N_E)^{\sigma}$. We denote by π_{A_p} the Frobenius p-th power endomorphism of the reduction A_p of A modulo p. We denote by $\pi_{E_{\mathfrak{p}}}$ the Frobenius p-th power homomorphism from the reduction $E_{\mathfrak{p}}$ of E modulo $\mathfrak{p}$ to the reduction $E_{\mathfrak{p}}^{\sigma}$ of E^{σ} modulo $\mathfrak{p}$ and by $\pi_{E_{\mathfrak{p}}^{\sigma}}$ the one from $E_{\mathfrak{p}}^{\sigma}$ to $E_{\mathfrak{p}}$.

Proposition 3.16. *Assume that p remains prime in K and $\mathfrak{p}$ does not divide N_E. Then $\left(c_p/\sqrt{m^2 d}\varphi\right)^*((\omega_E)^{\sigma})=\chi(p)\tilde{c}_p^{\sigma}\omega_E$. Moreover the reduction of $\left(c_p/\sqrt{m^2 d}\right)\varphi$ modulo $\mathfrak{p}$ is $\pi_{E_{\mathfrak{p}}}+\chi(p)p\pi_{E_{\mathfrak{p}}^{\sigma}}^{-1}$.*

Proof. We have the following commutative diagrams:

$$\begin{tikzcd}
A_p \arrow[r, "\pi_{A_p}"] \arrow[d, "(\eta,\eta^\sigma)_{\mathfrak{p}}"'] & A_p \arrow[d, "(\eta^\sigma,\eta)_{\mathfrak{p}}"'] & A_p \arrow[r, "p\pi_{A_p}^{-1}"] \arrow[d, "(\eta,\eta^\sigma)_{\mathfrak{p}}"'] & A_p \arrow[d, "(\eta^\sigma,\eta)_{\mathfrak{p}}"'] \\
E_{\mathfrak{p}} \times E_{\mathfrak{p}}^\sigma \arrow[r, "\pi_{E_{\mathfrak{p}}} \times \pi_{E_{\mathfrak{p}}^\sigma}"] & E_{\mathfrak{p}}^\sigma \times E_{\mathfrak{p}} & E_{\mathfrak{p}} \times E_{\mathfrak{p}}^\sigma \arrow[r, "p\pi_{E_{\mathfrak{p}}^\sigma}^{-1} \times p\pi_{E_{\mathfrak{p}}}^{-1}"] & E_{\mathfrak{p}}^\sigma \times E_{\mathfrak{p}},
\end{tikzcd}$$

where $(\eta, \eta^\sigma)_{\mathfrak{p}}$ and $(\eta^\sigma, \eta)_{\mathfrak{p}}$ are the reductions modulo $\mathfrak{p}$ of (η, η^σ) and of (η^σ, η), respectively. Since $[c_p]_{A_p} = \pi_{A_p} + \chi(p)p\pi_{A_p}^{-1}$, we have

$$\begin{tikzcd}
A_p \arrow[r, "{[c_p]_{A_p}}"] \arrow[d, "(\eta,\eta^\sigma)_{\mathfrak{p}}"'] & A_p \arrow[d, "(\eta^\sigma,\eta)_{\mathfrak{p}}"'] \\
E_{\mathfrak{p}} \times E_{\mathfrak{p}}^\sigma \arrow[r, "\left(\pi_{E_{\mathfrak{p}}} + \chi(p)p\pi_{E_{\mathfrak{p}}^\sigma}^{-1}\right) \times \left(\pi_{E_{\mathfrak{p}}^\sigma} + \chi(p)p\pi_{E_{\mathfrak{p}}}^{-1}\right)"] & E_{\mathfrak{p}}^\sigma \times E_{\mathfrak{p}},
\end{tikzcd}$$

which is the reduction of the diagram:

$$\begin{tikzcd}
A \arrow[r, "{[c_p]_A}"] \arrow[d, "(\eta,\eta^\sigma)"'] & A \arrow[d, "(\eta^\sigma,\eta)"'] \\
E \times E^\sigma \arrow[r, "\left(c_p/\sqrt{m^2d}\right)\varphi \times \left(c_p/\sqrt{m^2d}\right)\varphi^\sigma"] & E^\sigma \times E.
\end{tikzcd}$$

