J. Math. Soc. Japan
Vol. 56, No. 2, 2004

A classification of $\boldsymbol{Q}$-curves with complex multiplication

By Tetsuo Nakamura

(Received Jan. 31, 2002)
(Revised Dec. 16, 2002)

Abstract. Let H be the Hilbert class field of an imaginary quadratic field K. An elliptic curve E over H with complex multiplication by K is called a $\boldsymbol{Q}$-curve if E is isogenous over H to all its Galois conjugates. We classify $\boldsymbol{Q}$-curves over H, relating them with the cohomology group $H^2(H/\boldsymbol{Q}, \pm 1)$. The structures of the abelian varieties over $\boldsymbol{Q}$ obtained from $\boldsymbol{Q}$-curves by restriction of scalars are investigated.

1. Introduction.

Let K be an imaginary quadratic field and H the Hilbert class field of K. Let E be an elliptic curve over H with complex multiplication by K. We say that E is a $\boldsymbol{Q}$-curve if E and E^{σ} are isogenous over H for all $\sigma \in \mathrm{Gal}(H/\boldsymbol{Q})$. Denote by ψ_E the Hecke character of H associated with E. Then E is a $\boldsymbol{Q}$-curve if and only if $\psi_E = \psi_E^{\sigma}$ for all $\sigma \in \mathrm{Gal}(H/\boldsymbol{Q})$.

As in the case without complex multiplication (see [**Q**]), we attach to a $\boldsymbol{Q}$-curve E a two-cocycle class $c(E) \in H^2(H/\boldsymbol{Q}, K^{\times})$. For $\boldsymbol{Q}$-curves E, E', we see that $c(E) = c(E')$ if and only if $\psi_E = \psi_{E'} \cdot \chi \circ N_{K/\boldsymbol{Q}}$ with a quadratic Dirichlet character χ. Let Γ be the subset of $H^2(H/\boldsymbol{Q}, K^{\times})$ consisting of $c(E)$ for all $\boldsymbol{Q}$-curves E over H. We show that there exists a bijection between Γ and a subspace Y of $H^2(H/\boldsymbol{Q}, \pm 1)$ over $\boldsymbol{F}_2$. Relating Y to an embedding problem associated with the exact sequence

$$1 \to \pm 1 \to G \to \mathrm{Gal}(H/\boldsymbol{Q}) \to 1,$$

we characterize the structure of Y and, as a consequence, we obtain that $\dim_{\boldsymbol{F}_2} Y = t(t-1)/2$, where t is the number of distinct prime factors of the discriminant of K. In some case where K is called exceptional, there are no $\boldsymbol{Q}$-curves with complex multiplication over H. Replacing H by the ring class field of conductor 2, we obtain a similar classification of $\boldsymbol{Q}$-curves (Theorem 2).

The abelian variety $B = R_{H/K}E$ obtained by restriction of scalars from a $\boldsymbol{Q}$-curve E can be defined over $\boldsymbol{Q}$. The structures of the endomorphism algebras $R = \mathrm{End}_{\boldsymbol{Q}} B \otimes \boldsymbol{Q}$ are studied according to this classification (Section 5). Some examples are discussed in the last section.

Notation. Throughout the paper we fix the following notation.
K: an imaginary quadratic field of discriminant $D \neq -3, -4$.
t: the number of distinct primes dividing D.

2000 *Mathematics Subject Classification*. Primary 11G05; Secondary 11G10, 11G15.
Key Words and Phrases. $\boldsymbol{Q}$-curve, elliptic curve, complex multiplication, embedding problem, restriction of scalars.

H: the Hilbert class field of K.
Cl_K: the ideal class group of K.
$\mathfrak{g}$: $\mathrm{Gal}(H/K)$.
ρ: the complex conjugation.
j_E: the j-invariant of an elliptic curve E.

All $\boldsymbol{Q}$-curves treated in this paper are assumed to have complex multiplication. The symbol "dim" always refers to the dimension over $\boldsymbol{F}_2$. Galois cohomology groups $H^i(\mathrm{Gal}(M/L), A)$ are denoted by $H^i(M/L, A)$. We call K exceptional if the discriminant D of K is of the form

$$D = -4p_1 \cdots p_{t-1} \quad (t \geq 2)$$

where $p_1, \ldots, p_{t-1}$ are primes satisfying $p_1 \equiv \cdots \equiv p_{t-1} \equiv 1 \mod 4$.

2. Quadratic characters of local unit groups of K.

Let p be a rational prime and $\mathfrak{p}$ a prime ideal of K dividing p. Denote by $U_\mathfrak{p}$ the group of local units for $\mathfrak{p}$ and put $U_p = \prod_{\mathfrak{p}|p} U_\mathfrak{p}$. Let X_p be the set of characters $\lambda : U_p \to \pm 1$. We regard X_p as a vector space over $\boldsymbol{F}_2$. The complex conjugation ρ acts on X_p and put $X_p^0 = \{\lambda \in X_p \mid \lambda^\rho = \lambda\}$. We shall determine a basis of X_p.

1) p is odd. Denote by $\kappa_p : \boldsymbol{Z}_p^\times \to \pm 1$ the unique non-trivial character and put $\lambda_p = \kappa_p \circ N_{K/\boldsymbol{Q}}$.

Proposition 1. (i) *Suppose that p splits in K, i.e. $(p) = \mathfrak{p}\mathfrak{p}^\rho$. Let $\lambda_\mathfrak{p} : U_\mathfrak{p} \cong \boldsymbol{Z}_p^\times \to \pm 1$ be the unique non-trivial character. Then $\lambda_\mathfrak{p}\lambda_\mathfrak{p}^\rho = \kappa_p \circ N_{K/\boldsymbol{Q}}$ and $X_p = \langle \lambda_\mathfrak{p}, \lambda_\mathfrak{p}^\rho \rangle$ and $X_p^0 = \langle \lambda_p \rangle$.*

(ii) *If p is inert in K, then $X_p = X_p^0 = \langle \lambda_p \rangle$.*

(iii) *If p is ramified in K, then there exists a unique non-trivial character η_p such that $\eta_p(-1) = (-1)^{(p-1)/2}$ and $X_p = X_p^0 = \langle \eta_p \rangle$.*

2) $p = 2$. Let κ_4, κ_8 be the characters of $\boldsymbol{Z}_2^\times$ satisfying

$$\kappa_4(n) = (-1)^{(n-1)/2}, \quad \kappa_8(n) = (-1)^{(n^2-1)/8} \quad \text{for odd integers } n.$$

We put $\varepsilon_4 = \kappa_4 \circ N_{K/\boldsymbol{Q}}$, $\varepsilon_8 = \kappa_8 \circ N_{K/\boldsymbol{Q}}$.

If 2 is inert in K, we have

$$U_2/U_2^2 = \langle -1, 1+2\omega, 1+4\omega \rangle \cong (\boldsymbol{Z}/2\boldsymbol{Z})^3 \quad \text{with } \omega^2 + \omega + 1 = 0.$$

Define $\nu \in X_2$ by $\mathrm{Ker}\,\nu = \langle 1+2\omega, 1+4\omega \rangle$. We have $\nu\nu^\rho = \varepsilon_4$.

If 2 is ramified in K, put $D = 4m$. If m is odd, we have

$$U_2/U_2^2 = \langle \sqrt{m}, 3-2\sqrt{m}, 5 \rangle \cong (\boldsymbol{Z}/2\boldsymbol{Z})^3.$$

We define ν and $\eta_{-4} \in X_2$ by $\mathrm{Ker}\,\nu = \langle \sqrt{m}, 3-2\sqrt{m} \rangle$ and $\mathrm{Ker}\,\eta_{-4} = \langle 3-2\sqrt{m}, 5 \rangle$. Then $\nu\nu^\rho = \varepsilon_8$, $\eta_{-4} = \eta_{-4}^\rho$, $\eta_{-4}(-1) = 1$. If m is even, we have

$$U_2/U_2^2 = \langle 1+\sqrt{m}, -1, 5 \rangle \cong (\boldsymbol{Z}/2\boldsymbol{Z})^3.$$

Define η_8 and $\eta_{-8} \in X_2$ by $\mathrm{Ker}\,\eta_8 = \langle 1+\sqrt{m}, -1 \rangle$ and $\mathrm{Ker}\,\eta_{-8} = \langle 1+\sqrt{m}, -5 \rangle$. Then if $D/8 \equiv 1 \mod 4$, we have $\eta_8^\rho = \eta_8$, $\eta_{-8}\eta_{-8}^\rho = \varepsilon_4$ and if $D/8 \equiv -1 \mod 4$, we have $\eta_{-8}^\rho = \eta_{-8}$, $\eta_8\eta_8^\rho = \varepsilon_4$. Notation being as above, we obtain

PROPOSITION 2. (i) *Assume that* 2 *splits in* K, *i.e.* $(2) = \mathfrak{m}\mathfrak{m}^{\rho}$. *Let* $j : U_2 \to U_{\mathfrak{m}} \cong \boldsymbol{Z}_2^{\times}$ *be the projection and put* $\nu = \kappa_4 \circ j$, $\mu = \kappa_8 \circ j$. *Then we have* $X_2 = \langle \nu, \mu, \varepsilon_4 = \nu\nu^{\rho}, \varepsilon_8 = \mu\mu^{\rho} \rangle$ *and* $X_2^0 = \langle \varepsilon_4, \varepsilon_8 \rangle$.

