79. Classification of a Family of Abelian Varieties Parametrized by Reduction modulo $\mathfrak{P}$ of a Shimura Curve

By Yasuo MORITA
Department of Mathematics, Faculty of Science, Hokkaido University

(Communicated by Shokichi IYANAGA, M. J. A., Sept. 12, 1980)

Deuring classified elliptic curve defined over $\bar{F}_p$ in [2]. In this paper, we obtain similar results for a certain family of abelian varieties parametrized by reduction modulo $\mathfrak{P}$ of a Shimura curve. The results may be regarded as a generalization of an unpublished paper of Shimura in which he obtained similar results for the canonical family of abelian varieties parametrized by reduction modulo $\mathfrak{P}$ of the Shimura curve for the unit group of a maximal order of an indefinite quaternion algebra over $\boldsymbol{Q}$.

§1. **Notation and assumptions.** Let the notation be as in Shimura [9] (and [10]), and let $\Omega_0=(L, \Phi, \rho; F^+\cdot T, \mathfrak{M})$ be the weak PEL-type which Shimura constructed in 7.13 of [9] (we assume that Ω_0 has no level structure). Let p be a prime number, and let $p=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_t^{e_t}$ be the factorization of p in $\mathfrak{r}_F$. Let $\mathfrak{p}=\mathfrak{p}_1$, and let $\mathfrak{P}$ be an extension of $\mathfrak{p}$ to a place of $\boldsymbol{C}$. We assume that (i) $\mathfrak{p}$ does not divide the discriminant $D(B/F)$ of B; (ii) each $\mathfrak{p}_i$ $(i=1, \cdots, t)$ is decomposed in K/F as $\mathfrak{p}_i=\mathfrak{P}_i\overline{\mathfrak{P}}_i$; (iii) $\tau_1=\mathrm{id.}$ and none of the $\overline{\mathfrak{P}}_i^{\tau_\nu}$ $(i=1, \cdots, t, \nu=1, \cdots, g)$ is contained in $\mathfrak{P}$. We note that there exist infinitely many such extensions $(K, \tau_1, \cdots, \tau_g)$ for each given $(F, \tau_{0,1}=\mathrm{id.}, \cdots, \tau_{0,g})$.

§2. **Representations of $\mathfrak{r}_K$ on tangent spaces.** Let $\mathcal{R}=(A, \mathcal{D}, \theta)$ be a weak PEL-structure of type Ω_0. If $\mathcal{R}$ has good reduction at $\mathfrak{P}$, then let $\tilde{\mathcal{R}}=(\tilde{A}, \tilde{\mathcal{D}}, \tilde{\theta})$ be $\mathcal{R}$ modulo $\mathfrak{P}$ (cf. Morita [7]). Then we have a representation Σ of the ring $\mathfrak{r}_K/p\mathfrak{r}_K$ on the tangent space at the origin of $\tilde{A}$. Since this representation is obtained by taking reduction modulo $\mathfrak{P}$ of the representation of $\mathfrak{r}_K$ at the origin of A, and since $\mathcal{R}$ is of type Ω_0, we can determine Σ. The result is the following: For each $\mathfrak{P}_i$, let f_i and π_i be the residue degree of $\mathfrak{p}_i$ and a prime element of $\mathfrak{P}_i$, and let $\tau(i)$ be an element of $\{\tau_1, \cdots, \tau_g\}$ satisfying $\mathfrak{P}_i^{\tau(i)}\subseteqq\mathfrak{P}$. We assume $\tau(1)=\tau_1$. Since $\mathfrak{o}_\mathfrak{p}\cong M_2(\mathfrak{r}_{F\mathfrak{p}})$, and since elements of $\mathfrak{o}$ and elements of $\mathfrak{r}_K$ commute, Σ is the direct sum of two copies of a representation Σ' of $\mathfrak{r}_K$. Let α be an element of $\mathfrak{r}_K$. Then the set of eigen values of $\Sigma'(\alpha)$ is $\{\alpha \bmod \mathfrak{P}\ (2e_1-1 \text{ times}), \bar{\alpha} \bmod \mathfrak{P}\ (\text{once}), \alpha^{p^j\tau(i)} \bmod \mathfrak{P}\ (1\leq i\leq t, 0\leq j\leq f_i-1, (i,j)\neq(1,1), 2e_i \text{ times})\}$. Accordingly, we can decompose

