TOKYO J. MATH.
VOL. 25, NO. 2, 2002

Isogenies of Degree p of Elliptic Curves over Local Fields and Kummer Theory

Mayumi KAWACHI

Tokyo Metropolitan University

(Communicated by K. Nakamula)

Abstract. Let p be a prime number. In order to calculate the Selmer group of a p-isogeny $\nu : E \to E'$ of elliptic curves, we determine the image of a local Kummer map $E'(K)/\nu E(K) \to H^1(K, \ker\nu)$ over a finite extension K of $\mathbf{Q}_p$. We describe the image using a filtration on a unit group of a local field and the valuation of a coefficient of a leading term in a formal power series of an isogeny.

1. Introduction.

Let $\nu : E \to E'$ be an isogeny of elliptic curves over a number field $\mathcal{K}$. We are interested in its Selmer group $\mathrm{Sel}(\nu)$ which is a subgroup of $H^1(\mathcal{K}, \ker\nu)$ generated by the elements whose local images in $H^1(\mathcal{K}_v, \ker\nu)$ are in $\mathrm{Im}\,\delta_v$ for all primes v. Here δ_v is a connecting homomorphism of an exact sequence over $\mathcal{K}_v$

$$1 \longrightarrow \ker\,\nu \longrightarrow E \xrightarrow{\nu} E' \longrightarrow 1\,.$$

So δ_v fits in an exact sequence

$$1 \longrightarrow E'(\mathcal{K}_v)/\nu E(\mathcal{K}_v) \xrightarrow{\delta_v} H^1(\mathcal{K}_v, \ker\nu) \longrightarrow H^1(\mathcal{K}_v, E)$$

for each v. Let p be a prime number. We assume ν is a p-isogeny, namely $\ker\nu$ is a group of order p. In order to study such Selmer group $\mathrm{Sel}(\nu)$, one of the difficult problems is to know $\mathrm{Im}\,\delta_v$ for primes v over p. If E has good reduction at v and v does not divide p, then $\mathrm{Im}\,\delta_v = H^1_{ur}(\mathcal{K}_v, \ker\nu)$, where $H^1_{ur}(\mathcal{K}_v, \ker\nu) = \ker(H^1(\mathcal{K}_v, \ker\nu) \to H^1(\mathcal{K}_v^{ur}, \ker\nu))$. But if v divides p then the equation does not hold. This paper is devoted to the study of $\mathrm{Im}\,\delta_v$ for v over p. In [1], Berkovič treated the case when E has a complex multiplication and $\nu \in \mathrm{End}(E)$, and expressed $\mathrm{Im}\,\delta_v$ as a subgroup of $\mathcal{K}_v^\times/\mathcal{K}_v^{\times p}$, under the assumption $\mathcal{K}_v \supset \mu_p$ and $E(\mathcal{K}_v) \supset \ker\nu$. In this paper we treat the case when ν is a general p-isogeny.

We also assume that $\mathcal{K}_v \supset \mu_p$ and $E(\mathcal{K}_v) \supset \ker\nu$. Let $\mathcal{O}_v$ be the ring of integers of $\mathcal{K}_v$, $\mathfrak{M}_v$ the maximal ideal of $\mathcal{O}_v$ and U the unit group of $\mathcal{O}_v$. Let $U^0 = U$ and $U^i = 1 + \mathfrak{M}_v^i$ for $i \geq 1$. This gives a filtration on the unit group of $\mathcal{K}_v$, $\mathcal{K}_v^\times \supset U^0 \supset U^1 \supset U^2 \supset \cdots$. It also induces a filtration $\mathcal{K}_v^\times/\mathcal{K}_v^{\times p} \supset C^0 \supset C^1 \supset \cdots \supset C^{pe_0+1} = \{1\}$, where $C^i = U^i/K^{\times p} \cap U^i$ for $i \geq 0$ and e_0 is the ramification index of $\mathcal{K}_v$ over $\mathbf{Q}_p(\zeta_p)$. On the other hand let E

Received March 22, 2000; revised March 5, 2002

be a minimal Weierstrass model over $\mathcal{O}_v$, E_0 be the set of points with nonsingular reduction and $E_i = \{(x, y) \in E(\mathcal{K}_v) \mid v(x) \leq -2i, v(y) \leq -3i\}$ for $i \geq 1$. This gives filtrations $E(\mathcal{K}_v) \supset E_0 \supset E_1 \cdots$ and $E'(\mathcal{K}_v) \supset E'_0 \supset E'_1 \supset \cdots$. The filtration on $E'(\mathcal{K}_v)$ induces the filtration $E'(\mathcal{K}_v)/\nu E(\mathcal{K}_v) \supset D^0 \supset D^1 \supset \cdots$, where $D^i = E'_i(\mathcal{K}_v)/\nu E(\mathcal{K}_v) \cap E'_i(\mathcal{K}_v)$ for $i \geq 0$. Let t be the index such that the generator of $\ker \nu$ is contained in $E_t(\mathcal{K}_v) \setminus E_{t+1}(\mathcal{K}_v)$. We regard δ_v as a homomorphism

$$\delta_v : E'(\mathcal{K}_v)/\nu E(\mathcal{K}_v) \longrightarrow \mathcal{K}_v^\times/\mathcal{K}_v^{\times p}$$

by identifying

$$H^1(\mathcal{K}_v, \ker \nu) \simeq H^1(\mathcal{K}_v, \mu_p) \simeq \mathcal{K}_v^\times/\mathcal{K}_v^{\times p}\,.$$

Then δ_v maps the filtration on $E'(\mathcal{K}_v)/\nu E(\mathcal{K}_v)$ to that on $\mathcal{K}_v^\times/\mathcal{K}_v^{\times p}$. By investigating this map, we will show the following theorem.

THEOREM. 1) *If E has ordinary good reduction over $\mathcal{K}_v$, then*

$$\operatorname{Im} \delta_v = \begin{cases} C^1 & \text{if } \pi(\ker \nu) = \{0\} \\ C^{e_0 p} & \text{if } \pi(\ker \nu) \neq \{0\} \end{cases}$$

where π is the reduction map.

2) *If E has supersingular good reduction over $\mathcal{K}_v$, then*

$$\operatorname{Im} \delta_v = C^{1+(e_0-t)p}\,.$$

3) *If E has multiplicative reduction over $\mathcal{K}_v$ and $p \neq 2$, then E has split multiplicative reduction and*

$$\operatorname{Im} \delta_v = \begin{cases} \mathcal{K}_v^\times/\mathcal{K}_v^{\times p} & \text{if } \ker \nu = \langle \zeta_p \rangle \\ 1 & \text{if } \ker \nu = \langle \zeta_p^i \sqrt[p]{q} \rangle \quad \text{for } i = 0, \cdots, p-1\,. \end{cases}$$

We here remark that if E has bad reduction, $\operatorname{Im} \delta_v$ is not necessarily contained in C^1, as in the case 3). In the case 2), $\operatorname{Im} \delta_v$ can be written by using the parameter t. In §5, we give some examples and calculate that values of t for them.

ACKNOWLEDGMENT. The author wishes to thank Professor M. Kurihara for many valuable comments and suggestions.