(ii) *If* 2 *is inert in* K, *then we have* $X_2 = \langle \nu, \varepsilon_4 = \nu\nu^{\rho}, \varepsilon_8 \rangle$ *and* $X_2^0 = \langle \varepsilon_4, \varepsilon_8 \rangle$.

(iii) *Assume* 2 *is ramified in* K. *If* $D/4$ $(\neq -1)$ *is odd, we have* $X_2 = \langle \nu, \eta_{-4}, \varepsilon_8 = \nu\nu^{\rho} \rangle$ *and* $X_2^0 = \langle \eta_{-4}, \varepsilon_8 \rangle$. *If* $D/4$ *is even, we have*

$$\eta_8(-1) = 1, \quad \eta_{-8}(-1) = -1, \quad X_2 = \langle \eta_8, \eta_{-8}, \varepsilon_4 \rangle,$$

$$X_2^0 = \begin{cases} \langle \eta_8, \varepsilon_4 = \eta_{-8}\eta_{-8}^{\rho} \rangle, & \text{if } D/8 \equiv 1 \mod 4 \\ \langle \eta_{-8}, \varepsilon_4 = \eta_8\eta_8^{\rho} \rangle, & \text{if } D/8 \equiv -1 \mod 4. \end{cases}$$

3. An embedding problem associated with the Hilbert class field.

An element γ of the Galois cohomology group $H^2(H/\boldsymbol{Q}, \pm 1)$ corresponds to an equivalence class of group extensions

$$(1) \qquad 1 \to \pm 1 \to G \to \mathrm{Gal}(H/\boldsymbol{Q}) \to 1.$$

If there exists a quadratic extension k of H such that $k/\boldsymbol{Q}$ is Galois and the natural map $\mathrm{Gal}(k/\boldsymbol{Q}) \to \mathrm{Gal}(H/\boldsymbol{Q})$ corresponds to the epimorphism in (1), we say that an embedding problem $(H/\boldsymbol{Q}, \pm 1, \gamma)$ has a solution k.

Let Y be the set of $\gamma \in H^2(H/\boldsymbol{Q}, \pm 1)$ such that $(H/\boldsymbol{Q}, \pm 1, \gamma)$ has a solution. We see that Y is a $\boldsymbol{F}_2$-subspace of $H^2(H/\boldsymbol{Q}, \pm 1)$. Write $\mathfrak{g} = \mathrm{Gal}(H/K) \cong \mathrm{Cl}_K$ and denote by $\mathrm{Ext}(\mathfrak{g}, \pm 1)$ the elements of $H^2(\mathfrak{g}, \pm 1)$ corresponding to extensions of $\mathfrak{g}$ by $\{\pm 1\}$ that are abelian groups. The vector space over $\boldsymbol{F}_2$ of bilinear alternating forms on $\mathfrak{g}/\mathfrak{g}^2$ is denoted by $\mathrm{Alt}(\mathfrak{g})$. Then we have an exact sequence

$$0 \to \mathrm{Ext}(\mathfrak{g}, \pm 1) \to H^2(\mathfrak{g}, \pm 1) \to \mathrm{Alt}(\mathfrak{g}) \to 0.$$

By [**M**, §1], $\dim \mathrm{Ext}(\mathfrak{g}, \pm 1) = t - 1$, $\dim H^2(\mathfrak{g}, \pm 1) = t(t-1)/2$, since $\dim \mathfrak{g}/\mathfrak{g}^2 = t - 1$ (t is the number of distinct primes dividing the discriminant of K).

Let res: $H^2(H/\boldsymbol{Q}, \pm 1) \to H^2(\mathfrak{g}, \pm 1)$ be the restriction map and put $Y_0 = \{\gamma \in Y \mid \mathrm{res}(\gamma) \in \mathrm{Ext}(\mathfrak{g}, \pm 1)\}$. Let k be a solution of $(H/\boldsymbol{Q}, \pm 1, \gamma)$ with $\gamma \in Y_0$. Then k is a quadratic extension of H such that $k/\boldsymbol{Q}$ is Galois and k/K is abelian. We denote by

$$U_K = \prod_{p} U_p$$

the maximal compact subgroup of the idele group I_K of K and by $K_{\infty}^{\times}$ the archimedean part of I_K. Let $\chi = \chi_{k/H}$ be the character of I_H corresponding to k/H. Since k/K is abelian, there is a non-trivial character

$$\theta : U_K K^{\times} K_{\infty}^{\times} \to \pm 1$$

such that $\chi = \theta \circ N_{H/K}$ and $\theta(K^{\times} K_{\infty}^{\times}) = 1$; hence θ is determined by its restriction on U_K. Since $k/\boldsymbol{Q}$ is Galois, we have $\chi^{\rho} = \chi$ and this means that $\theta^{\rho} = \theta$. Conversely for any non-trivial character $\theta : U_K \to \pm 1$ such that

$$\theta^{\rho} = \theta \quad \text{and} \quad \theta(-1) = 1,$$

$\chi = \theta \circ N_{H/K}$ determines a solution k of $(H/\boldsymbol{Q}, \pm 1, \gamma)$ for some $\gamma \in Y_0$.

PROPOSITION 3. *If K is exceptional* (see §1), *we have* $\dim Y_0 = t$. *Otherwise we have* $\dim Y_0 = t-1$.

PROOF. Let W be the set of characters $\theta : U_K \to \pm 1$ such that $\theta^\rho = \theta$ and $\theta(-1) = 1$. Denote by W_0 the set of $\theta \in W$ of the form $\theta = \kappa \circ N_{K/\boldsymbol{Q}}$ with a quadratic Dirichlet character κ. Noting that the characters in W_0 exactly correspond to the trivial class in $H^2(H/\boldsymbol{Q}, \pm 1)$, we obtain $Y_0 \cong W/W_0$. For a rational prime l, we denote by l^* the prime discriminant defined as follows;

$$l^* = \begin{cases} (-1)^{(l-1)/2} l, & \text{if } l \text{ is odd} \\ -4, 8 \text{ or } -8, & \text{if } l = 2. \end{cases}$$

We have the unique decomposition of D into prime discriminants:

$$D = p_1^* \cdots p_r^* q_1^* \cdots q_s^* \quad (t = r+s)$$

where $p_1^*, \dots, p_r^*$ are positive discriminants or -4 and $q_1^*, \dots, q_s^*$ are negative discriminants except -4. If l^* appears in the above decomposition, we define

$$\theta_l = \begin{cases} \eta_l, & \text{if } l \text{ is odd} \\ \eta_{l^*}, & \text{if } l = 2, \end{cases}$$

where η_l are defined in Proposition 1 and 2. Composing with the projection $U_K \to U_l$, we also regard θ_l as a character of U_K. From Proposition 1 and 2 one deduces that $\theta_{p_1}, \dots, \theta_{p_r}, \theta_{q_1}\theta_{q_2}, \dots, \theta_{q_1}\theta_{q_s}$ generate W/W_0 and considering their conductors, they are linearly independent. This completes the proof. $\square$

THEOREM 1. $\dim(Y/Y_0) = (t-1)(t-2)/2$.

PROOF. If $t \le 2$, then $\mathrm{Alt}(\mathfrak{g}) = (0)$, so that $Y = Y_0$ and our statement holds. Assume $t \ge 3$. Composing the natural map

$$H^2(\mathfrak{g}, \pm 1) \to H^2(\mathfrak{g}, \pm 1)/\mathrm{Ext}(\mathfrak{g}, \pm 1) \cong \mathrm{Alt}(\mathfrak{g})$$

with the restriction map $Y \subset H^2(H/\boldsymbol{Q}, \pm 1) \to H^2(\mathfrak{g}, \pm 1)$, we obtain a linear map $g : Y \to \mathrm{Alt}(\mathfrak{g})$. Since $\mathrm{Ker}\, g = Y_0$ and $\dim \mathrm{Alt}(\mathfrak{g}) = (t-1)(t-2)/2$, it suffices to show that g is surjective. Let $D = \prod_{i=1}^t p_i^*$ be the decomposition of D into prime discriminants. We may suppose that $p_1, \dots, p_{t-1}$ are odd primes. The genus field H_0 of K is $K(\sqrt{p_1^*}, \dots, \sqrt{p_{t-1}^*})$ and $\mathrm{Gal}(H_0/K) \cong \mathfrak{g}/\mathfrak{g}^2 \cong (\boldsymbol{Z}/2\boldsymbol{Z})^{t-1}$. Let $s_1, \dots, s_{t-1}$ be elements of $\mathfrak{g}/\mathfrak{g}^2$ such that

$$s_i(\sqrt{p_i^*}) = -\sqrt{p_i^*}, \quad s_i(\sqrt{p_j^*}) = \sqrt{p_j^*} \quad (i \ne j).$$