Hence the reduction of $\left(c_p/\sqrt{m^2d}\right)\varphi$ modulo $\mathfrak{p}$ is $\pi_{E_{\mathfrak{p}}} + \chi(p)p\pi_{E_{\mathfrak{p}}^\sigma}^{-1}$. □

4. Formal groups associated to certain Q-curves over quadratic fields

Let notations and assumptions be the same as in the previous sections. In this section, we fix a Weierstrass model

$$Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X + A_6 \ (A_i \in \mathcal{O}_K) \tag{4.1}$$

for E and we take the canonical invariant differential $dX/(2Y + A_1X + A_3)$ as ω_E. We denote by Δ and $\mathfrak{D}_E$ the discriminant of (4.1) and the minimal discriminant of E over K, respectively. Then we can write

$$(\Delta) = \mathfrak{D}_E \cdot \mathfrak{a}^{12}$$

for some integral ideal $\mathfrak{a}$ in $\mathcal{O}_K$.

Let $\hat{E}(x_1, x_2)$ be the formal group associated to the Weierstrass model (4.1). Then $\hat{E}(x_1, x_2)$ is the formal group over $\mathcal{O}_K$ with transformer

$$f(x) = \sum_{n\geq 1} \frac{b_n}{n} x^n, \ \text{where } \omega_E = \sum_{n\geq 1} b_n Z^{n-1} \text{ for } Z := -\frac{X}{Y} \text{ (cf. e.g. [5]; (33.1.14)).}$$

If necessary, we replace S by a larger finite set satisfying the following conditions:

$$(4.2)\qquad \begin{array}{rl} \text{(i)} & \text{If } \alpha/m \notin \mathcal{O}_{K,\mathfrak{p}}, \text{ then } \mathfrak{p} \in S. \\ \text{(ii)} & \text{If either } \mathfrak{p} \text{ or } \mathfrak{p}^{\sigma} \text{ divides } \mathfrak{a}, \text{ then } \mathfrak{p} \in S. \\ \text{(iii)} & \text{If } \mathfrak{p} \text{ is ramified, then } \mathfrak{p} \in S. \\ \text{(iv)} & \text{If } d < 0 \text{ and } \mathfrak{p} \text{ divides } N_E, \text{ then } \mathfrak{p} \in S. \end{array}$$

We note the condition (i) is the same as in (3.11). Then we have:

Theorem 4.1. *$\hat{L}_{\alpha}(x_1, x_2)$ is defined over $\mathcal{O}_{K,S}$, and it is strongly isomorphic over $\mathcal{O}_{K,S}$ to $\hat{E}(x_1, x_2)$.*

Proof. The former part follows from Theorem 3.12. For the proof of the latter part, it is enough to show that $\hat{E}(x_1, x_2)$ over $\mathcal{O}_{K,\mathfrak{p}}$ belongs to the same special element as in Theorem 3.12, that is, $p - \tilde{c}_p T + \chi(p)T^2$, for each prime $\mathfrak{p} \notin S$. Theorem 4.1 follows from Theorem 4.2 as below, since each prime which is not in S is unramified by (iii). □

As below, we fix an unramified prime $\mathfrak{p}$ in K and we denote by p the prime integer lying in $\mathfrak{p}$. We prove:

Theorem 4.2. *Assume that $\mathfrak{p}$ is unramified. Unles $d < 0$ and $\mathfrak{p}$ divides N_E, $\hat{E}(x_1, x_2)$ over $\mathcal{O}_{K,\mathfrak{p}}$ belongs to the following special element*:

$$\begin{cases} p - \tilde{c}_p T + \chi(p)T^2 & \textit{if } \mathfrak{p} \textit{ does not divide } \mathfrak{a} \\ p & \textit{if } \mathfrak{p} \textit{ divides } \mathfrak{a}. \end{cases}$$