2. Preliminaries from formal groups.

2.1. The map δ of formal groups. Let K be a finite extension of $\mathbf{Q}_p$, v be a normalized valuation on K, $\mathcal{O}_K$ the ring of integers of K, $\mathfrak{M}_K$ the maximal ideal in $\mathcal{O}_K$ and $k = \mathcal{O}_K/\mathfrak{M}_K$ the residue field. We put $e = v(p)$. Let ζ_p be a primitive p-th root of unity. Let $\mathfrak{F}_K, \mathfrak{F}'_K$ be formal groups over $\mathcal{O}_K$. Assume that there is an isogeny $\nu : \mathfrak{F}_K \to \mathfrak{F}'_K$ over K. We regard ν as a power series $\nu(z) = a_1 z + a_2 z^2 + \cdots \in \mathcal{O}_K[[z]]$.

LEMMA 2.1.1 (cf. [1], Lemma 1.1.1). *Let $\varphi(z)$ be an isogeny of formal groups defined over a commutative ring of characteristic p. Then there exists an integer $h \geq 0$ such that $\varphi(z)$ is a power series in z^{p^h}.*

PROOF. See [3], Chap. 1, §3, Theorem 2.

By the above lemma, we define the height of an isogeny over $\mathcal{O}_K$ as follows.

1) If there is a positive integer h such that $\nu(z) \equiv \psi(z^{p^h}) \bmod \mathfrak{M}_K$, where $\psi(z) = b_1 z + b_2 z^2 + \cdots \in \mathcal{O}_K[[z]]$, $b_1 \notin \mathfrak{M}_K$ and $b_i \in \mathcal{O}_K$, then the height of ν is defined to be h. We denote h by $\mathrm{ht}(\nu)$.

2) If $\nu(z) \equiv 0 \bmod \mathfrak{M}_K$, then the height of ν is defined to be infinity.

We also define a height of a formal group $\mathfrak{F}_K$ to be the height of $[p]$, the multiplication by p on $\mathfrak{F}_K$. We assume that $\mathrm{ht}(\nu) = 1$ and that the points of $\ker \nu$ are defined over K. For an algebraic extension L, we define $\mathfrak{F}_K(L) = \mathfrak{F}_K(\mathfrak{M}_L)$. For a point P of $\mathfrak{F}_K(L)$, we denote by $z(P)$ the corresponding element of $\mathfrak{M}_L$. We will denote $\mathfrak{F}_K(K)$ simply by $\mathfrak{F}_K$. We define a decreasing filtration on $\mathfrak{F}_K$ by $\mathfrak{F}_K^i = \mathfrak{F}(\mathfrak{M}_K^i)$. So we have $\mathfrak{F}_K = \mathfrak{F}_K^1 \supset \mathfrak{F}_K^2 \supset \cdots$. Put $\mathfrak{D}_K = \mathfrak{F}'_K / \nu\mathfrak{F}_K$. The filtration on $\mathfrak{F}_K$ induces a filtration on $\mathfrak{D}_K$. Namely put $\mathfrak{D}_K^i = \mathfrak{F}_K'^i / \nu\mathfrak{F}_K \cap \mathfrak{F}_K'^i$, then we have a filtration $\mathfrak{D}_K = \mathfrak{D}_K^1 \supset \mathfrak{D}_K^2 \supset \cdots$.

LEMMA 2.1.2 (cf. [1], Lemma 2.1.1). *For i such that $p \nmid i$, we have $a_1 \mid a_i$.*

PROOF. If $a_1 \notin \mathfrak{M}_K$, it is obvious. In the case $a_1 \in \mathfrak{M}_K$, by Corollary 1 in p. 112 of [3], there exists a dual isogeny $\check{\nu}$ of ν, that is $\check{\nu} \circ \nu = [p]$. So we have $a_1 \mid p$. Put $R = \mathcal{O}_K/(a_1)$ and consider an isogeny $\bar{\nu} = \nu \bmod (a_1) : \mathfrak{F}_K/(a_1) \to \mathfrak{F}'_K/(a_1)$. Then R is a ring of characteristic p, and we have an isogeny $\bar{\nu}(z) = \nu(z) \bmod (a_1) = \overline{a_1} z + \cdots + \overline{a_p} z^p + \cdots$ over R. Since $\overline{a_1} = 0$, $\mathrm{ht}(\bar{\nu}) \neq 0$. By Lemma 2.1.1, $\bar{\nu}(z)$ is a power series in z^p. Hence for i such that $p \nmid i$, $\overline{a_i} = 0$, that is $a_1 \mid a_i$.

We define

$$t = \frac{v(a_1)}{p-1}.$$

The following lemma shows that t is an integer.

LEMMA 2.1.3 (cf. [1], Lemma 1.1.2). *For any non-zero point $P \in \ker \nu$, the valuation of $z(P)$ does not depend on the choice of P. In fact P is in $\mathfrak{F}_K^t \setminus \mathfrak{F}_K^{t+1}$, where t is in the number defined above.*

PROOF. Let $z = z(P)$, then $\nu(z) = a_1 z + a_2 z^2 + \cdots + a_p z^p + \cdots = 0$. By Lemma 2.1.2, we have $a_1 \mid a_i$ for $p \nmid i$. So $v(a_1 z) = v(a_p z^p)$. Hence we have $v(z) = \frac{v(a_1)}{p-1} = t$, since $v(a_p) = 0$.

LEMMA 2.1.4 (cf. [1], Lemma 1.1.2).

1) *If $1 \le i < pt$, then*

$$\mathfrak{D}_K^i / \mathfrak{D}_K^{i+1} \simeq \begin{cases} k & \text{if } p \nmid i \\ 1 & \text{if } p \mid i \,. \end{cases}$$

2) *If $i \ge pt + 1$, then $\mathfrak{D}_K^i = 1$.*

3)

$$\mathfrak{D}_K^{pt} / \mathfrak{D}_K^{pt+1} \simeq \mathbf{Z}/p\mathbf{Z}.$$

PROOF. 1) If $1 \leq j < t$, then $\nu(\mathfrak{F}^j) \subset \mathfrak{F}'^{pj}$. So $\tilde{\nu} : \mathfrak{F}^j/\mathfrak{F}^{j+1} \to \mathfrak{F}'^{pj}/\mathfrak{F}'^{pj+1}$ is induced by ν. This is identified with $\tilde{\nu} : k \to k$, $\tilde{\nu}(x) = a_p x^p$, for $x \in k$. Since k is perfect, $\tilde{\nu}$ is an isomorphism. If $i = pj$, then $\mathfrak{D}_K^{pj}/\mathfrak{D}_K^{pj+1} = 1$. If $p \nmid i$ then $\mathfrak{D}_K^i/\mathfrak{D}_K^{i+1} \simeq \mathfrak{F}_K'^i/\mathfrak{F}_K'^{i+1} \simeq k$.