Clearly $\{s_1, \dots, s_{t-1}\}$ is a basis of $\mathfrak{g}/\mathfrak{g}^2$. For i, j $(1 \le i < j \le t-1)$, let $f_{i,j}$ denote an element of $\mathrm{Alt}(\mathfrak{g})$ satisfying

$$f_{i,j}(s_i, s_j) = 1 \quad \text{and} \quad f_{i,j}(s_k, s_l) = 0 \quad \text{if } (i,j) \ne (k,l) \text{ and } k < l.$$

Then $\{f_{i,j} \mid 1 \le i < j \le t-1\}$ forms a basis of $\mathrm{Alt}(\mathfrak{g})$. Therefore it suffices to show that for each $f_{i,j}$, there exists a quadratic extension k/H such that k is a solution of the embedding problem $(H/\boldsymbol{Q}, \pm 1, \gamma)$ with $g(\gamma) = f_{i,j}$. For a number field M and given elements $a, b \in M^{\times}$, we denote by $(a, b) \in \mathrm{Br}_2(M) = H^2(\mathrm{Gal}(\overline{M}/M), \pm 1)$ the class of the quaternion algebra over M generated by two elements I, J with

$$I^2 = a, \quad J^2 = b, \quad JI = -IJ.$$

We claim that there exists $\gamma \in Y$ such that $g(\gamma) = f_{1,2}$. If one of (p_1^*, p_2^*), $(p_1^*, p_1^* p_2^*)$ or $(p_2^*, p_1^* p_2^*)$ is trivial in $\mathrm{Br}_2(\boldsymbol{Q})$, then there exists a Galois extension $M_0/\boldsymbol{Q}$ containing $\boldsymbol{Q}(\sqrt{p_1^*}, \sqrt{p_2^*})$ such that $\mathrm{Gal}(M_0/\boldsymbol{Q})$ is isomorphic to the dihedral group D_4 of degree 8 (cf. [**J-Y**, p. 177]). Put

$$L = K(\sqrt{p_1^*}, \sqrt{p_2^*}), \quad M = M_0 K, \quad k = M_0 H.$$

Obviously k is Galois over $\boldsymbol{Q}$ and $\mathrm{Gal}(k/\boldsymbol{Q})$ defines an element $\gamma \in Y$. We have the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(M/L) & \longrightarrow & \mathrm{Gal}(M/K) & \longrightarrow & \mathrm{Gal}(L/K) & \longrightarrow & 1 \\ & & \wr\uparrow & & \mu\uparrow & & \nu\uparrow & & \\ 1 & \longrightarrow & \mathrm{Gal}(k/H) & \longrightarrow & \mathrm{Gal}(k/K) & \longrightarrow & \mathfrak{g} & \longrightarrow & 1. \end{array}$$

Let $f = g(\gamma) \in \mathrm{Alt}(\mathfrak{g})$. Since $\mathrm{Gal}(M/K) \cong D_4$, we obtain $f(s_1, s_2) = 1$. We see that $\mathrm{Ker}\,\mu \cong \mathrm{Ker}\,\nu$ and $\mathrm{Ker}\,\nu$ in $\mathfrak{g}/\mathfrak{g}^2$ is $\langle s_3, \dots, s_{t-1} \rangle$. Hence it follows that $f(s_i, s_j) = 0$ for $3 \le j \le t-1$. This means $g(\gamma) = f_{1,2}$, as desired. If $p_1 \equiv p_2 \equiv -1 \bmod 4$, then $(p_1^*, p_1^* p_2^*)$ or $(p_2^*, p_1^* p_2^*)$ is trivial in $\mathrm{Br}_2(\boldsymbol{Q})$. Therefore we may suppose that $p_1 (= p_1^*) \equiv 1 \bmod 4$. If p_2 splits in $\boldsymbol{Q}(\sqrt{p_1})$, then (p_1, p_2^*) is trivial in $\mathrm{Br}_2(\boldsymbol{Q})$. Consequently, we may suppose that p_2 is inert in $\boldsymbol{Q}(\sqrt{p_1})$. Since $L_1 = K(\sqrt{p_1})/K$ is unramified, we see that the Hilbert symbol $((p_1, p_2^*)/\mathfrak{l})$ is trivial for each place $\mathfrak{l}$ of K. This implies that (p_1, p_2^*) is trivial in $\mathrm{Br}_2(K)$, so that there exist $a, b \in K^{\times}$ satisfying $p_2^* = a^2 - b^2 p_1$. Let $\mathfrak{p}_2$ be the prime ideal of K dividing p_2. Then $\mathfrak{p}_2$ is inert in L_1 and let $\mathfrak{P}_2$ be the prime ideal of L_1 dividing $\mathfrak{p}_2$. Put $\alpha = a + b\sqrt{p_1} \in L_1$. Since $N_{L_1/K}(\alpha^{-1}\mathfrak{P}_2) = \mathfrak{o}_K$, there is an ideal $\mathfrak{A}$ in L_1 such that $\alpha^{-1}\mathfrak{P}_2 = \mathfrak{A}/\mathfrak{A}^{\tau}$ where τ is the generator of $\mathrm{Gal}(L_1/K)$. Choose an odd prime ideal $\mathfrak{L}$ of degree 1 in L_1 which belongs to the ideal class of $\mathfrak{A}$. Then $\mathfrak{P}_2\mathfrak{L}^{\tau}/\mathfrak{L}$ is a principal ideal (β) and $N_{L_1/K}(\beta) = N_{L_1/K}(\alpha) = p_2^*$. Therefore $M = L_1(\sqrt{\beta}, \sqrt{p_2^*})$ is a D_4-extension of K containing $K(\sqrt{p_1}, \sqrt{p_2^*})$. Moreover, it is now easy to check that $\mathrm{Gal}(MH/K)$ determines an element $\delta \in H^2(\mathfrak{g}, \pm 1)$ which corresponds to $f_{1,2}$. We note that

$$(\beta\beta^{\rho}) = N_{L_1/\boldsymbol{Q}(\sqrt{p_1})}(\mathfrak{P}_2\mathfrak{L}^{\tau}/\mathfrak{L}) = (p_2 l)/(\mathfrak{L}\mathfrak{L}^{\rho})^2,$$

where l is the rational prime contained in $\mathfrak{L}$. Since the class number of $\boldsymbol{Q}(\sqrt{p_1})$ is odd, $\mathfrak{L}\mathfrak{L}^{\rho}$ is principal, so that $\beta\beta^{\rho} = p_2 l a^2$ with $a \in \boldsymbol{Q}(\sqrt{p_1})$. Admitting the following lemma, our proof will be completed immediately.

Lemma 1. *There exists an abelian extension $H(\sqrt{c})$ $(c \in H)$ over K such that $cc^{\rho}\beta\beta^{\rho} \in H^{\times 2}$.*

Put $k = H(\sqrt{\beta c})$. Notice that k is Galois over $\boldsymbol{Q}$, since $H(\sqrt{\beta}) = MH$ is Galois over K. Since $\mathrm{Gal}(H(\sqrt{c})/K)$ corresponds to an element $\delta_0 \in \mathrm{Ext}(\mathfrak{g}, \pm 1)$, we see that $\mathrm{Gal}(k/\boldsymbol{Q})$ corresponds to $\gamma \in H^2(H/\boldsymbol{Q}, \pm 1)$ such that $\mathrm{res}(\gamma) = \delta + \delta_0$; thus $g(\gamma) = f_{1,2}$, as claimed. Applying the same arguements for any $f_{i,j}$, our proof of Theorem 1 is completed. $\square$

Proof of Lemma 1. For a non-trivial character $\chi : U_K \to \pm 1$ satisfying $\chi(-1) = 1$, there exists the unique quadratic extension $H(\sqrt{c})$ over H such that $\chi \circ N_{H/K}$ is the character of I_H corresponding to $H(\sqrt{c})/H$ and $H(\sqrt{c})/K$ is abelian. We need to choose $c \in H^\times$ such that $cc^\rho \in (-1)^{(p_2-1)/2} l H^{\times 2}$. Thus it suffices to show that χ can be chosen such that $\chi\chi^\rho = \kappa \circ N_{K/\boldsymbol{Q}}$, where κ is the quadratic Dirichlet character corresponding to a quadratic field $S = \boldsymbol{Q}(\sqrt{(-1)^{(p_2-1)/2} ln})$ for some $n \in \boldsymbol{Z}$ with $\sqrt{n} \in H$. We consider cases.

1) If $p_2 \equiv l \equiv -1 \mod 4$, let $\mathfrak{l}$ be a prime of K dividing l and put $\chi = \lambda_\mathfrak{l} \eta_{p_2}$, where $\lambda_\mathfrak{l}, \eta_{p_2}$ are those defined in Proposition 1. We have $\chi\chi^\rho = \kappa_l \circ N_{K/\boldsymbol{Q}}$ and $S = \boldsymbol{Q}(\sqrt{-l})$.