Proof. We divide our discussion into two cases. In Lemma 4.3 we deal with the case where $\mathfrak{p}$ divides Δ. Next, in Lemma 4.4 we consider the case where $\mathfrak{p}$ does not divide Δ. Theorem 4.2 follows from these two lemmas. □

Lemma 4.3. *Assume that $\mathfrak{p}$ is unramified and it divides Δ.*
(i) *If $\mathfrak{p}$ divides $\mathfrak{a}$, then $\hat{E}(x_1, x_2)$ over $\mathcal{O}_{K,\mathfrak{p}}$ is of type p.*
(ii) *Assume $d > 0$. If $\mathfrak{p}$ does not divide $\mathfrak{a}$, $\hat{E}(x_1, x_2)$ over $\mathcal{O}_{K,\mathfrak{p}}$ is of type $p - \tilde{c}_p T + \chi(p)T^2$.*

Proof. We show (i) and the case of $a_{\mathfrak{p}} = 0$ in (ii). In the case where either $\mathfrak{p}$ divides $\mathfrak{a}$ or $a_{\mathfrak{p}} = 0$, the reduction of the group law of E modulo $\mathfrak{p}$ is the additive group, and so is the reduction of $\hat{E}(x_1, x_2)$ modulo $\mathfrak{p}$. Thus the transformer $f(x)$ of $\hat{E}(x_1, x_2)$ satisfies

$$(4.3)\qquad f^{-1}(pf(x)) \equiv 0 \mod \mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}.$$

By Propositions 2.2 and 2.4, it follows from (4.3) that

$$pf(x) \equiv 0 \quad \bmod \mathfrak{p}\mathcal{O}_{K,\mathfrak{p}},$$

namely, $\hat{E}(x_1, x_2)$ over $\mathcal{O}_{K,\mathfrak{p}}$ is of type p. This completes the proof of (i). In addition, if $a_\mathfrak{p} = 0$, we have $p = p - \tilde{c}_p T + \chi(p)T^2$ by Lemma 3.5 and (3.9). Thus the case of $a_\mathfrak{p} = 0$ in (ii) is verified.

Now we show the remaining case in (ii). In the case where $\mathfrak{p}$ does not divide $\mathfrak{a}$ and $a_\mathfrak{p} = \pm 1$, p splits completely in K by Lemma 3.6. The reduction of the group law of E modulo $\mathfrak{p}$ is the multiplicative group over the quadratic extension of $\mathcal{O}_K/\mathfrak{p}$ and is isomorphic to it over $\mathcal{O}_K/\mathfrak{p}$ if and only if $a_\mathfrak{p} = 1$. So is the reduction of $\hat{E}(x_1, x_2)$ modulo $\mathfrak{p}$. Thus $\hat{E}(x_1, x_2)$ over $\mathcal{O}_{K,\mathfrak{p}}$ is of type $p - a_\mathfrak{p} T$ by Proposition 3 in [6]. In addition, $p - a_\mathfrak{p} T = p - \tilde{c}_p T + \chi(p)T^2$ by Lemma 3.5 and (3.9). Thus the case of $a_\mathfrak{p} \neq 0$ in (ii) follows. □

Lemma 4.4. *Assume that* $\mathfrak{p}$ *is unramified and it does not divide* Δ. *Then* $\hat{E}(x_1, x_2)$ *over* $\mathcal{O}_{K,\mathfrak{p}}$ *is of type* $p - \tilde{c}_p T + \chi(p)T^2$.