2) If $j \geq t+1$, $\nu(\mathfrak{F}_K^j) \subset \mathfrak{F}_K'^{j+(p-1)t}$. So $\tilde{\nu} : \mathfrak{F}_K^j/\mathfrak{F}_K^{j+1} \to \mathfrak{F}_K'^{j+(p-1)t}/\mathfrak{F}_K'^{j+(p-1)t+1}$ is induced by ν. Put $a_1 = \pi_K^{t(p-1)}u$, where π_K is a prime element of K and $u \in \mathcal{O}_K^\times$. Then $\tilde{\nu} : k \to k$ can be regarded as $\tilde{\nu}(x) = ux$ for $x \in k$. So $\tilde{\nu}$ is an isomorphism. Hence $\nu : \mathfrak{F}_K^j \to \mathfrak{F}_K'^{j+(p-1)t}$ is an isomorphism. So if $i \geq pt+1$, then $\mathfrak{D}_K^i = 1$.

3) For $i = pt$, $\nu(\mathfrak{F}_K^t) \subset \mathfrak{F}_K'^{pt}$. So ν induces $\tilde{\nu} : \mathfrak{F}_K^t/\mathfrak{F}_K^{t+1} \to \mathfrak{F}_K'^{pt}/\mathfrak{F}_K'^{pt+1}$ and $\tilde{\nu}(x) = ux + a_p x^p$ for $x \in k$. This is extended to $\tilde{\nu} : \bar{k} \to \bar{k}$. Because $H^1(k, \bar{k}) = 1$, we have $k/\tilde{\nu}(k) \simeq H^1(k, \ker\tilde{\nu})$. Since $\ker\nu \subset \mathfrak{F}_K^t \setminus \mathfrak{F}_K^{t+1}$, $\ker\tilde{\nu} \simeq \mathbf{Z}/p\mathbf{Z}$ as $\mathrm{Gal}(\bar{k}/k)$-modules. Using the fact that k is finite, we have $k/\tilde{\nu}(k) \simeq H^1(k, \ker\tilde{\nu}) \simeq H^1(k, \mathbf{Z}/p\mathbf{Z}) \simeq \mathbf{Z}/p\mathbf{Z}$.

For $[P] \in \mathfrak{D}_K$, let $Q \in \mathfrak{F}_K(\bar{K})$ be a point such that $P = \nu(Q)$. Let $K' = K(Q)$ be a definition field of Q over K. We prepare the next lemma for Theorem 2.1.6 which is the general p-isogenies' case of Theorem 2.1.1 in Berkovič [1]. Since $\mathrm{ht}(\nu) = 1$, we can write

$$\nu(z) - z(P) = (b_0 + b_1 z + \cdots + z^p)U(z)\,,$$

where $b_i \in \mathcal{O}_K$ and $U(z) \in \mathcal{O}_K[[z]]^\times$, by Weierstrass preparation theorem. So $z(Q)$ is a solution of the equation of degree p. Since $\ker\nu \subset \mathfrak{F}_K(K)$, K'/K is a Galois extension of degree $\leq p$. Let $G = \mathrm{Gal}(K'/K)$. For $\sigma \in G$, $\sigma(Q)$ can be written as $\sigma(Q) = Q \oplus T$, where $T \in \ker\nu$ and $\oplus$ is the formal group law of $\mathfrak{F}$. For a prime element π of K', define $i_G(\sigma) = v_{K'}(\sigma(\pi) - \pi)$. Then it does not depend on the choice of π. By calculating $i_G(\sigma)$, we give a simpler proof of Theorem 2.1.6 than that of [1]. The idea of this proof is adviced by Kurihara.

LEMMA 2.1.5. *Let* $[P] \in \mathfrak{D}_K^i \setminus \mathfrak{D}_K^{i+1}$, *then*

1) *If* $1 \leq i < pt$ *and* $p \nmid i$, *then* K'/K *is a totally ramified extension of degree* p *and* $i_G(\sigma) = pt - i + 1$ *for* $\sigma \in G$.

2) *If* $i = pt$, *then* K'/K *is an unramified extension of degree* p.

PROOF. 1) Let $v_{K'}(z(Q)) = j$ then $v_{K'}(z(\nu(Q))) = pj$. If $v_K = v_{K'}$ then $i = v_K(z(P)) = pj$. This contradicts to $p \nmid i$. So K'/K is a totally ramified extension of degree p. Let $y = z(Q)$ and π_K be a prime element of K. We can choose integers a, b such that $ai + bp = 1$. Then $\pi = y^a \pi_K^b$ is a prime element of K'. We have $i_G(\sigma) = v_{K'}(\frac{\sigma(\pi)}{\pi} - 1) + 1 = v_{K'}(\frac{\sigma(y)^a \pi_K^b}{y^a \pi_K^b} - 1) + 1$. Let $\ker\nu \ni T \neq 0$ and $\xi = z(T)$. Then $v_{K'}(y) = i$, $v_{K'}(\xi) = tp$ and $\sigma(y) = y \oplus \xi = y + \xi + \gamma$, where $v_{K'}(\gamma) > v_{K'}(y + \xi)$. Therefore $\sigma(\pi) = \sigma(y)^a \pi_K^b = (y + \xi + \gamma)^a \pi_K^b = (y^a + a y^{a-1}\xi + \gamma')\pi_K^b$, where $v_{K'}(\gamma') > v_{K'}(a y^{a-1}\xi) > v_{K'}(y^a)$. So $v_{K'}(\frac{\sigma(\pi)}{\pi} - 1) = v_{K'}(\frac{y^a + a y^{a-1}\xi + \gamma'}{y^a} - 1) = v_{K'}(\xi) - v_{K'}(y) = pt - i$. Hence $i_G(\sigma) = pt - i + 1$.

2) Since $a_1 = \pi_K^{(p-1)t}u$, where $u \in \mathcal{O}_K^\times$, $\nu(\pi_K^t x) = \pi_K^{pt}(ux + \cdots + a_p x^p + \cdots)$. Let $z(P) = \pi_K^{pt}\beta$, where $\beta \in \mathcal{O}_K^\times$. Because $P \notin \nu\mathfrak{F}_K$, by Hensel's lemma, the solution

of $\beta \equiv ux + a_p x^p \bmod \mathfrak{M}_K$ is not contained in k. So the solution is contained in a finite extension over k of degree p. Since $u \not\equiv 0 \bmod \mathfrak{M}_K$, $ux + a_p x^p \bmod \mathfrak{M}_K$ is separable. So we have a solution in an unramified extension over K of degree p.

We will consider the special case that $\mathfrak{F}_K$ is isomorphic to $\mathbf{G}_m$, that is $\mathfrak{F}_K = U^1 = 1 + \mathfrak{M}_K$. We take ν to be the p-th power. We assume $K \ni \zeta_p$ and let $e_0 = \frac{e}{p-1}$, $\mathfrak{F}_K^i = U^i = 1 + \mathfrak{M}_K^i$, $\mathfrak{D}_K^i = C_K^i = U^i / K^{\times p} \cap U^i$ and $t = e_0$. We fix an arbitrary formal group and denote it by $\mathfrak{F}_K$ again. Then we will consider the correspondence of $\mathfrak{F}_K$ to $\mathbf{G}_m$. We use the same notation ν, t and $\mathfrak{D}_K$ for $\mathfrak{F}_K$. Let $[P] \in \mathfrak{D}_K$ and $\nu(Q) = P$. If $\mathfrak{F}_K(K) \supset \ker \nu$ and $K \ni \zeta_p$, the definiton field K' of Q is a Kummer extension over K, that is $K' = K(\sqrt[p]{\alpha})$, where $[\alpha] \in K^\times / K^{\times p}$. We can define the map $\delta : \mathfrak{D}_K \to K^\times / K^{\times p}$ by $\delta([P]) = [\alpha]$. Then we have the next theorem.