2) Assume $p_2 \equiv -1 \mod 4$ and $l \equiv 1 \mod 4$. If D is odd, put $\chi = \lambda_\mathfrak{l} \eta_{p_2} \nu$ with ν defined in Proposition 2. Then $\chi\chi^\rho = \kappa_l \kappa_4 \circ N_{K/\boldsymbol{Q}}$ and $S = \boldsymbol{Q}(\sqrt{-l})$. If $D = 4m$ with an odd integer m, put $\chi = \lambda_\mathfrak{l}$. Then $S = \boldsymbol{Q}(\sqrt{l})$. Since $\sqrt{-1} \in H$, this satisfies our requirement. If $D = 8m$ with $m \equiv 1 \mod 4$, put $\chi = \lambda_\mathfrak{l} \eta_{p_2} \eta_{-8}$ and if $D = 8m$ with $m \equiv -1 \mod 4$, put $\chi = \lambda_\mathfrak{l} \eta_8$. Then we have $\chi\chi^\rho = (\kappa_l \kappa_4) \circ N_{K/\boldsymbol{Q}}$.

3) Assume $p_2 \equiv 1 \mod 4$. We claim that it is always possible to choose β such that $l \equiv 1 \mod 4$. We put

$$K_0 = K(\sqrt{-1}), \quad L_0 = L_1(\sqrt{-1}) = K(\sqrt{p_1}, \sqrt{-1})$$

and let σ and τ be generators of $\mathrm{Gal}(L_0/L_1)$ and $\mathrm{Gal}(L_0/K_0)$, respectively. Decompose p_2 as $\pi\pi^\sigma$ in $\boldsymbol{Q}(\sqrt{-1})$. There exists a prime ideal $\mathfrak{P}_0$ in L_0 such that $N_{L_0/K_0}(\mathfrak{P}_0) = (\pi)$. Since (p_1, π) is trivial in $\mathrm{Br}_2(K_0)$, there is an $\alpha_1 \in L_0$ such that $N_{L_0/K_0}(\alpha_1) = \pi$. This implies that there exists a prime ideal $\mathfrak{L}_0$ in L_0 of degree 1 such that $\mathfrak{P}_0 \mathfrak{L}_0^\tau / \mathfrak{L}_0$ is principal. Putting

$$\mathfrak{P}_2 = N_{L_0/L_1}(\mathfrak{P}_0), \quad \mathfrak{L} = N_{L_0/L_1}(\mathfrak{L}_0),$$

we see that $\mathfrak{P}_2 \mathfrak{L}^\tau / \mathfrak{L}$ is a principal ideal (β) with $N_{L_1/K}(\beta) = N_{L_0/K}(\alpha_1) = p_2$. By the choice of $\mathfrak{L}_0$, the rational prime l in $\mathfrak{L}$ satisfies $l \equiv 1 \mod 4$, as claimed. Therefore $\chi = \lambda_\mathfrak{l}$ satisfies our requirement.

4. Elliptic $\boldsymbol{Q}$-curves with complex multiplication.

Let L be a Galois extension over $\boldsymbol{Q}$ containing H. An elliptic curve E over L with complex multiplication by K is called a $\boldsymbol{Q}$-curve if E^σ and E are isogenous over L for all $\sigma \in \mathrm{Gal}(L/\boldsymbol{Q})$. Let ψ_E be the Hecke character of the idele group I_L of L associated with E. Then E is a $\boldsymbol{Q}$-curve if and only if $\psi_E = \psi_E^\sigma$ for all $\sigma \in \mathrm{Gal}(L/\boldsymbol{Q})$ (cf. [**G**, §11]). For a $\boldsymbol{Q}$-curve E over L, choose isogenies $\varphi_\sigma : E^\sigma \to E$ for $\sigma \in \mathrm{Gal}(L/\boldsymbol{Q})$. Then

$$c(\sigma, \tau) = \varphi_\sigma \varphi_\tau^\sigma (\varphi_{\sigma\tau})^{-1} \in K^\times$$

defines a two-cocycle and the cohomology class of $\{c(\sigma, \tau)\}$ in $H^2(L/\boldsymbol{Q}, K^\times)$ depends only on the curve E, and not on the isogenies φ_σ chosen. We will denote by $c(E)$ this cohomology class. Let us denote by Γ_L the subset of $H^2(L/\boldsymbol{Q}, K^\times)$ consisting of elements of the form $c(E)$ for all $\boldsymbol{Q}$-curves E over L. Furthermore, we denote by Y_L the subspace of $H^2(L/\boldsymbol{Q}, \pm 1)$ consisting of all γ such that the embedding problems $(L/\boldsymbol{Q}, \pm 1, \gamma)$ are solvable.

Proposition 4. *If Γ_L is not empty, then Y_L operates on Γ_L simply transitively in an obvious manner. For $\boldsymbol{Q}$-curves E and E', we have $c(E) = c(E')$ if and only if $\psi_E = \psi_{E'} \cdot \kappa \circ N_{L/\boldsymbol{Q}}$, where κ is a quadratic Dirichlet character.*

Proof. For $\boldsymbol{Q}$-curves E and E' over L, there exists an isogeny $\lambda : E \to E'$ defined over a finite extension of L. For each $\sigma \in \mathrm{Gal}(\overline{L}/L)$, we have $\lambda^\sigma = \lambda v(\sigma)$ with $v(\sigma) \in K^\times$. Since $\lambda^{\sigma^n} = \lambda$ for sufficiently large n, we have $v(\sigma)^n = 1$, so that $v(\sigma) = \pm 1$. This means that if E and E' are not isogenous over L, there exists the unique quadratic extension k over L such that λ is defined over k. We also see that E and E' are isogenous over k^σ for all $\sigma \in \mathrm{Gal}(L/\boldsymbol{Q})$, because E and E' are $\boldsymbol{Q}$-curves; hence k is Galois over $\boldsymbol{Q}$. Therefore the Galois group $\mathrm{Gal}(k/\boldsymbol{Q})$ determines a cohomology class $\gamma = \{\gamma(\sigma, \tau)\} \in H^2(L/\boldsymbol{Q}, \pm 1)$; thus $\gamma \in Y_L$. For each $\sigma \in \mathrm{Gal}(L/\boldsymbol{Q})$, choose an extension $\tilde{\sigma} \in \mathrm{Gal}(k/\boldsymbol{Q})$ of σ. Then $\gamma(\sigma, \tau) = \lambda^{\tilde{\sigma}\tilde{\tau}}/\lambda^{\widetilde{\sigma\tau}}$ for $\sigma, \tau \in \mathrm{Gal}(L/\boldsymbol{Q})$. One can find isogenies

$$\varphi_\sigma : E^\sigma \to E, \quad \varphi'_\sigma : E'^\sigma \to E'$$

such that $\lambda \varphi_\sigma = \varphi'_\sigma \lambda^{\tilde{\sigma}}$. Then by a short computation, we obtain

$$c(E) = c(E')\gamma.$$

Now we claim that the natural map

$$H^2(L/\boldsymbol{Q}, \pm 1) \to H^2(L/\boldsymbol{Q}, K^\times)$$

is injective. From the exact sequence

$$1 \to \pm 1 \to K^\times \to K^{\times 2} \to 1$$

it suffices to show that $H^1(L/\boldsymbol{Q}, K^{\times 2}) = (0)$. This follows easily from the restriction-inflation sequence

$$0 \to H^1(K/\boldsymbol{Q}, K^{\times 2}) \to H^1(L/\boldsymbol{Q}, K^{\times 2}) \to H^1(L/K, K^{\times 2}),$$

since $H^1(K/\boldsymbol{Q}, K^{\times 2}) = (0)$ and $H^1(L/K, K^{\times 2}) = \mathrm{Hom}(\mathrm{Gal}(L/K), K^{\times 2}) = (0)$. If $c(E) = c(E')$ and E and E' are not isogenous over L, let k be the quadratic extension of L stated as above. Then the group extension

$$1 \to \pm 1 \to \mathrm{Gal}(k/\boldsymbol{Q}) \to \mathrm{Gal}(L/\boldsymbol{Q}) \to 1$$

splits, which implies that the character associated with k/L is of the form $\kappa \circ N_{L/\boldsymbol{Q}}$ with a quadratic Dirichlet character κ. Since E' is isogenous to the twist of E with respect to k/L, the last statement is clear. □

In [**S**] a class of elliptic curves (more generally abelian varieties) with complex multiplication whose Hecke characters satisfy a certain condition are studied. We recall briefly what we need here.

For an integer $f \geq 1$, let $H^{(f)}$ denote the ring class field of K of conductor f. Let

$$U_{K,f} = \{u \in U_K \mid u(\boldsymbol{Z} + f\mathfrak{o}_K) = \boldsymbol{Z} + f\mathfrak{o}_K\}.$$

Then $P = U_{K,f} K^\times K_\infty^\times$ is the subgroup of I_K corresponding to $H^{(f)}$ by class field theory. Let E be an elliptic curve over $H^{(f)}$ with $\mathrm{End}\, E = \boldsymbol{Z} + f\mathfrak{o}_K$. Let us consider the following condition on the Hecke character ψ_E of E (see [**S**, Theorem 4]).