Proof. Since the Frobenius $\mathbf{N}\mathfrak{p}$-th power endomorphism ξ of $E_\mathfrak{p}$ satisfies

$$\xi^2 - a_\mathfrak{p}\xi + \mathbf{N}\mathfrak{p} = 0,$$

$f(x)$ satisfies

$$f^{-1}\left(\mathbf{N}\mathfrak{p} f(x) - a_\mathfrak{p} f\left(x^{\mathbf{N}\mathfrak{p}}\right) + f\left(x^{\mathbf{N}\mathfrak{p}^2}\right)\right) \equiv 0 \quad \bmod \mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}. \tag{4.4}$$

Since $\mathfrak{p}$ is unramified, by Propositions 2.2 and 2.4, (4.4) implies

$$\mathbf{N}\mathfrak{p} f(x) - a_\mathfrak{p} f\left(x^{\mathbf{N}\mathfrak{p}}\right) + f\left(x^{\mathbf{N}\mathfrak{p}^2}\right) \equiv 0 \quad \bmod \mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}. \tag{4.5}$$

We first assume that p splits completely in K. Then (4.5) implies

$$pf(x) - a_\mathfrak{p} f\left(x^p\right) + f\left(x^{p^2}\right) \equiv 0 \quad \bmod \mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}, \tag{4.6}$$

namely, $\hat{E}(x_1, x_2)$ over $\mathcal{O}_{K,\mathfrak{p}}$ is of type $p - a_\mathfrak{p} T + T^2$. In addition, $p - a_\mathfrak{p} T + T^2 = p - \tilde{c}_p T + \chi(p)T^2$ by Lemma 3.5 and (3.9).

Secondly we assume that p remains prime in K and p divides $a_\mathfrak{p}$. Then we have $a_\mathfrak{p} = -2\chi(p)p$ by Lemma 3.8. Since the height of $\hat{E}(x_1, x_2)$ over $\mathcal{O}_{K,\mathfrak{p}}$ is two, it follows from Proposition 2.3 that $\hat{E}(x_1, x_2)$ over $\mathcal{O}_{K,\mathfrak{p}}$ is of type $p + bT + cT^2$ for $b \in \mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$ and $c \in \mathcal{O}_{K,\mathfrak{p}}^*$. From Propositions 2.2 and 2.5, we have

$$\begin{cases} \left(p - bT + c^{-1}T^2\right)\left(p + bT + cT^2\right) = p^2 + 2\chi(p)pT^2 + T^4 \\ -bb^{\sigma_\mathfrak{p}} + pc + pc^{-1} = 2\chi(p)p \\ bc^{-1} - bc = 0. \end{cases} \tag{4.7}$$

In particular, the second equation in (4.7) implies

$$bb^{\sigma_{\mathfrak{p}}} = pc^{-1}(c - \chi(p))^2. \tag{4.8}$$

The orders at $\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$ of p and of c are equal to 1 and 0, respectively. Thus that of the right hand side of (4.8) is odd. On the other hand, that of the left hand side of (4.8) is even unless $b = 0$. Thus we have $b = 0$, and consequently $c = \chi(p)$. Namely, $\hat{E}(x_1, x_2)$ over $\mathcal{O}_{K,\mathfrak{p}}$ is of type $p + \chi(p)T^2$. In addition, $p + \chi(p)T^2 = p + \tilde{c}_p T + \chi(p)T^2$ by Lemma 3.8 and (3.9).

Lastly we assume that p remains prime in K and p does not divide $a_{\mathfrak{p}}$. Since the height of $\hat{E}(x_1, x_2)$ over $\mathcal{O}_{K,\mathfrak{p}}$ is one, it follows from Proposition 2.3 that $\hat{E}(x_1, x_2)$ over $\mathcal{O}_{K,\mathfrak{p}}$ is of type $p - cT$ for $c \in \mathcal{O}_{K,\mathfrak{p}}^*$, that is,

$$pf(x) - cf^{\sigma}(x^p) \equiv 0 \mod \mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}. \tag{4.9}$$

We note that $\hat{E}^{\sigma}(x_1, x_2)$ over $\mathcal{O}_{K,\mathfrak{p}}$ is of type $p - c^{\sigma_{\mathfrak{p}}}T$. By Propositions 2.2 and 2.4, (4.9) implies

$$(f^{\sigma})^{-1}(pc^{-1}f(x)) \equiv x^p \mod \mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}. \tag{4.10}$$