THEOREM 2.1.6. *Assume that* $\mathfrak{F}_K \supset \ker \nu$ *and* $K \ni \zeta_p$. *If* $[P] \in \mathfrak{D}_K^i \setminus \mathfrak{D}_K^{i+1}$ *for* $1 \le i < pt$ *and* $p \nmid i$ *or* $i = pt$, *then* $\delta([P]) \in C_K^{i+(e_0-t)p} \setminus C_K^{i+(e_0-t)p+1}$.

PROOF. Let K' be a definition field of Q, where $\nu(Q) = P$. If $1 \le i < pt$ and $p \nmid i$, then by Lemma 2.1.5, 1), K'/K is a totally ramified extension and $i_G(\sigma) = pt - i + 1$. On the other hand K' is regarded as a Kummer extension $K(\sqrt[p]{\alpha})$, where $\alpha \in C_K^j \setminus C_K^{j+1}$. Then $[\alpha] = \delta([P])$. Since K'/K is a totally ramified extension, by applying the Lemma 2.1.5, 1) to the case when $\mathfrak{F}_K = \mathbf{G}_m$, that is, ν is p-th power map and $t = e_0$, we have $i_G(\sigma) = pe_0 - j + 1$. So by comparing the two representation of $i_G(\sigma)$, we have $j = i + (e_0 - t)p$. If $i = pt$ then by Lemma 2.1.5, 2), K' is an unramified extension. So $\delta([P]) = [\alpha]$, where $[\alpha] \in C_K^{e_0 p} \setminus C_K^{e_0 p+1}$.

COROLLARY 2.1.7. $\delta(\mathfrak{D}_K^1) = C_K^{1+(e_0-t)p}$.

PROOF. By Theorem 2.1.6, δ induces an injection and by Lemma 2.1.4 this ia an isomorphism of finite groups,

$$\mathfrak{D}_K^i / \mathfrak{D}_K^{i+1} \simeq C_K^{i+(e_0-t)p} / C_K^{i+(e_0-t)p+1} \simeq \begin{cases} k & \text{if } p \nmid i, 1 \le i < pt \\ 1 & \text{if } p \mid i, 1 \le i < pt \,, \end{cases}$$

$$\mathfrak{D}_K^i = C_K^{i+(e_0-t)p} = 1 \quad \text{for } i \ge tp + 1$$

and

$$\mathfrak{D}_K^{pt} / \mathfrak{D}_K^{pt+1} \simeq C_K^{e_0 p} / C_K^{e_0 p+1} \simeq \mathbf{Z}/p\mathbf{Z}\,.$$

Hence we have $\delta(\mathfrak{D}_K^1) = C_K^{1+(e_0-t)p}$.

3. Elliptic curves over K.

3.1. The map δ of elliptic curves. Let E and E' be elliptic curves defined over K, $\nu : E \to E'$ be an isogeny of degree p defined over K and $\check{\nu} : E' \to E$ be a dual isogeny of ν. We assume $E(K) \supset \ker \nu$ and $E'(K) \supset \ker \check{\nu}$. Then we easily see $K \ni \zeta_p$ by using Weil pairing.

An exact sequence

$$1 \longrightarrow \ker\nu \longrightarrow E \longrightarrow E' \longrightarrow 1$$

induces an exact sequence

$$1 \longrightarrow E'(K)/\nu E(K) \xrightarrow{\delta_1} H^1(K, \ker\nu) \longrightarrow H^1(K, E)$$

where δ_1 is a connecting homomorphism. We fix an isomorphism $\ker\nu \simeq \mu_p$. Then we have an isomorphism

$$\kappa : H^1(K, \ker\nu) \xrightarrow{\sim} H^1(K, \mu_p)\,.$$

By Kummer theory, there is an isomorphism

$$\delta_2 : K^\times/K^{\times P} \xrightarrow{\sim} H^1(k, \mu_p)\,.$$

Let $\delta = \delta_2^{-1} \circ \kappa \circ \delta_1$.

Put $K' = K(\nu^{-1}(E(K)))$. Then K'/K is an abelian extension of exponent p, hence a Kummer extension. So there is a subgroup B of $K^\times/K^{\times p}$ such that $K' = K(\sqrt[p]{B})$. Put $D_K = E'(K)/\nu E(K)$.

LEMMA 3.1.1. *The image $\delta(D_K)$ does not depend on the choice of the isomorphism κ. In fact we have $\delta(D_K) = B$.*

PROOF. Let $[P] \in D_K$, $[P] \neq 0$ and $\nu(Q) = P$. Put $L = K(Q)$ and $\delta([P]) = [\alpha]$. By a commutative diagram

$$\begin{array}{ccccccc}
D_L & \longrightarrow & H^1(L, \ker\nu) & \longrightarrow & H^1(L, \mu_p) & \longrightarrow & L^\times/L^{\times p} \\
\uparrow & & \uparrow{\scriptstyle \mathrm{Res}} & & \uparrow{\scriptstyle \mathrm{Res}} & & \uparrow \\
D_k & \xrightarrow{\delta_1} & H^1(K, \ker\nu) & \xrightarrow{\kappa} & H^1(K, \mu_p) & \xrightarrow{\delta_2^{-1}} & K^\times/K^{\times p}\,,
\end{array}$$

we have $\alpha \in L^{\times p}$. So $L = K(\sqrt[p]{\alpha})$ since $[L : K] = p$, this implies $\alpha \in B$. Conversely let $\alpha \in B$ and $L = K(\sqrt[p]{\alpha})$. Then there exists $Q \in \nu^{-1}(E(K))$ such that $L = K(Q)$. By the above diagram, $\delta([\nu(Q)]) = [\alpha]$.

3.2. The case of good reduction. Let E be a minimal Weierstrass model over $\mathcal{O}_K$ and $\pi : E(K) \to \tilde{E}(k)$ be a reduction map. Define $E_0(K) = \pi^{-1}(\tilde{E}_{ns}(k))$, $E_1(K) = \ker\pi$ and for $i \geq 1$, $E_i(K) = \{(x, y) \in E(K) \mid v(x) \leq -2i, v(y) \leq -3i\}$. Let $\nu : E \to E'$ be an isogeny of degree p over K such that E' is a minimal Weierstrass model over $\mathcal{O}_K$. Assume that $\ker\nu \subset E(K)$ and $\ker\check{\nu} \subset E'(K)$. We define $E'_i(K)$ by the same way of $E_i(K)$ for $i \geq 1$. Let $D_K = E'(K)/\nu E(K)$ and $D_K^i = E'_i(K)/\nu E(K) \cap E'_i(K)$ for $i \geq 0$, then we have a filtration $D_K \supset D_K^0 \supset D_K^1 \supset \cdots$.