(Sh) *There exists a Hecke character* $\phi : U_{K,f}K^{\times}K_{\infty}^{\times} \to \boldsymbol{C}^{\times}$ *such that* $\psi_E = \phi \circ N_{H^{(f)}/K}$.

Here ϕ must satisfy the following conditions:

$$\phi(K^{\times}) = 1, \quad \phi(y) = y^{-1} \quad \text{for every } y \in K_{\infty}^{\times}, \tag{3}$$

$$\phi(U_{K,f}) = \pm 1 \quad \text{and} \quad \phi(-1) = -1 \quad \text{for } -1 \in U_{K,f}. \tag{4}$$

If ψ_E satisfies (Sh), then clearly $\psi_E = \psi_E^{\sigma}$ for all $\sigma \in \mathrm{Gal}(H^{(f)}/K)$. Conversely from a character $\phi : U_{K,f} \to \pm 1$ with $\phi(-1) = -1$, extending it on $P = U_{K,f}K^{\times}K_{\infty}^{\times}$ by (3), we obtain $\psi = \phi \circ N_{H^{(f)}/K}$, which is a Hecke character of an elliptic curve E over $H^{(f)}$. Furthermore in this case E is a $\boldsymbol{Q}$-curve if and only if $\phi^{\rho} = \phi$ on $U_{K,f}$ (cf. [**S**, Proposition 9]).

Assume first that K is not exceptional. If D has a prime divisor q with $q \equiv -1 \bmod 4$, we put $\phi = \eta_q : U_K \to \pm 1$ where η_q is the local character defined in Proposition 1. Here we view η_q as a character of U_K by composing with the projection $U_K \to U_q$. Otherwise since D is of the form $8m$ with $m \equiv -1 \bmod 4$, we put $\phi = \eta_{-8}$, where η_{-8} is defined in Proposition 2. Then ϕ satisfies

$$\phi(-1) = -1, \quad \phi^{\rho} = \phi. \tag{5}$$

Therefore there exists a $\boldsymbol{Q}$-curve over H.

Next assume that K is exceptional. Then there is no character $\phi : U_K \to \pm 1$ satisfying (5). This follows from the fact that if a local character $\theta : U_p \to \pm 1$ satisfies $\theta^{\rho} = \theta$, we have $\theta(-1) = 1$ by Proposition 1 and 2.

The following assertion is stated in [**G**, §11] without proof.

Proposition 5. *If K is exceptional, there are no $\boldsymbol{Q}$-curves over H.*

Proof. Choose a rational prime q such that q splits in K and $q \equiv -1 \bmod 4$. Let $\lambda_{\mathfrak{q}} : U_{\mathfrak{q}} \to \pm 1$ be as in Proposition 1 where $\mathfrak{q}|q$. We put $\lambda = \lambda_{\mathfrak{q}} \circ pr$ where $pr : U_K \to U_{\mathfrak{q}}$ is the projection. Then λ determines an elliptic curve E_1 over H with $\psi_{E_1} = \lambda \circ N_{H/K}$. Clearly E_1 is not a $\boldsymbol{Q}$-curve over H, since $\psi_{E_1}^{\rho}/\psi_{E_1} = \lambda_{\mathfrak{q}}\lambda_{\mathfrak{q}}^{\rho} \circ N_{H/K} = \kappa_q \circ N_{H/\boldsymbol{Q}}$. (It is a $\boldsymbol{Q}$-curve over $H(\sqrt{-q})$.) Now assume that a $\boldsymbol{Q}$-curve E over H exists. Put $\chi_1 = \psi_{E_1}/\psi_E$. Then χ_1 is a quadratic character of I_H and it determines a quadratic extension k_1 of H which is Galois over K. Since $g : Y \to \mathrm{Alt}(\mathfrak{g})$ is surjective as shown in the proof of Theorem 1, there exists a quadratic extension k of H which is Galois over $\boldsymbol{Q}$ such that $\mathrm{Gal}(k/K)$ and $\mathrm{Gal}(k_1/K)$ correspond to the same element in $\mathrm{Alt}(\mathfrak{g})$. This means that denoting by χ the character associated with k/H, $\chi\chi_1$ corresponds to a quadratic extension of H which is abelian over K, i.e. $\chi\chi_1 = \theta \circ N_{H/K}$ with a character $\theta : U_K \to \pm 1$. Put $\psi = \psi_E \cdot \chi$. We easily find that $\psi = (\lambda\theta) \circ N_{H/K}$ and $\psi^{\rho} = \psi$, since $\psi_E^{\rho} = \psi_E$ and $\chi^{\rho} = \chi$; this implies that $\phi = \lambda\theta : U_K \to \pm 1$ satisfies (5). As remarked above, this is impossible if K is exceptional. $\square$

Applying Theorem 1, we obtain the following result concerning a classification of $\boldsymbol{Q}$-curves.

Theorem 2. *If K is not exceptional, the cohomology classes $c(E)$ classify isogeny classes of $\boldsymbol{Q}$-curves over H into $2^{t(t-1)/2}$ classes. Among them there are 2^{t-1} classes* *whose Hecke characters satisfy* (Sh). *If K is exceptional, take $H^{(2)}$, the ring class field of K of conductor* 2, *instead of H. Then exactly the same statements hold for isogeny classes of $\boldsymbol{Q}$-curves over $H^{(2)}$.*

Proof. Let the notation be as in Proposition 3. The first statement is clear by Theorem 1 and Proposition 3. Let E_0 be a $\boldsymbol{Q}$-curve over H such that ψ_{E_0} satisfies (Sh). Then $c(E_0)\gamma$ $(\gamma \in Y_0)$ correspond to those $\boldsymbol{Q}$-curves whose Hecke characters satisfy (Sh).

Next assume that K is exceptional. Let $\mathfrak{m}$ denote the prime ideal of the local completion of K at 2 and put

$$P^{(2)} = \prod_{p \neq 2} U_p \cdot (1 + \mathfrak{m}^2) K^{\times} \cdot K_{\infty}^{\times}.$$

Then $P^{(2)}$ is the subgroup of I_K corresponding to $H^{(2)}$ by class field theory. Let $\theta : 1 + \mathfrak{m}^2 \to \pm 1$ denote the character such that $\operatorname{Ker} \theta = 1 + \mathfrak{m}^3$ and put $\phi = \theta \circ j$, where $j : \prod_{p \neq 2} U_p \cdot (1 + \mathfrak{m}^2) \to 1 + \mathfrak{m}^2$ is the projection. Then $\phi \circ N_{H^{(2)}/K}$ is a Hecke character of a $\boldsymbol{Q}$-curve over $H^{(2)}$, since $\phi^\rho = \phi$. Therefore a $\boldsymbol{Q}$-curve over $H^{(2)}$ exists. Let $\mathfrak{g}' = \operatorname{Gal}(H^{(2)}/K)$ and put $Y_0' = \{\gamma \in Y_{H^{(2)}} \mid \operatorname{res}(\gamma) \in \operatorname{Ext}(\mathfrak{g}', \pm 1)\}$. It suffices to show that $\dim Y_0' = t - 1$ and $\dim Y_{H^{(2)}} = t(t-1)/2$. If a non-trivial local character $\lambda : 1 + \mathfrak{m}^2 \to \pm 1$ satisfies $\lambda(-1) = 1$ and $\lambda^\rho = \lambda$, we see easily that $\lambda = \kappa_8 \circ N_{K/\boldsymbol{Q}}$. As in the proof of Proposition 3,

$$\theta_{p_1}, \dots, \theta_{p_{t-1}} \quad (D/4 = -p_1 \cdots p_{t-1})$$

form a basis of W/W_0; hence $\dim Y_0' = t - 1$. Note that $v = (1 + \sqrt{D/4})^2/2$ is prime to 2 and $v \notin 1 + \mathfrak{m}^2$. Then we see that the class containing the ideal $\mathfrak{n}$ with $\mathfrak{n}^2 = (2)$ has order 4 in $I_K/P^{(2)}$. This shows that $\mathfrak{g}'/\mathfrak{g}'^2 \cong \mathfrak{g}/\mathfrak{g}^2$; hence we obtain $\dim(Y_{H^{(2)}}/Y_0') = \dim \operatorname{Alt}(\mathfrak{g}') = (t-1)(t-2)/2$ by Theorem 1. $\square$

5. Restriction of scalars of $\boldsymbol{Q}$-curves.

In this section we suppose that K is non-exceptional. Let E be a $\boldsymbol{Q}$-curve over H. Let us denote by $B = R_{H/K}(E)$ the abelian variety obtained from E by restriction of scalars from H to K. It is an abelian variety defined over K of dimension $h_K = [H : K]$. Since E is defined over $\boldsymbol{Q}(j_E)$ (cf. [**G**, Theorem 10.1.3]), we have

$$B \cong R_{\boldsymbol{Q}(j_E)/\boldsymbol{Q}}(E) \otimes K,$$

so that B is defined over $\boldsymbol{Q}$. Concerning the structure of the endomorphism algebra $R_0 = \operatorname{End}_{\boldsymbol{Q}}(B) \otimes \boldsymbol{Q}$ we obtain

Theorem 3. *Let $R_0 = \operatorname{End}_{\boldsymbol{Q}}(B) \otimes \boldsymbol{Q}$ be as above and h_K the class number of K. The center Z_0 of R_0 is a field of degree h_0 over $\boldsymbol{Q}$ and $R_0 \cong M_{2^m}(Z_0)$ or $R_0 \cong M_{2^{m-1}}(D_0)$, where D_0 is a division quaternion algebra over Z_0 and $h_K = 2^{2m} h_0$. R_0 is commutative if and only if ψ_E satisfies* (Sh).