Σ' into the direct sum of the subrepresentations Σ'_{11}, $\bar{\Sigma}'_{11}$, Σ'_{ij} $((i,j)\neq(1,1))$. Then $\Sigma'_{11}(\pi_1)$ and $\Sigma'_{ij}(\pi_i)$ are represented by

$$\begin{bmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{bmatrix} \oplus \begin{bmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{bmatrix} \in M_{e_1-1}(\boldsymbol{F}_p)\oplus M_{e_1}(\boldsymbol{F}_p)$$

and

$$\begin{bmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{bmatrix} \oplus \begin{bmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{bmatrix} \in M_{e_i}(\boldsymbol{F}_p)\oplus M_{e_i}(\boldsymbol{F}_p).$$

§ 3. **The Frobenius element.** Now we assume that $\tilde{\mathfrak{R}}$ is defined over a finite field $\boldsymbol{F}_q$. Let π be the q-th power endomorphism of $\tilde{A}$. We say $\tilde{\mathfrak{R}}$ is *super-singular* if some power of π belongs to $\tilde{\theta}(\mathfrak{r}_K)$. Otherwise we say $\tilde{\mathfrak{R}}$ is *singular*. Let $G_{n,m}$ be as in Manin [6]. Then we have the following

Theorem 1. *If $\tilde{\mathfrak{R}}$ is super-singular,*

(i) End $(\tilde{A},\tilde{\theta})\otimes_{\boldsymbol{Z}}\boldsymbol{Q}$ *is isomorphic to the tensor product over F of K and the totally definite quaternion algebra D over F with discriminant $\mathfrak{p}D(B/F)$.*

(ii) *If $q=p^{2af_1}$ is sufficiently large, then*

$$(\tilde{\theta}^{-1}(\pi))=\mathfrak{P}_1^{(2e_1f_1-1)a}\bar{\mathfrak{P}}_1^{a}\mathfrak{P}_2^{2e_2af_1}\cdots\mathfrak{P}_t^{2e_taf_1}.$$

(iii) *Let $T_p(\tilde{A})=\oplus_{i=1}^t(T_{\mathfrak{P}_i}(\tilde{A})\oplus T_{\bar{\mathfrak{P}}_i}(\tilde{A}))$ be the decomposition of the p-divisible group $T_p(\tilde{A})$ of $\tilde{A}$ by the action of $\mathfrak{r}_K$. Then* (a) *the $T_{\mathfrak{P}_i}(\tilde{A})$ $(i\geq 2)$ are multiplicative,* (b) *the $T_{\bar{\mathfrak{P}}_i}(\tilde{A})$ $(i\geq 2)$ are etale, and* (c) *$T_{\mathfrak{P}_i}(\tilde{A})\cong 2G_{2e_1f_1-1,1}$ and $T_{\mathfrak{P}_i}(\tilde{A})\cong 2G_{1,2e_1f_1-1}$.*

Theorem 2. *If $\tilde{\mathfrak{R}}$ is singular,*

(i) End $(\tilde{A},\tilde{\theta})\otimes_{\boldsymbol{Z}}\boldsymbol{Q}$ *is isomorphic to the tensor product over F of K and another totally imaginary quadratic extension M of F such that* (a) *$B\otimes_F M\cong M_2(M)$ and* (b) *$\mathfrak{p}$ is decomposed in M/F.*

(ii) *Let $\mathfrak{p}=\mathfrak{Q}'\mathfrak{Q}''\bar{\mathfrak{Q}}'\bar{\mathfrak{Q}}'$ $(\mathfrak{P}_1\subseteqq\mathfrak{Q}'$, $\mathfrak{P}_1\subseteqq\mathfrak{Q}''$, $\mathfrak{Q}'\subseteqq\mathfrak{P})$ be the decomposition of $\mathfrak{p}$ in $K\otimes_F M$. If $q=p^{af_1}$ is sufficiently large, then there exist elements λ and μ of M and K such that $\tilde{\theta}^{-1}(\pi)=\lambda\mu$, $(\lambda)=(\bar{\mathfrak{Q}}'\mathfrak{Q}'')^a$ and $(\mu)=\mathfrak{P}_1^{(e_1f_1-1)a}\mathfrak{P}_2^{e_2f_1a}\cdots\mathfrak{P}_t^{e_tf_1a}$.*