We make change of variable $z = -x/y$. By mapping (x, y) to z, $E_1(K)$ (resp. $E'_1(K)$) is isomorphic to the formal group $\hat{E}(\mathfrak{M}_K)$ (resp. $\hat{E}'(\mathfrak{M}_K)$). Let Φ be a finite subgroup of $\hat{E}(\mathfrak{M}_K)$ such that $\ker\nu \cap E_1(K) \simeq \Phi$. Then there exists a formal group $\mathfrak{G}$ and an isogeny $\hat{\nu} : \hat{E} \to \mathfrak{G}$ both defined over $\mathcal{O}_K$ such that $\ker\hat{\nu} = \Phi$ by Theorem 4 in p. 112 of [3]. Since E' is a minimal model over $\mathcal{O}_K$, $\mathfrak{G} = \hat{E}'$. Since $\Phi \simeq \ker\nu$ or $\Phi = \{0\}$, $\mathrm{ht}(\hat{\nu}) = 1$ or 0.

If $\mathrm{ht}(\hat{\nu}) = 1$, we denote $\hat{\nu}$ by ν. Then we define $\mathfrak{D}_K = \hat{E}'(\mathfrak{M}_K)/\nu\hat{E}(\mathfrak{M}_K) \cap \hat{E}'(\mathfrak{M}_K)$. By mapping (x, y) to z, $E_i(K) \simeq \hat{E}(\mathfrak{M}_K^i)$ and $E_i'(K) \simeq \hat{E}'(\mathfrak{M}_K^i)$, for $i \geq 1$. Then the map induces $D_K^i \simeq \mathfrak{D}_K^i$, where $\mathfrak{D}_K^i = \hat{E}'(\mathfrak{M}_K^i)/\nu\hat{E}(\mathfrak{M}_K) \cap \hat{E}'(\mathfrak{M}_K^i)$. By Lemma 3.1.1, $\delta(D_K^1) = \delta(\mathfrak{D}_K)$.

LEMMA 3.2.1. *If E has ordinary (resp. supersingular) good reduction, then E' has ordinary (resp. supersingular) good reduction.*

PROOF. By Cor. 7.2 of Chap. 7 in [9], isogenous elliptic curves both have good reduction or neither have. Let $\check{\hat{\nu}}$ be a dual isogeny of $\hat{\nu}$. Since $\check{\hat{\nu}} \circ \hat{\nu} = [p] : \hat{E} \to \hat{E}$ and $\hat{\nu} \circ \check{\hat{\nu}} = [p] : \hat{E}' \to \hat{E}'$, $\hat{E}$ and $\hat{E}'$ have the same height.

In this case $E = E_0$ and $E' = E_0'$. We define $\tilde{\nu} : \tilde{E} \to \tilde{E}'$ to be an isogeny such that $\ker\tilde{\nu} = \pi(\ker\nu)$. By Remark 4.13.2 of Chap. 3 of [9], $\tilde{\nu}$ is defined over k. Then we have a commutative diagram,

(3.1)

$$\begin{array}{ccccccccc}
 & & & & 1 & & 1 & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & \ker\nu & \longrightarrow & \ker\tilde{\nu} & & \\
 & & & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & E_1(K) & \longrightarrow & E_0(K) & \xrightarrow{\pi} & \tilde{E}(k) & \longrightarrow & 1 \\
 & & \nu\downarrow & & \nu\downarrow & & \downarrow\tilde{\nu} & & \\
1 & \longrightarrow & E_1'(K) & \longrightarrow & E_0'(K) & \xrightarrow{\pi} & \tilde{E}'(k) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & E_1'(K)/\nu E_1(K) & \longrightarrow & D_K^0 & \xrightarrow{\pi} & \tilde{E}'(k)/\tilde{\nu}\tilde{E}(k) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & & .
\end{array}$$

LEMMA 3.2.3. *If* $\ker\tilde{\nu} = \{0\}$, *then* $D_K^0/D_K^1 = 1$.

PROOF. Since $\tilde{\nu}$ is injective and $\#\tilde{E}(k) = \#\tilde{E}'(k)$ (see e.g. [2], Chap. 25), $\tilde{\nu}$ is an isomorphism. So $D_K^0/(E_1'(K)/\nu E_1(K)) = 1$ by (3.1). Hence $D_K^0/D_K^1 \simeq \nu E_0(K) \cap E_1'(K)/\nu E_1(K)$. Let $x \in E_0(K)$. If $\nu(x) \in \nu E_0(K) \cap E_1'(K)$ then $\pi(\nu(x)) = 1$. Since $\tilde{E}(k) \simeq \tilde{E}'(k)$, $\pi(x) = 1$. Hence $x \in E_1(K)$. So $\nu E_0(K) \cap E_1'(K)/\nu E_1(K) = 1$.

LEMMA 3.2.4. *If* $\ker\tilde{\nu} \neq \{0\}$, *then* $E_1'(K)/\nu E_1(K) = 1$ *and* $E_1'(K_{ur})/\nu E_1(K_{ur}) = 1$.

PROOF. If $\ker\tilde{\nu} \neq \{0\}$ then $\ker\tilde{\nu} \simeq \ker\nu$. So $\nu : E_1(K) \to E'_1(K)$ is injective. Then the isogeny $\hat{\nu} : \hat{E}(\mathfrak{M}_K) \to \hat{E}'(\mathfrak{M}_K)$ as formal groups is height 0. By the similar argument of Lemma 2.1.4, 2), $\hat{\nu}$ is an isomorphism. Hence $E'_1(K)/\nu E_1(K) = 1$. Let $\pi' : E_0(K_{ur}) \to \tilde{E}(\bar{k})$ be a reduction map. The minimal model of $E/\mathcal{O}_{K_{ur}}$ is equal to that of $E/\mathcal{O}_K$. So $\pi'(\ker\nu) = \pi(\ker\nu) \neq \{0\}$. Therefore we can apply the same argument to $E_1(K_{ur})$.

LEMMA 3.2.5. *If* $\ker\tilde{\nu} \neq \{0\}$, *then* $\delta(D_K^0) = C_K^{e_0 p}$.

PROOF. Let Res_1 be a restriction map of $H^1(K, \ker\nu)$ to $H^1(K_{ur}, \ker\nu)$. Then we will first prove that $\delta_1(D_K^0) = \ker(\mathrm{Res}_1)$, where δ_1 was defined in §3.1. Since $E'_1(K_{ur})/\nu E_1(K_{ur}) = 1$ by Lemma 3.2.4 and $\tilde{E}'(\bar{k})/\tilde{\nu}\tilde{E}(\bar{k}) = 1$, $D_{K_{ur}}^0 = 1$ by the exact sequence

$$E'_1(K_{ur})/\nu E_1(K_{ur}) \longrightarrow D_{K_{ur}}^0 \xrightarrow{\pi} \tilde{E}'(\bar{k})/\tilde{\nu}\tilde{E}(\bar{k}) \longrightarrow 1\,.$$

Since the diagram below is commutative

$$\begin{array}{ccc} H^1(K, \ker\nu) & \xrightarrow{\mathrm{Res}_1} & H^1(K_{ur}, \ker\nu) \\ {\scriptstyle\delta_1}\uparrow & & \uparrow \\ D_K^0 & \longrightarrow & D_{K_{ur}}^0\,, \end{array}$$

$\delta_1(D_K^0) \subset \ker(\mathrm{Res}_1)$. In order to prove equatlity, we consider an exact sequence

$$1 \longrightarrow \tilde{E}'(k)/\tilde{\nu}\tilde{E}(k) \xrightarrow{\widetilde{\delta_1}} H^1(k, \ker\tilde{\nu}) \longrightarrow H^1(k, \tilde{E})\,.$$

Since $H^1(k, \tilde{E}) = 1$ (see e.g. [2], Chap. 25), $\widetilde{\delta_1}$ is an isomorphism. By Lemma 3.2.4, $E'_1(K)/\nu E_1(K) = 1$. So $D_K^0 \simeq \tilde{E}'(k)/\tilde{\nu}\tilde{E}(k) \simeq H^1(k, \ker\tilde{\nu}) \simeq \ker(\mathrm{Res}_1)$. Here, the last isomorphism is a consequence of the exact sequence

$$1 \longrightarrow H^1(k, \ker\tilde{\nu}) \longrightarrow H^1(K, \ker\nu) \longrightarrow H^1(K_{ur}, \ker\nu)\,.$$

Hence $\delta_1(D_K^0) = \ker(\mathrm{Res}_1)$.