Proof. We recall some facts on the structure of $R = \operatorname{End}_K(B) \otimes \boldsymbol{Q}$ (cf. [**G**, §15] and [**N**]). For $\sigma \in \mathfrak{g} = \operatorname{Gal}(H/K)$, one can choose a prime ideal $\mathfrak{p}$ of K, of degree 1, prime to the conductor of ψ_E such that $\sigma = \sigma_{\mathfrak{p}}^{-1}$, where $\sigma_{\mathfrak{p}}$ is the Frobenius automorphism of H/K at $\mathfrak{p}$. Let $\mathfrak{P}$ be a prime of H lying over $\mathfrak{p}$ and p the rational prime in $\mathfrak{p}$. Then there exists an isogeny (a $\mathfrak{p}$-multiplication in the sense of [**S-T**, §7]) $u(\mathfrak{p}) : E^{\sigma} \to E$ such that $u(\mathfrak{p}) \bmod \mathfrak{P}$ is the p-th power Frobenius map (see [**Si**, II Proposition 5.3]). Let $t(\mathfrak{p})$ be the corresponding K-endomorphism of B. If σ is of order n, we have

$$\psi_E(\mathfrak{P}) = t(\mathfrak{p})^n \in K^{\times}, \quad \mathfrak{p}^n = (\psi_E(\mathfrak{P})). \tag{6}$$

Take $\varphi_{\sigma} = u(\mathfrak{p})$ and $t_{\sigma} = t(\mathfrak{p})$ for each $\sigma \in \mathfrak{g}$. Then R is the twisted group algebra $K^{c(E)}[\mathfrak{g}] = \sum_{\sigma \in \mathfrak{g}} K t_{\sigma}$ over K subject to the relation

$$t_{\sigma} t_{\tau} = c(\sigma, \tau) t_{\sigma\tau} \quad \text{for } \sigma, \tau \in \mathfrak{g}$$

where $c(E) = \{c(\sigma, \tau)\}$ is the two-cocycle attached to $\{\varphi_{\sigma}\}$ (see Section 4).

The complex conjugation ρ operates on R and $R_0 = \{\alpha \in R \mid \rho(\alpha) = \alpha\}$. Changing E by some E^{σ} if necessary, we may assume that $\rho(E) = E$. By transport of structure, $\rho(u(\mathfrak{p})) : E^{\sigma\rho} = E^{\rho\sigma^{-1}} = E^{\sigma^{-1}} \to E$ is a $\mathfrak{p}^{\rho}$-multiplication whose reduction $\bmod \mathfrak{P}^{\rho}$ is the p-th power Frobenius map. This implies that $\rho(t(\mathfrak{p})) = t(\mathfrak{p}^{\rho})$. Moreover, since $\mathfrak{p}\mathfrak{p}^{\rho} = (p)$ we have

$$t(\mathfrak{p}) t(\mathfrak{p}^{\rho}) = \pm p, \quad R_0 \cap K(t(\mathfrak{p})) = \boldsymbol{Q}(s(\mathfrak{p})), \tag{7}$$

where $s(\mathfrak{p}) = t(\mathfrak{p}) + t(\mathfrak{p}^{\rho})$.

Now we have $t_{\sigma} t_{\tau} = f(\sigma, \tau) t_{\tau} t_{\sigma}$, where $f(\sigma, \tau) = c(\sigma, \tau) c(\tau, \sigma)^{-1}$ is the alternating form on $\mathfrak{g}$ associated with $c(E)$. Let $\mathfrak{g}_0 (\supset \mathfrak{g}^2)$ be the kernel of f. If $\mathfrak{g} \neq \mathfrak{g}_0$, then $\mathfrak{g}/\mathfrak{g}_0$ is an orthogonal sum of hyperbolic planes $T_1, \dots, T_m$; each T_i is two dimensional and f induces on T_i a non-degenerate alternating form. Choose $x_i, y_i \in \mathfrak{g}$ such that they induce a basis of T_i, and define $\mathfrak{h}_i = \langle x_i, y_i, \mathfrak{g}_0 \rangle$. Then $Z = \sum_{\sigma \in \mathfrak{g}_0} K t_{\sigma}$ is the center of R and the subalgebra $D_i = \sum_{\sigma \in \mathfrak{h}_i} K t_{\sigma}$ of R is a quaternion algebra over Z. We have

$$R = D_1 \otimes \cdots \otimes_Z D_m$$

and $h_K = 2^{2m} h_0$ with $[Z : K] = h_0$ (see [**N**, Theorem 3]). Furthermore it easily follows: $Z_0 = \{\alpha \in Z \mid \rho(\alpha) = \alpha\}$ is the center of R_0, $D_i^0 = \{\alpha \in D_i \mid \rho(\alpha) = \alpha\}$ are quaternion algebras over Z_0 and $R_0 = D_1^0 \otimes \cdots \otimes_{Z_0} D_m^0$. Observe that $[Z_0 : \boldsymbol{Q}] = [Z : K] = h_0$ and R is commutative if and only if R_0 is commutative. Then our assertion can be proved exactly in the same manner as Theorem 3 in [**N**]. □

Proposition 6. *Let E, E' be $\boldsymbol{Q}$-curves over H and put:*

$$B = R_{H/K}(E), \quad B' = R_{H/K}(E'), \quad R_0 = \mathrm{End}_{\boldsymbol{Q}}(B) \otimes \boldsymbol{Q}, \quad R_0' = \mathrm{End}_{\boldsymbol{Q}}(B') \otimes \boldsymbol{Q}.$$

Then if $c(E) = c(E')$, we have $R_0 \cong R_0'$. Conversely if R_0 is commutative and $R_0 \cong R_0'$, we have $c(E) = c(E')$.

Proof. If $c(E) = c(E')$, then $\psi_E = \psi_{E'} \cdot \kappa \circ N_{H/\boldsymbol{Q}}$ with a quadratic Dirichlet character κ by Proposition 4. Let k_0 be the corresponding quadratic field to κ. We may assume that k_0 is different from K and $j_E = j_{E'}$. Then E and E' are isomorphic over $k_0(j_E)$ (see [**G**, Theorem 10.2.1]), so that B and B' are isomorphic over k_0. Since k_0-endomorphism algebra of B is R_0, we obtain $R_0 \cong R_0'$.

Now assume that R_0 is commutative and $R_0 \cong R_0'$. By Theorem 3 ψ_E and $\psi_{E'}$ satisfy (Sh), i.e.

$$\psi_E = \phi \circ N_{H/K}, \quad \psi_{E'} = \phi' \circ N_{H/K}$$

with characters ϕ, ϕ' of I_K. We see that B is of CM-type over K, ϕ is the Hecke character of B over K and

$$\mathrm{End}_K(B) \otimes \boldsymbol{Q} = R_0 K \cong K(\{\phi(\mathfrak{a}) \mid \mathfrak{a} \in \mathrm{Cl}_K\}).$$

Here Hecke characters are also viewed as functions of ideals. Since R_0K and $R_0'K$ are K-isomorphic, the maximal $(2, \dots, 2)$ subextension L over K contained in R_0K coincide with that in $R_0'K$. We have $L = K(\{\phi(\mathfrak{a}) \mid \mathfrak{a} \in \mathrm{Cl}_K[2]\})$, where $\mathrm{Cl}_K[2] = \{\mathfrak{a} \in \mathrm{Cl}_K \mid \mathfrak{a}^2 = 1\}$. Observe that the map $\mathrm{Cl}_K[2] \ni \mathfrak{a} \to \phi(\mathfrak{a})^2 \in K^\times/K^{\times 2}$ is injective, since $\mathfrak{a}^2 = (\phi(\mathfrak{a})^2)$ by (6). In particular we have $\sqrt{-1} \notin L$. We may assume that E and E' are not isogenous over H but isogenous over a quadratic extension k of H. Put $\xi = \phi/\phi'$. Then ξ is a character of the idele class group C_K of K and $\xi \circ N_{H/K}$ is the character associated with k/H. Therefore k/H is abelian. Let N and N' be the norm subgroups in C_K corresponding to H and k, respectively.

Claim. $C_K/N' (\cong \mathrm{Gal}(k/K)) \cong \varDelta \times N/N'$ with a subgroup $\varDelta$ of C_K/N' such that $\varDelta \cong \mathrm{Cl}_K$.