By acting $\sigma_{\mathfrak{p}}$ on (4.10), we have

$$f^{-1}\left(p(c^{\sigma_{\mathfrak{p}}})^{-1}f^{\sigma}(x)\right) \equiv x^p \mod \mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}. \tag{4.11}$$

It follows from the congruences (4.10) and (4.11) that the reduction modulo $\mathfrak{p}$ of the homomorphisms in the left hand side of (4.10) and (4.11) are the formal completion of the Frobenius homomorphisms $\pi_{E_{\mathfrak{p}}}$ and $\pi_{E_{\mathfrak{p}}^{\sigma}}$, respectively.

Since $(p - c^{\sigma_{\mathfrak{p}}}T)c^{\sigma_{\mathfrak{p}}} = c^{\sigma_{\mathfrak{p}}}(p - cT)$, it follows from Proposition 2.1 that $(f^{\sigma})^{-1}(c^{\sigma_{\mathfrak{p}}}f(x))$ is a homomorphism over $\mathcal{O}_{K,\mathfrak{p}}$ from $\hat{E}(x_1, x_2)$ to $\hat{E}^{\sigma}(x_1, x_2)$. Since the composite of $f^{-1}(p(c^{\sigma_{\mathfrak{p}}})^{-1}f^{\sigma}(x))$ and $(f^{\sigma})^{-1}(c^{\sigma_{\mathfrak{p}}}f(x))$ is equal to $[p]_{\hat{E}}(x)$, the reduction modulo $\mathfrak{p}$ of $(f^{\sigma})^{-1}(c^{\sigma_{\mathfrak{p}}}f(x))$ is the formal completion of $p\pi_{E_{\mathfrak{p}}^{\sigma}}^{-1}$. Hence the reduction modulo $\mathfrak{p}$ of $(f^{\sigma})^{-1}((c^{-1}p + \chi(p)c^{\sigma_{\mathfrak{p}}})f(x))$ is that of $\pi_{E_{\mathfrak{p}}} + \chi(p)p\pi_{E_{\mathfrak{p}}^{\sigma}}^{-1}$, and consequently, it follows from Proposition 3.16 that $c^{-1}p + \chi(p)c^{\sigma_{\mathfrak{p}}} = \chi(p)\tilde{c}_p^{\sigma}$, equivalently, $\chi(p)(c^{\sigma_{\mathfrak{p}}})^{-1}p + c = \tilde{c}_p$.

Since $(1 - \chi(p)(c^{\sigma_{\mathfrak{p}}})^{-1}T)(p - cT) = p - \tilde{c}_pT + \chi(p)T^2$, $\hat{E}(x_1, x_2)$ over $\mathcal{O}_{K,\mathfrak{p}}$ is of type $p - \tilde{c}_pT + \chi(p)T^2$. □

REMARK. In Theorem 4.1, we can not exclude the condition (iii) in (4.2) on S. Indeed, there exists the following example.

We take the $\mathbf{Q}$-curve, over $K = \mathbf{Q}\left(\sqrt{-1}\right)$, defined by the Weierstrass model

$$Y^2 + \left(1 - \sqrt{-1}\right)XY + \left(-1 + \sqrt{-1}\right)Y = X^3 - X^2 + \left(3 + 6\sqrt{-1}\right)X + 5 - 3\sqrt{-1},$$

as E. It is the minimal model for the **Q**-curve $E_3^{(5)}$ defined by Hasegawa [4], and it has an isogeny φ over K from E to E^σ of degree 5 with $\alpha = 1 - \sqrt{-1}$. In fact, it is a modular elliptic curve with respect to $\Gamma_0(416)$ (cf. [4]). We see that

$$\Delta = -2^3 \cdot \left(3 - 2\sqrt{-1}\right) \cdot 13 \text{ and } \mathfrak{a} = (1).$$

Thus we can take the empty set as S if we do not assume (iii).