(iii) *Let $T_p(\tilde{A})\cong\oplus_{i=1}^t(T_{\mathfrak{P}_i}(\tilde{A})\oplus T_{\bar{\mathfrak{P}}_i}(\tilde{A}))$ be the decomposition of the p-divisible group $T_p(\tilde{A})$ of $\tilde{A}$ by the action of $\mathfrak{r}_K$. Then* (a) *the $T_{\mathfrak{P}_i}(\tilde{A})$ $(i\geq 2)$ are multiplicative,* (b) *the $T_{\bar{\mathfrak{P}}_i}(\tilde{A})$ $(i\geq 2)$ are etale, and* (c) *$T_{\mathfrak{P}_i}(\tilde{A})\cong 2(G_{e_1f_1-1,1}\oplus e_1f_1G_{1,0})$ and $T_{\bar{\mathfrak{P}}_i}(\tilde{A})\cong 2(G_{1,e_1f_1-1}\oplus e_1f_1G_{0,1})$.*

§ 4. **Classification.** Let $\Omega_0=(L,\Phi,\rho\,;F^+T,\mathfrak{M})$ be as in § 1. Then $G^+(T)=\{\alpha\in L\mid T(x\alpha,y\alpha)=\mu(\alpha)T(x,y)$ for some $\mu(\alpha)\in F^+\}=K^\times B^+$. Let $\boldsymbol{X}$ and $\boldsymbol{Y}$ be sets of representatives of $\{x\in B_A^\times\mid \mathfrak{o}x=\mathfrak{o}\}\backslash B_A^\times/B^+$ and $\{x\in K_A^\times\mid \mathfrak{r}_K x=\mathfrak{r}_K\}F_A^\times\backslash K_A^\times/K^\times$. For any $x\in\boldsymbol{X}$ and $y\in\boldsymbol{Y}$, let $\Omega_{0,x,y}$

$=(L, \Phi, \rho; F^+T, y\mathfrak{M}x)$, and let $\Sigma(\Omega_{0,x,y})$ be the family of weak PEL-structures of type $\Omega_{0,x,y}$. By 7.3 of Shimura [9], we may assume that $\Sigma(\Omega_{0,x,y})$ is parametrized by the complex upper-half-plane $\mathfrak{H}$, and that the action of $\alpha \in B^+ \subseteqq G^+(T)$ coincides with the usual action as an element of $B^+ \subseteqq GL^+(2, \boldsymbol{R})$.

We say that $\mathcal{R}_z \in \Sigma(\Omega_{0,x,y})(z \in \mathfrak{H})$ is *singular* if $\{\alpha \in B^+ \mid \alpha(z)=z, y\mathfrak{M}x\alpha \subset y\mathfrak{M}x\}$ is the set $\mathfrak{r}(\mathcal{R}_z)\backslash\{0\}$ of non-zero elements of an order $\mathfrak{r}(\mathcal{R}_z)$ of a totally imaginary quadratic extension $M(\mathcal{R}_z)$ of F. Let $\mathcal{C}$ be the set consisting of all isomorphism classes of singular $\mathcal{R}_z \in \Sigma(\Omega_{0,x,y})$ $(x \in \boldsymbol{X}, y \in \boldsymbol{Y}, z \in \mathfrak{H})$ such that $\mathfrak{p}$ is decomposed in $M(\mathcal{R}_z)/F$ and the conductor of $\mathfrak{r}(\mathcal{R}_z)$ is prime to $\mathfrak{p}$. Let $\mathcal{F}$ be the set consisting of all isomorphism classes of $\tilde{\mathcal{R}}_z = \mathcal{R}_z$ modulo $\mathfrak{P}$ of elements $\mathcal{R}_z$ of $\Sigma(\Omega_{0,x,y})$ $(x \in \boldsymbol{X}, y \in \boldsymbol{Y}, z \in \mathfrak{H})$ which can be defined over $\bar{\boldsymbol{F}}_p$, and let $\mathcal{F}_s$ and $\mathcal{F}_{ss}$ be the subsets of $\mathcal{F}$ consisting of singular elements and super-singular elements, respectively.

Theorem 3. (i) *Let $\mathcal{R}_z$ be a singular element of $\Sigma(\Omega_{0,x,y})$ $(x \in \boldsymbol{X}, y \in \boldsymbol{Y})$. Then $\mathcal{R}_z$ belongs to $\mathcal{F}$. $\tilde{\mathcal{R}}_z$ belongs to $\mathcal{F}_s$ iff $\mathfrak{p}$ is decomposed in $M(\mathcal{R}_z)/F$.*

(ii) *Reduction* modulo $\mathfrak{P}$ *induces a bijection of $\mathcal{C}$ to $\mathcal{F}_s$. Furthermore, for any two elements $\mathcal{R}$ and $\mathcal{R}'$ of $\mathcal{C}$, reduction* modulo $\mathfrak{P}$ *induces a bijection of* Hom $((A, \theta), (A', \theta'))$ *to* Hom $((\tilde{A}, \tilde{\theta}), (\tilde{A}', \tilde{\theta}'))$.