We have only to show the corresponding assertion for the 2-Sylow subgroup of C_K/N'. Let $\mathfrak{a}$ be any ideal in K of even order n in Cl_K, which is prime to the conductor of ϕ. We have $\phi(\mathfrak{a}^n) = \phi'(\mathfrak{a}^n)\xi(\mathfrak{a}^n) \in K$. If $\xi(\mathfrak{a}^n) = -1$, then by assumption we have $\sqrt{-1} \in R_0K$, which is a contradiction. Therefore $\xi(\mathfrak{a}^n) = 1$. Let $\mathfrak{a}_1, \dots, \mathfrak{a}_r$ be a set of ideals of K such that they form a set of independent generators for the 2-Sylow subgroup of Cl_K and denote by $\varDelta'$ the subgroup of C_K/N' generated by $\mathfrak{a}_1, \dots, \mathfrak{a}_r$. Since ξ is non-trivial on N/N', we have $\varDelta' \cap N/N' = 1$. Thus our claim is proved.

Let k_0 be the quadratic extension of K which corresponds to $\varDelta$ by class field theory and denote by ξ_0 the character of I_K associated to k_0/K. Then we may assume that $\phi = \phi'\xi_0$. Take any ideal $\mathfrak{a}$ of K prime to the conductor of ϕ and ϕ'. Then by (7) we have $R_0 \cap K(\phi(\mathfrak{a})) = \boldsymbol{Q}(s)$ with $s = \phi(\mathfrak{a}) + \phi(\mathfrak{a}^\rho)$: $\boldsymbol{Q}(s)$ is totally real (resp. of CM-type) if and only if $\phi(\mathfrak{a}\mathfrak{a}^\rho) > 0$ (resp. $\phi(\mathfrak{a}\mathfrak{a}^\rho) < 0$). Therefore $R_0 \cong R_0'$ implies that $\xi_0(\mathfrak{a}\mathfrak{a}^\rho) = 1$, hence $\xi_0 = \xi_0^\rho$. This shows that $k_0 = k_0^\rho$; thus $k_0/\boldsymbol{Q}$ is Galois. Since $k_0 \supset K$, we see that $k_0/\boldsymbol{Q}$ is of type $(2, 2)$. Hence we have $c(E) = c(E')$. $\square$

6. Examples.

First we consider non-exceptional case. For the sake of simplicity, we assume that K is an imaginary quadratic field of discriminant D such that $\mathrm{Cl}_K \cong \boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}/2\boldsymbol{Z}$; hence in this case $t = 3$ and the class number $h_K = 4$.

Let ϕ_0 be a character of U_K which satisfies the condition (5). Then as explained in Section 4, we obtain a Hecke character $\psi_0 = \phi_0 \circ N_{H/K}$ of I_H. Take any quadratic extension k of H such that $k/\boldsymbol{Q}$ is Galois and denote by χ the character of I_H associated with it. We put $\psi = \psi_0 \cdot \chi$. Now choose a prime ideal $\mathfrak{p}$ of K such that $\mathfrak{p}$ is of order 2 in Cl_K and prime to the conductor of ϕ_0 and χ. Let L be the decomposition field of $\mathfrak{p}$ in H and F be the subfield of L fixed by ρ. Then k/F is a Galois extension of degree 8. Let E_0 and E_1 be $\boldsymbol{Q}$-curves such that $\psi_{E_0} = \psi_0$ and $\psi_{E_1} = \psi_0 \cdot \chi$ and put

$$B_0 = R_{H/L}(E_0), \quad B_1 = R_{H/L}(E_1).$$

Then they are abelian varieties of dimension 2 defined over F. Set:

$$S = \mathrm{End}_F(B_0) \otimes \boldsymbol{Q}, \quad T = \mathrm{End}_F(B_1) \otimes \boldsymbol{Q}.$$

Proposition 7. *Notation being as above, put* $s = \phi_0(\mathfrak{p}) + \phi_0(\mathfrak{p}^\rho)$. *Then* S *is a quadratic field* $\boldsymbol{Q}(s)$. *Write* $S = \boldsymbol{Q}(\sqrt{n})$ *and set*:

$$S' = \boldsymbol{Q}(\sqrt{D/n}), \quad \bar{S} = \boldsymbol{Q}(\sqrt{-n}), \quad \overline{S'} = \boldsymbol{Q}(\sqrt{-D/n}).$$

(1) *Assume that* k/L *is an extension of type* $(2,2)$. *If* k/F *is abelian, we have* $T = S$ *and otherwise we have* $T = S'$.

(2) *Assume that* k/L *is cyclic of order* 4. *If* k/F *is abelian, we have* $T = \bar{S}$ *and otherwise we have* $T = \overline{S'}$.

Proof. Since k/L is abelian, we can write $\chi = \chi' \circ N_{H/L}$ for a character χ' of I_L. Then $\psi = \phi \circ N_{H/L}$ with $\phi = (\phi_0 \circ N_{L/K}) \cdot \chi'$, so that ϕ is a Hecke character of B_1 over L. By Artin map we may regard χ' as a character of $\mathrm{Gal}(k/L)$. Let $\mathfrak{P}$ be a prime ideal of L lying above $\mathfrak{p}$ and we denote by σ the Frobenius automorphism in k/L associated with $\mathfrak{P}$. We have $\chi'(\mathfrak{P}) = \chi'(\sigma)$,

$$\phi(\mathfrak{P})^2 = \phi_0(\mathfrak{p})^2 \chi'(\mathfrak{P})^2 \quad \text{and} \quad \phi(\mathfrak{P}\mathfrak{P}^\rho) = \phi_0(\mathfrak{p}\mathfrak{p}^\rho)\chi'(\mathfrak{P}\mathfrak{P}^\rho).$$

Let τ be the non-trivial automorphism of k over H. Note that $T = \boldsymbol{Q}(\phi(\mathfrak{P}) + \phi(\mathfrak{P}^\rho))$ and that T is totally real if and only if $\phi(\mathfrak{P}\mathfrak{P}^\rho) > 0$.

In the case (1) we have $\chi'(\mathfrak{P})^2 = 1$, hence $KT = KS$. If k/F is abelian, $\chi'(\mathfrak{P}) = \chi'(\mathfrak{P}^\rho) = \chi'(\rho\sigma\rho)$. Thus $T = S$. If k/F is non-abelian, we have $\rho\sigma\rho = \sigma\tau$. Since $\chi'(\tau) = -1$, we obtain $\chi'(\mathfrak{P}\mathfrak{P}^\rho) = -1$, which shows $T = S'$.

In the case (2) we have $\chi'(\mathfrak{P})^2 = -1$, hence $KT = K\bar{S}$. If k/F is abelian, $\chi'(\mathfrak{P}\mathfrak{P}^\rho) = \chi'(\mathfrak{P})^2 = -1$ and hence $T = \bar{S}$. If k/F is non-abelian, we have $\chi'(\mathfrak{P}\mathfrak{P}^\rho) = \chi'(\sigma^2\tau) = 1$, which shows $T = \overline{S'}$. □

Now let us determine the endomorphism algebras $R_0 = \mathrm{End}_{\boldsymbol{Q}}(R_{H/K}(E)) \otimes \boldsymbol{Q}$ for some $\boldsymbol{Q}$-curves E.

1) $D = -4 \cdot 3 \cdot 7$.

Let $\mathfrak{p}$ and $\mathfrak{p}'$ be the prime ideals of K such that $\mathfrak{p}^2 = (2 + \sqrt{-21})$ and $\mathfrak{p}'^2 = (10 + \sqrt{-21})$. The decomposition field in H of $\mathfrak{p}$ is $K(\sqrt{21})$ and that of $\mathfrak{p}'$ is $K(\sqrt{3})$. We see that Cl_K is generated by $\mathfrak{p}$ and $\mathfrak{p}'$. Let $\mathfrak{q}$ be the prime ideal of K with $\mathfrak{q}^2 = (3)$. Let ϕ_0 be a character of I_K of conductor $\mathfrak{q}$ such that

$$\phi_0((\alpha)) = \left(\frac{\alpha}{\mathfrak{q}}\right)\alpha \quad \text{for every } \alpha \in K^\times,$$

where $(\alpha/\mathfrak{q})$ denotes the norm residue symbol. Then ϕ_0 satisfies (5) and put $\psi_0 = \phi_0 \circ N_{H/K}$. Using local characters (see §2), we define:

$$\omega_1 = \eta_3\eta_7 \circ N_{H/K}, \quad \omega_2 = \eta_{-4} \circ N_{H/K}.$$

Since $(21, -3)$ is trivial in $\mathrm{Br}_2(\boldsymbol{Q})$, there exists a D_4-extension k_0 over $\boldsymbol{Q}$ containing $\boldsymbol{Q}(\sqrt{-3}, \sqrt{21})$. Let χ be the character of I_H associated with k_0H/H. Then by Theorem 2, the equivalence classes of $\boldsymbol{Q}$-curves over H are exactly represented by the Hecke characters $\psi = \psi_0\omega$, $\omega \in \langle\omega_1, \omega_2, \chi\rangle$.