However, $\hat{L}_\alpha(x_1, x_2)$ and $\hat{E}(x_1, x_2)$ are not strongly isomorphic over $\mathcal{O}_{K,\mathfrak{p}}$ at the ramified prime $\mathfrak{p} = \left(1 + \sqrt{-1}\right)$ lying above $p = 2$. Indeed, it follows from Proposition 2.7 that $\hat{L}_\alpha(x_1, x_2)$ over $\mathcal{O}_{K,\mathfrak{p}}$ is of type π for a prime element in $\mathfrak{p}$. On the other hand, $\hat{E}(x_1, x_2)$ over $\mathcal{O}_{K,\mathfrak{p}}$ is not of type π, since it has the transformer $x + \left(-1 + \sqrt{-1}\right)x^2/2 + \left(-1 - 2\sqrt{-1}\right)x^3/3 + \cdots$. Thus these formal groups are not strongly isomorphic over $\mathcal{O}_{K,\mathfrak{p}}$.

Hence Theorem 4.1 does not hold without the condition (iii).

As a corollary of Theorem 4.1 we have:

Corollary 4.5. *The congruence* $b_p \equiv \tilde{c}_p \mod \mathfrak{p}$ *holds for* $\mathfrak{p} \notin S$.

Proof. We have

$$\begin{aligned} 0 &\equiv \left(p - \tilde{c}_p T + \chi(p) T^2\right) * f(x) \\ &\equiv \sum_{n\geq 1} \frac{b_{np}}{n} x^{np} - \tilde{c}_p \sum_{n \geq 1} \frac{b_n^\sigma}{n} x^{np} + \chi(p) \sum_{n\geq 1} \frac{b_n}{n} x^{np^2} \\ &\equiv \sum_{\substack{n\geq 1 \\ (n,p)=1}} \frac{b_{np} - \tilde{c}_p b_n^\sigma}{n} x^{np} - \sum_{n\geq 1} \frac{b_{np^2} - \tilde{c}_p b_{np}^{\sigma_\mathfrak{p}} + \chi(p) p b_n}{np} x^{np^2} \quad \mod \mathfrak{p}. \end{aligned}$$

Thus the congruence $b_{np} - \tilde{c}_p b_n^\sigma \equiv 0 \mod \mathfrak{p}$ holds for each natural number n which is coprime to p. We note that $b_1 = 1$. By substituting $n = 1$ to the congruence, we get Corollary 4.5. □

Together with Weil's inequality: $|c_p| \leq 2\sqrt{p}$ and Corollary 4.5, we see that $\hat{E}(x_1, x_2)$ determines c_p for large prime integers p. We give a numerical example in the following.

EXAMPLE. We put $\zeta := \left(1 + \sqrt{-3}\right)/2$ and $K := \mathbf{Q}(\zeta)$. We take the **Q**-curve, over K, defined by the Weierstrass model

$$Y^2 + (1 - \zeta)XY - (1 + \zeta)Y = X^3 + \zeta X^2 + (19 + \zeta)X + 18 - 30\zeta,$$

as E. Then it is the minimal model for the **Q**-curve $E_{-26}^{(3)}$ defined by Hasegawa [4] and it has an isogeny φ over K from E to E^σ of degree 3 with $\alpha = 2 - \zeta$. Since we

p	$(-3/p)$	b_p	b_p mod p	c_p
2	-1	$-1+\zeta$	$1+\zeta$	$-\sqrt{3}$
3	0	0	0	0
5	-1	$27+7\zeta$	$2+2\zeta$	$2\sqrt{3}$
7	1	$57-196\zeta$	1	1
11	-1	$9403-26149\zeta$	$-2-2\zeta$	$-2\sqrt{3}$
13	1	$-234583+113464\zeta$	2	2
17	-1	$-34917577+7749873\zeta$	$-2-2\zeta$	$-2\sqrt{3}$
19	1	$95051239+3653700\zeta$	-4	-4
23	-1	$1705031103+24795239311\zeta$	$2+2\zeta$	$2\sqrt{3}$
29	-1	$21826646904619-28272514599109\zeta$	0	0

have $\alpha\alpha^\sigma = 3$, we have $\varepsilon = 1$, $m = 1$, $d = 3$. Furthermore it is a modular elliptic curve with respect to $\Gamma_0(63)$ (cf. [4]). We have

$$\Delta = -\zeta^2 \cdot 3^3 \cdot 7^2 \cdot (3-\zeta) \text{ and } \mathfrak{a} = (1).$$

We can take the set of the ramified primes in K as S.