(iii) *Let $\tilde{\mathcal{R}}$ be an element of $\mathcal{F}_{ss}$, and let* End $(\tilde{\mathcal{R}})$ *be the set of all isogenies of $\tilde{\mathcal{R}}$ onto $\tilde{\mathcal{R}}$. Then* End $(\tilde{\mathcal{R}})$ *can be identified with the set of all $\mathfrak{r}_F$-valued points of the F-group $K^\times \cdot D^\times = \{k \cdot d \in K \otimes_F D \mid k \in K^\times, d \in D^\times\}$* (*cf.* Theorem 2). *For each prime ideal $\mathfrak{l}$ of F,* End $(\tilde{\mathcal{R}})_\mathfrak{l}$ *is identified with $\{k \cdot d \in K_\mathfrak{l} \otimes_{F_\mathfrak{l}} D_\mathfrak{l} \mid k \in K_\mathfrak{l}^\times \cap \mathfrak{r}_{K_\mathfrak{l}}, d \in D_\mathfrak{l}^\times \cap \mathcal{O}_\mathfrak{l}\}$, where $\mathcal{O}_\mathfrak{l}$ is a maximal order of $D_\mathfrak{l}$. Furthermore,* (a) *for any element $k \cdot d$ of $K_A^\times \cdot D_A^\times$, the $k \cdot d$-multiplication of $\tilde{\mathcal{R}}$ belongs to $\mathcal{F}_{ss}$ and* (b) *this map induces a bijection of $\prod_\mathfrak{l}$* End $(\tilde{\mathcal{R}})_\mathfrak{l} \cdot K_\infty^\times \cdot D_\infty^\times \backslash K_A^\times \cdot D_A^\times / K^\times \cdot D^\times$ *to $\mathcal{F}_{ss}$. In particular, any two elements of $\mathcal{F}_{ss}$ are separably isogenious.*

Remark. Let $\mathfrak{e}$ be an integral ideal of K which is prime to $\mathfrak{p}_1\mathfrak{P}_2 \cdots \mathfrak{P}_t$. Then we can obtain similar results for the family of weak PEL-structures (or PEL-structures) with level $\mathfrak{e}$-structures. In particular, by making use of Eichler [3] and Shimizu [8], we can show that the number of super-singular PEL-structures with level $\mathfrak{e}$-structures coincides with the number which Ihara defined in [4], if $\mathfrak{e}$ is divisible by a rational integer e satisfying $e \geq 3$.

Remark. Our results hold without assuming $F \neq \boldsymbol{Q}$ (cf. Shimura [9, p. 192, footnote 4]).

References

[1] M. Demazure: Lecture on p-divisible groups. Lect. notes in Math., vol. 302, 1–98 (1972).

[2] M. Deuring: Die Typen der Multiplicatorenringe elliptischer Funktionenkörper. Abh. Math. Sem. Hamburg, **14**, 197–272 (1941).

[3] M. Eichler: Über die Idealklassenzahl total definiter Quarternionalgebren. Math. Z., **43**, 102–109 (1938).

[4] Y. Ihara: On congruence monodromy problems. vol. 1, Lect. note at Univ. of Tokyo (1968).

[5] ——: Some fundamental groups in the arithmetic of algebraic curves over finite fields. Proc. Nat. Acad. Sci. U. S. A., **72**, 3281–3284 (1975).

[6] I. Manin: The theory of commutative formal groups over fields of finite characteristics. Russian Math. Survey, **18**, 1–83 (1963) (English trans.).

[7] Y. Morita: On potential good reduction of abelian varieties. J. Fac. Sci. Univ. Tokyo, sec. IA, **22**, 437–447 (1975).

[8] H. Shimizu: On zeta functions of quaternion algebras. Ann. of Math., **81**, 166–193 (1965).

[9] G. Shimura: Construction of class fields and zeta functions of algebraic curves. Ibid., **85**, 58–159 (1967).

[10] ——: On canonical models of arithmetic quotients of bounded symmetric domains. Ibid., **91**, 144–222 (1970).

[11] J. Tate: Endomorphisms of abelian varieties over finite fields. Invent. Math., **2**, 134–144 (1966).

[12] W. C. Waterhouse and J. S. Milne: Abelian varieties over finite fields. Proc. Symp. Pure Math., **20**, 53–64 (1971).