Next, let δ_2 be defined in §3.1 and Res_2 be a restriction map of $H^1(K, \mu_p)$ to $H^1(K_{ur}, \mu_p)$. By Lemma 2.1.5, 2), $\delta_2(C_K^{e_0 p}) \subset \ker(\mathrm{Res}_2)$. Since $C_K^{e_0 p} \simeq \mathbf{Z}/p\mathbf{Z}$ by Lemma 2.1.4, 3) and $|\ker(\mathrm{Res}_2)| = |H^1(K_{ur}/K, \mu_p)| = p$, we have $\delta_2(C_K^{e_0 p}) = \ker(\mathrm{Res}_2)$.

We fix an isomorphism $\ker\nu \simeq \mu_p$. Then we have an isomorphism κ and a commutative diagram

$$\begin{array}{ccc} H^1(K, \ker\nu) & \xrightarrow{\kappa} & H^1(K, \mu_p) \\ {\scriptstyle\mathrm{Res}_1}\downarrow & & \downarrow{\scriptstyle\mathrm{Res}_2} \\ H^1(K_{ur}, \ker\nu) & \longrightarrow & H^1(K_{ur}, \mu_p)\,. \end{array}$$

Therefore $\kappa \circ \delta_1(D_K^0) = \kappa(\ker(\mathrm{Res}_1)) = \ker(\mathrm{Res}_2) = \delta_2(C_K^{e_0 p})$. Since $\delta = \delta_2^{-1} \circ \kappa \circ \delta_1$ and $\mathrm{Im}\,\delta$ does not depend on the choice of κ by Lemma 3.1.1, we have $\delta(D_K^0) = C_K^{e_0 p}$.

THEOREM 3.2.6. 1) *If E has ordinary good reduction over K, then*

$$\delta(D_K) = \begin{cases} C_K^{e_0 p} & \text{if } \ker \tilde{\nu} \neq \{0\} \\ C_K^1 & \text{if } \ker \tilde{\nu} = \{0\} \,. \end{cases}$$

2) *If E has supersingular good reduction over K and the generator of* $\ker \nu$ *is contained in $E_t(K) \setminus E_{t+1}(K)$, then*

$$\delta(D_K) = C_K^{1+(e_0-t)p} \,.$$

PROOF. 1) If E has ordinary good reduction, then there is an exact sequence

$$1 \longrightarrow X_p \longrightarrow E[p] \xrightarrow{\bar{\pi}} \tilde{E}[p] \longrightarrow 1$$

where $\bar{\pi}$ is a reduction mod $\mathfrak{M}_{\bar{K}}$ and the kernel X_p is a cyclic group order p. If $\ker \tilde{\nu} = \{0\}$ then $D_K^0 = D_K^1$ by Lemma 3.2.3. Since $t = e_0$, $\delta(D_K) = C_K^1$ by Corollary 2.1.7. If $\ker \tilde{\nu} \neq \{0\}$ then we can apply Lemma 3.2.5 to this case.

2) If E has supersingular good reduction then $\tilde{E}[p] = \{0\}$, so $\ker \tilde{\nu} = \{0\}$. By Lemma 3.2.3, $D_K^0 = D_K^1$. So $\delta(D_K) = C_K^{1+(e_0-t)p}$ by Corollary 2.1.7.

4. Multiplicative reduction case.

4.1. Multiplicative reduction case.

LEMMA 4.1.1. *If E has multiplicative* (*resp. additive*) *reduction over K, then E' has multiplicative* (*resp. additive*) *reduction.*

PROOF. Let l be a prime number distinct from p, and let $T_l(E)$ and $T_l(E')$ be the Tate modules. Then $\nu : T_l(E) \to T_l(E')$ is an isomorphism. The action of $\mathrm{Gal}(\bar{K}/K)$ is compatible with ν. So the representations $\rho : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}(T_l(E))$ and $\rho' : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}(T_l(E'))$ have the same images. By [4], E has semistable reduction if and only if $\mathrm{Im}\,\rho|_I$ is unipotent, where I is the inertia group of $\mathrm{Gal}(\bar{K}/K)$. This is equivalent to the unipotentness of $\mathrm{Im}\,\rho'|_I$. Hence E' has semistable reduction. By Lemma 3.2.1 the reduction type of E is equal to that of E'.

If E has multiplicative reduction, then $v(j(E)) < 0$. So by [10], Chap. 5, Theorem 5.3, there exists a unique $q \in K^\times$, with $v(q) > 0$ such that E is isomorphic over $\bar{K}$ to the Tate curve E_q. Then we define the isomorphism by $\psi : E_q \to E$. By Lemma 4.1.1, E' also has multiplicative reduction. So we can define an isomorphism $\psi' : E_{q'} \to E'$ over $\bar{K}$ for a unique $q' \in K^\times$ with $v(q') > 0$. Let L be a unique quadratic extension over K which is unramified. Since E_q (resp. $E_{q'}$) is defined over K by [10], Chap. 5, Theorem 3.1 (a), E_q (resp. $E_{q'}$) is a quadratic twist of E (resp. E') that is, ψ (resp. ψ') is defined over L. If ψ (resp. ψ') is defined over K, E (resp. E') has split multiplicative reduction, otherwise it has non-split multiplicative reduction.

Let $\phi : \bar{K}^\times/\langle q\rangle \to E_q$ (resp. $\phi' : \bar{K}^\times/\langle q'\rangle \to E_{q'}$) be an isomorphism defined by a power series of q (resp. q') as in [10], Chap. 5, Theorem 3.1 (c). This isomorphism is compatible with the action of $\mathrm{Gal}(\bar{K}/K)$.

For $\psi^{-1}(\ker\nu)$, there exists a Tate curve $E_q/\psi^{-1}(\ker\nu)$ and an isogeny $E_q \to E_q/\psi^{-1}(\ker\nu)$. Then ψ induces an isomorphism $E_q/\psi^{-1}(\ker\nu) \to E/\ker\nu$. So $E_q/\psi^{-1}(\ker\nu)$ must be $E_{q'}$, since $E_{q'}$ is a unique Tate curve isomorphic to E'.