For each prime p such that $2 \leq p \leq 29$, b_p, b_p mod p, c_p are given in the above table. We note that c_p is given by Fourier coefficients of the new form with respect to $\Gamma_0(63)$, corresponding to the restriction A of scalars of E. From the table, we can check Corollary 4.5 for $5 \leq p \leq 29$.

Conversely, by using Corollary 4.5 and Weil's inequality: $|c_p| \leq 2\sqrt{p}$, we can determine c_p $(5 \leq p \leq 29)$ from the values of b_p mod p in the above table.

For example, when $p = 5$, p remains prime in K and we have $\tilde{c}_5 \equiv 2\alpha^\sigma \bmod 5$ by Corollary 4.5. Thus we have $\tilde{c}_5/\alpha^\sigma = c_5/\sqrt{3} \equiv 2 \bmod 5$ by Proposition 3.11. Together with Weil's inequality $|c_5| \leq 2\sqrt{5}$, we see $c_5 = 2\sqrt{3}$.

When $p = 7$, p splits completely in K. Since it follows from Corollary 4.5 that $\tilde{c}_7 \equiv 1 \bmod \mathfrak{p}$ holds for each prime $\mathfrak{p}$ lying above p, we have $\tilde{c}_7 \equiv 1 \bmod 7$. Thus we have $\tilde{c}_7 = c_7 \equiv 1 \bmod 7$ by Proposition 3.11. Together with Weil's inequality $|c_7| \leq 2\sqrt{7}$, we see $c_7 = 1$.

References

[1] M. Atkin and H. Swinnerton-Dyer: *Modular forms on non congruence subgroups*, Proc. Symp. Pure Math XIX. Amer. Math. Soc. Providence (1971).

[2] C. Deninger and E. Nart: *Formal groups and L-series*, Comment. Math. Helv. **65** (1990), 318–333.

[3] A. Fröhlich: Formal groups, Lecture note in Mathematics, Springer, 1968.

[4] Y. Hasegawa: ***Q**-curves over quadratic fields*, Manuscripta Math. **94** (1997), 347–364.

[5] M. Hazewinkel: Formal Groups and Applications, New York, Academic Press, 1978.

[6] T. Honda: *Formal groups and zeta-functions*, Osaka J. Math. **5** (1968), 199–213.

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

[8] T. Honda: *Invariant Differentials and L-functions-Reciplocity law for quadratic fields and elliptic curves over* **Q**, Rend. Sem. Mat. Univ. Padova, **49** (1973), 323–335.

[9] J.S. Milne: *On the Arithmetic of Abelian Varieties*, Invention Math. **17** (1972), 177–190.

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

[11] G. Shimura: *Algebraic number fields and symplectic discontinuous groups*, Ann. of Math. **86** (1967), 503–592.

[12] J.H. Silverman: The Arithmetic of Elliptic curves, Springer, G.T.M. 106.

[13] J. Tate: *The Arithmetic of elliptic curves*, Invent. Math. **23** (1974), 179–206.

[14] M.J. Vélu: *Isogénes entre courbes elliptiques*, C.R. Acad. Sc. Paris, t. **273** (1971), 238–241.

[15] A. Weil: *The field of definition of a variety*, Amer. J. Math. **78** (1956), 509–524.

Department of Mathematics
Graduate School of Science
Osaka University
Toyonaka, Osaka 560-0043, Japan
e-mail: sairaiji@math.sci.osaka-u.ac.jp