(a) $\psi = \psi_0$. A simple calculation shows that

$$\phi_0(\mathfrak{p}^2) = -2 - \sqrt{-21} = \left(\frac{\sqrt{6} - \sqrt{-14}}{2}\right)^2 \quad \text{and} \quad \phi_0(\mathfrak{p}\mathfrak{p}^\rho) = \phi_0((5)) = -5.$$

Therefore $\phi_0(\mathfrak{p}) + \phi_0(\mathfrak{p}^\rho) = \pm\sqrt{-14}$. Similarly we have $\phi_0(\mathfrak{p}') + \phi_0(\mathfrak{p}'^\rho) = \pm\sqrt{-2}$, since $\phi_0(\mathfrak{p}'^2) = ((\sqrt{42} + \sqrt{-2})/2)^2$ and $\phi_0(\mathfrak{p}'\mathfrak{p}'^\rho) = -11$. Hence $R_0 = \boldsymbol{Q}(\sqrt{-2}, \sqrt{-14})$.

(b) $\psi = \psi_0\omega_1$. We have:

$$\eta_3\eta_7(\mathfrak{p}^2) = -1, \quad \eta_3\eta_7((5)) = 1, \quad \eta_3\eta_7(\mathfrak{p}'^2) = -1, \quad \eta_3\eta_7((11)) = -1.$$

This implies $R_0 = \boldsymbol{Q}(\sqrt{-6}, \sqrt{2})$.

(c) $\psi = \psi_0 \cdot \chi$. We have:

$k_0H/K(\sqrt{21})$ is of type $(2,2)$ and $k_0H/\boldsymbol{Q}(\sqrt{21})$ is abelian;

$k_0H/K(\sqrt{3})$ is cyclic of order 4 and $k_0H/\boldsymbol{Q}(\sqrt{3})$ is non-abelian.

Applying Proposition 7, we obtain that R_0 is a division quaternion algebra $(-42, -14)$ over $\boldsymbol{Q}$.

The remaining cases are similarly computed and we have:

ψ	R_0 (field)
ψ_0	$\boldsymbol{Q}(\sqrt{-2}, \sqrt{-14})$
$\psi_0\omega_1$	$\boldsymbol{Q}(\sqrt{-6}, \sqrt{2})$
$\psi_0\omega_2$	$\boldsymbol{Q}(\sqrt{-6}, \sqrt{-42})$
$\psi_0\omega_1\omega_2$	$\boldsymbol{Q}(\sqrt{-14}, \sqrt{-42})$

ψ	R_0 (quaternion alg.)
$\psi_0\chi$	$(-14, -42)$
$\psi_0\omega_1\chi$	$(-6, 42)$
$\psi_0\omega_2\chi$	$(-6, -2)$
$\psi_0\omega_1\omega_2\chi$	$(-14, 2)$

Remark. The division quaternion algebras $(-14, -42)$ and $(-6, -2)$ over $\boldsymbol{Q}$ are isomorphic because they ramify at the same primes 2 and ∞. The quaternion algebras $(-6, 42)$ and $(-14, 2)$ are isomorphic to $M_2(\boldsymbol{Q})$.

2) $D = -3 \cdot 5 \cdot 13$.

Let $\mathfrak{p}$ and $\mathfrak{p}'$ be the prime ideals of K such that $\mathfrak{p}^2 = ((1 + \sqrt{D})/2)$ and $\mathfrak{p}'^2 = ((17 + \sqrt{D})/2)$. The decomposition field in H of $\mathfrak{p}$ is $K(\sqrt{65})$ and that of $\mathfrak{p}'$ is $K(\sqrt{5})$. We see that Cl_K is generated by $\mathfrak{p}$ and $\mathfrak{p}'$. Let $\mathfrak{q}$ be the prime ideal of K with $\mathfrak{q}^2 = (3)$. Let ϕ_0 be a character of I_K of conductor $\mathfrak{q}$ such that

$$\phi_0((\alpha)) = \left(\frac{\alpha}{\mathfrak{q}}\right)\alpha \quad \text{for every } \alpha \in K^\times$$

and put $\psi_0 = \phi_0 \circ N_{H/K}$. As in Case 1) we define:

$$\omega_1 = \eta_5 \circ j \circ N_{H/K}, \quad \omega_2 = \eta_{13} \circ j \circ N_{H/K}.$$

Since $(13, -3)$ is trivial in $\mathrm{Br}_2(\boldsymbol{Q})$, there exists a D_4 extension k_0 over $\boldsymbol{Q}$ containing $\boldsymbol{Q}(\sqrt{-3}, \sqrt{13})$. Let χ be the character of I_H associated with k_0H/H. Then by Theorem 2, the equivalence classes of $\boldsymbol{Q}$-curves over H are represented by the Hecke characters $\psi = \psi_0\omega$, $\omega \in \langle\omega_1, \omega_2, \chi\rangle$. By similar computations as in 1), we obtain:

ψ	R_0 (field)
ψ_0	$\boldsymbol{Q}(\sqrt{13}, \sqrt{-5})$
$\psi_0\omega_1$	$\boldsymbol{Q}(\sqrt{-13}, \sqrt{-5})$
$\psi_0\omega_2$	$\boldsymbol{Q}(\sqrt{-13}, \sqrt{5})$
$\psi_0\omega_1\omega_2$	$\boldsymbol{Q}(\sqrt{13}, \sqrt{5})$

ψ	R_0 (quaternion alg.)
$\psi_0\chi$	$(-15, -39)$
$\psi_0\omega_1\chi$	$(15, -39)$
$\psi_0\omega_2\chi$	$(15, 39)$
$\psi_0\omega_1\omega_2\chi$	$(-15, 39)$

REMARK. The division quaternion algebras $(15, -39)$ and $(-15, 39)$ over $\boldsymbol{Q}$ are isomorphic because they ramify at the same primes 3 and 13.

Next we give an example of exceptional case.

Let $K = \boldsymbol{Q}(\sqrt{-5})$. Then

$$h_K = t = 2, \quad H = K(\sqrt{-1}), \quad H^{(2)} = H(\sqrt{1+\sqrt{5}}).$$

In this case there exist two classes of $\boldsymbol{Q}$-curves over $H^{(2)}$ by Theorem 2. Let $\mathfrak{m}$ be the prime ideal of K with $\mathfrak{m}^2 = (2)$. As in the proof of Theorem 2, there exists a $\boldsymbol{Q}$-curve E_0 over $H^{(2)}$ such that $\psi_{E_0} = \phi_0 \circ N_{H^{(2)}/K}$, where $\phi_0 : U_{K,2} \to \pm 1$ has conductor $\mathfrak{m}^3$. Let $\mathfrak{q}$ be the prime ideal of K such that $\mathfrak{q}^2 = (2+\sqrt{-5})$. The Frobenius automorphism associated with $\mathfrak{q}$ in $\mathrm{Gal}(H^{(2)}/K)$ has order 4. We easily have

$$\phi_0(\mathfrak{q}^4) = -(2+\sqrt{-5})^2, \quad \phi_0(\mathfrak{q}\mathfrak{q}^\rho) = -3.$$

Therefore we obtain

$$\phi_0(\mathfrak{q})^2 + \phi_0(\mathfrak{q}^\rho)^2 = \pm 2\sqrt{5}, \quad \phi_0(\mathfrak{q}) + \phi_0(\mathfrak{q}^\rho) = \pm(\sqrt{-5} \mp \sqrt{-1}).$$

Hence we have $R_0 = \mathrm{End}_{\boldsymbol{Q}}(R_{H^{(2)}/K}(E_0)) \otimes \boldsymbol{Q} \cong H$. The other class of $\boldsymbol{Q}$-curves over $H^{(2)}$ is represented by a Hecke character $(\phi_0 \cdot \eta_5) \circ N_{H^{(2)}/K}$. Computing similarly we find that $R_0 \cong \boldsymbol{Q}(\sqrt{5}) \oplus \boldsymbol{Q}(\sqrt{5})$.

References

[G] B. H. Gross, Arithmetic on elliptic curves with complex multiplication, Lecture Notes in Math., **776**, Springer-Verlag, 1980.

[J-Y] L. U. Jensen and N. Yui, Quaternion extensions, In: Algebraic Geometry and Commutative Algebra, Vol. 1, Kinokuniya, Tokyo, 1988, 155–182.

[M] R. Massy, Construction de p-extensions Galoisiennes d'un corps de caractéristique différente de p, J. Algebra, **109** (1987), 508–535.

[N] T. Nakamura, Abelian varieties associated with elliptic curves with complex multiplication, Acta Arith., **97** (2001), 379–385.

[Q] J. Quer, $\boldsymbol{Q}$-curves and abelian varieties of GL_2-type, Proc. London Math. Soc., **81** (2000), 285–317.

[S] G. Shimura, On the zeta function of an abelian variety with complex multiplication, Ann. of Math., **94** (1971), 504–533.

[S-T] G. Shimura and Y. Taniyama, Complex Multiplication of Abelian Varieties and its Application to Number Theory, Publ. Math. Soc. Japan, No. 6, Math. Soc. Japan, Tokyo, 1961.

[Si] J. H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Springer-Verlag, 1994.

Tetsuo NAKAMURA

Mathematical Institute
Tohoku University
Sendai 980-8578
Japan
E-mail: nakamura@math.tohoku.ac.jp