Then there exists an isogeny $\bar{K}^\times/\langle q\rangle \to \bar{K}^\times/\langle q'\rangle$ whose kernel is $(\psi\circ\phi)^{-1}(\ker\nu)$. The kernel of multiplication-by-p map of $\bar{K}^\times/\langle q\rangle$ is $\langle \zeta_p^i, \sqrt[p]{q}\rangle$, where $i = 0, \cdots, p-1$. So $(\psi\circ\phi)^{-1}(\ker\nu)$ is one of the 1-dimensional subspaces of this $\mathbf{F}_p$-vector space $\langle \zeta_p^i, \sqrt[p]{q}\rangle$. Hence it is $\langle \zeta_p^i \sqrt[p]{q}\rangle$ or $\langle \zeta_p\rangle$.

LEMMA 4.1.2. *Assume that* $p \neq 2$, $\ker\nu \subset E(K)$ *and* $\zeta_p \in K$. *Then both E and E′ have split multiplicative reduction.*

PROOF. Assume that E has non-split multiplicative reduction. Let $N_{L/K} : L^\times/q^{\mathbf{Z}} \to K^\times/q^{2\mathbf{Z}}$ be a norm map. Then by [10], Chap. 5, Corollary 5.4, for $u \in L^\times/q^{\mathbf{Z}}$, $\psi\circ\phi(u) \in E(K)$ is equivalent to $N_{L/K}(u) \in q^{\mathbf{Z}}/q^{2\mathbf{Z}}$. Since $(\psi\circ\phi)^{-1}(\ker\nu) = \langle \zeta_p^i \sqrt[p]{q}\rangle$ for $i = 0, \cdots, p-1$ or $\langle\zeta_p\rangle$ and $\ker\nu \subset E(K)$, it must be $N_{L/K}(\sqrt[p]{q}) \in q^{\mathbf{Z}}/q^{2\mathbf{Z}}$ or $N_{L/K}(\zeta_p) = \zeta_p^2 \in q^{\mathbf{Z}}/q^{2\mathbf{Z}}$. Since $p \neq 2$, this is a contradiction. So E has split multiplicative reduction.

In this case, ψ is an isomorphism over K. So the induced isomorphism $E_q/\psi^{-1}(\ker\nu) \to E/\ker\nu$ is defined over K, that is, ψ' is an isomorphism over K. Hence E' has split multiplicative reduction.

By the above lemma, we can identify E (resp. E') with E_q (resp. $E_{q'}$). Hence we have the next proposition.

PROPOSITION 4.1.3. *Assume that* $p \neq 2$, $\ker\nu \subset E(K)$ *and* $\zeta_p \in K$. *Then*

$$\begin{cases} \operatorname{Im}\delta = K^\times/K^{\times p} & \textit{if} \ \ker\nu = \langle\zeta_p\rangle \\ \operatorname{Im}\delta = 1 & \textit{if} \ \ker\nu = \langle\zeta_p^i \sqrt[p]{q}\rangle \quad \textit{for} \ i = 0, \cdots, p-1\,. \end{cases}$$

PROOF. If $\ker\nu = \langle\zeta_p\rangle$, then $q' = q^p$ and the isogeny is written by

$$\nu : \bar{K}^\times/\langle q\rangle \longrightarrow \bar{K}^\times/\langle q'\rangle$$
$$z \bmod \langle q\rangle \longmapsto z^p \bmod \langle q^p\rangle\,.$$

For any $[z] \in K^\times/\langle q\rangle$, we have $K(\nu^{-1}([z])) = K(\sqrt[p]{z})$. Hence by Lemma 3.1.1, $\operatorname{Im}\delta = K^\times/K^{\times p}$.

If $\ker\nu = \langle\zeta_p^i \sqrt[p]{q}\rangle$, then $q' = \zeta_p^i \sqrt[p]{q}$ and ν is written by

$$\nu : \bar{K}^\times/\langle q\rangle \longrightarrow \bar{K}^\times/\langle q'\rangle$$
$$z \bmod \langle q\rangle \longmapsto z \bmod \langle\zeta_p^i \sqrt[p]{q}\rangle\,.$$

For $[z] \in K^\times/\langle\zeta_p^i \sqrt[p]{q}\rangle$, $K(\nu^{-1}([z])) = K(\sqrt[p]{q})$. Our assumption $\ker\nu \subset E(K)$ implies $\langle\zeta_p^i \sqrt[p]{q}\rangle \subset K^\times/\langle q\rangle$. So we have $\sqrt[p]{q} \in K$. Hence $K(\nu^{-1}([z])) = K$. So by Lemma 3.1.1, $\operatorname{Im}\delta = 1$.

5. The calculation of Im δ.

5.1. **p-isogenies over Q.** In this section we consider elliptic curves E and E' over $\mathbf{Q}$ and a p-isogeny $\nu : E \to E'$ over $\mathbf{Q}$. Take $\mathcal{K} = \mathbf{Q}(\ker \nu, \mu_p)$. Let K be a completion of $\mathcal{K}$ at a place of $\mathcal{K}$ above p.

LEMMA 5.1.1 *$K/\mathbf{Q}_p(\mu_p)$ is an unramified extension. So $e_0 = v_K(p)/(p-1) = 1$.*

PROOF. Following Mazur [6], §5, we consider the following character. Let $\chi : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}(\ker \nu) \simeq \mathbf{F}_p^\times$ be defined by $T^\sigma = \chi(\sigma)T$, where $\langle T \rangle = \ker \nu$. Since $\mathbf{Q}(\ker \nu)/\mathbf{Q}$ is an abelian extension, χ factors through $\mathrm{Gal}(\mathbf{Q}^{ab}/\mathbf{Q})$. By local class field theory, there exists an isomorphism $\rho : U(\mathbf{Q}_p) \simeq \mathrm{Gal}(\mathbf{Q}_p^{ab}/\mathbf{Q}_p^{ur})$ and we restrict χ to $\mathrm{Gal}(\mathbf{Q}_p^{ab}/\mathbf{Q}_p)$. So we have a homomorphism

$$\varepsilon : U(\mathbf{Q}_p) \xrightarrow{\rho} \mathrm{Gal}(\mathbf{Q}_p^{ab}/\mathbf{Q}_p) \xrightarrow{\chi} \mathbf{F}_p^\times .$$

Since $U(\mathbf{Q}_p) \simeq \mathbf{Z}_p^\times \simeq \mathrm{Gal}(\mathbf{Q}_p(\mu_{p^\infty})/\mathbf{Q}_p)$, ε is the cyclotomic character. Then there exists $k \in \mathbf{Z}$ such that $\chi = \varepsilon^k \alpha$, where α is an unramified character at p. Then the character group which corresponds to $\mathbf{Q}(\mu_p)$ (resp. $\mathbf{Q}(\ker \nu)$) is $\langle \varepsilon \rangle$ (resp. $\langle \chi \rangle$). So the character group which corresponds to $\mathcal{K}$ is $\langle \varepsilon, \chi \rangle = \langle \varepsilon, \alpha \rangle$.

5.2. **The case of $p = 5$.** We study an elliptic curve E over $\mathbf{Q}$ with a 5-isogeny ν over $\mathbf{Q}$. By Lecacheux [5], the j-invariant of such a curve is $j = -(n^2 - 10n + 5)^3/n$, where $n \in \mathbf{Q}$ and E is isomorphic to a curve

$$Y^2 = X^3 - (5n - 10n + n^2)\frac{d}{48}X + (-n - 4n + n^2)\frac{d^2}{864}$$

with discriminant $\Delta = -nd^3$, where $d = n^2 - 22n + 125$. Let $\mathcal{K} = \mathbf{Q}(\mu_5, \ker \nu)$ and $K = \mathbf{Q}_5(\mu_5, \ker \nu)$.

EXAMPLE 5.2.1. We take $n = 10$, then $j = -25/2$, $\Delta = -2 \cdot 5^4$ and $E_{(10)}$ over $\mathbf{Q}$ is written by

$$Y^2 = X^3 - \frac{25}{48}X + \frac{1475}{864} .$$

By [5], the coordinate of a generator P of $\ker \nu$ is $(x_P, y_P) = (\frac{5+6\sqrt{5}}{12}, \frac{\sqrt{50+10\sqrt{5}}}{4})$. So $\mathcal{K} = \mathbf{Q}(\zeta_5, \sqrt{-1})$. Since $e_0 = 1$ by Lemma 5.1.1, the ramification index of $K/\mathbf{Q}_5$ is 4. By Tate's algorithm [11], we can verify that a minimal model of $E_{(10)}$ over $\mathcal{O}_K$ is written by

$$Y^2 = X^3 - \frac{5}{48}X + \frac{59\sqrt{5}}{864} .$$

Then $E_{(10)}$ has additive reduction over $\mathcal{O}_K$ with type IV and $v_K(\Delta) = 4$. By this change of coordinates, we have $v_K(x_P) = v_K(y_P) = 0$. Put $z_P = -x_P/y_P$. We have $v_K(z_P) = 0$.

Let L be an extension over K with the ramification index 3. Since $j \equiv 0 \bmod 5$, E has supersingular good reduction over $\mathcal{O}_L$. Let π_L be a prime element of $\mathcal{O}_L$. Then a minimal model over $\mathcal{O}_L$ is written by

$$Y^2 = X^3 - \frac{5}{48\pi_L^4}X + \frac{59}{864u_1},$$

where $u_1 = \pi_L^6/\sqrt{5}$. By this change of coordinates, we have $v_L(x_P) = -2$ and $v_L(y_P) = -3$. Then $t = v_L(z_P) = 1$. Hence $\delta(D_L) = C_L^{1+(3-1)\cdot 5} = C_L^{11}$, by Theorem 3.2.6.

EXAMPLE 5.2.2. If $n = \frac{25}{2}$, $\Delta = -\frac{5^8}{2^6}$ and $j = -\frac{121945}{32}$ and $E_{(\frac{25}{2})}$ over $\mathbf{Q}$ is written by

$$Y^2 = X^3 - \frac{91\cdot 5^3}{2^8\cdot 3}X - \frac{421\cdot 5^4}{2^{11}\cdot 3^3}.$$

If $E'_{(10)}$ is 5-isogenous to $E_{(10)}$ over $\mathbf{Q}$, then $E_{(\frac{25}{2})}$ is isomorphic to $E'_{(10)}$ over $\mathbf{Q}(\sqrt{-1})$. The generator of $\ker\nu$ is $(x_P, y_P) = (-\frac{35}{48}, \frac{5\sqrt{5}}{4})$. So $\mathcal{K} = \mathbf{Q}(\zeta_5)$. By change of coordinates, $E_{(\frac{25}{2})}$ over $\mathcal{O}_K$ is written by

$$Y^2 = X^3 - \frac{91\cdot 5}{768}X - \frac{421\cdot 5}{55296}.$$

We have $v_K(x_P) = v_K(y_P) = 0$.

Let L be an extension over K with the ramification index 3. By change of coordinates, we have $v_L(\Delta) = 0$. So $E_{(\frac{25}{2})}$ is good reduction over $\mathcal{O}_L$. By this change of coordinates, $v_L(x_P) = -4$ and $v_L(y_P) = -6$. So $t = v_L(z_P) = 2$. Hence $\delta(D_L) = C_L^{1+(3-2)\cdot 5} = C_L^6$.

EXAMPLE 5.2.3. If $n = 7$, $j = 4096/7$, $\Delta = -2^6\cdot 5^3\cdot 7$ and $E_{(7)}$ over $\mathbf{Q}$ is written by

$$Y^2 = X^3 - \frac{20}{3}X + \frac{250}{27}.$$

Then generator of $\ker\nu$ is $(x_P, y_P) = (\frac{5+3\sqrt{5}}{3}, \sqrt{50+20\sqrt{5}})$. So $\mathcal{K} = \mathbf{Q}(\zeta_5, \sqrt{-2})$. Since $e_0 = 1$, the ramification index of $K/\mathbf{Q}_5$ is 4. By change of coordinates, $v_K(\Delta) = 0$. Therefore $E_{(7)}$ has good reduction over K and a minimal model of $E_{(7)}$ is written by

$$Y^2 = X^3 - \frac{4}{3}X + \frac{10\sqrt{5}}{27}.$$

By this change of coordinates, $v_K(x_P) = v_K(y_P) = 0$. So $t = v_K(z_P) = 0$. Because $j \not\equiv 0 \bmod 5$, $E_{(7)}$ has ordinary good reduction. Since $\ker\nu \not\subset E_{(7)_1}(K)$, $\operatorname{Im}\delta = C^{e_0 p} = C^5$ by Theorem 3.2.6.

References

[1] V. G. BERKOVIČ, On the division by an isogeny of the points of an elliptic curves, Math. USSR Sbornik **22** (1974), 473–492.

[2] J. W. S. CASSELS, *Lectures on Elliptic Curves*, Cambridge Univ. Press. (1991).

[3] A. FRÖHLICH, *Formal Groups*, Lecture Notes in Math. **74** (1968), Springer.

[4] A. GROTHENDIECK, *Modèles de Néron et monodromie*, SGA71 exposé IX, Lecture Notes in Math. **288** (1972), Springer, 313–523.

[5] O. LECACHEUX, *Courbes elliptiques et groupes de classes d'idéaux de corps quartiques*, C.R. Acad. Sci. Paris. t. **316**, Série I (1993), 217–220.

[6] B. MAZUR, Rational isogenies of prime degree, Invent. Math. **44** (1978), 129–162.

[7] J. P. SERRE, Propriété galoisiennes des points d'order fini des courbes elliptiques, Invent. Math. **15** (1972), 259–331.

[8] J. P. SERRE, *Local Fields*, Grad. Texts in Math. **67** (1979), Springer.

[9] J. H. SILVERMAN, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. **106** (1985), Springer.

[10] J. H. SILVERMAN, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts in Math. **151** (1994), Springer.

[11] J. TATE, Algorithm for determining the type of a singular fiber in an elliptic pencil, *Moduler Functions of One Variable IV*, Lecture Notes in Math. **476** (1975), Springer, 33–52.

Present Address:
DEPARTMENT OF MATHEMATICS, TOKYO METROPOLITAN UNIVERSITY,
MINAMI-OHSAWA, HACHIOJI-SHI, TOKYO, 192–0397 JAPAN.
e-mail: kawachi@comp.metro-u.ac.jp