Ihara's conjectures and moduli spaces of abelian varieties

By Yasuo Morita

§ 0. Introduction

0-1. The main results. Let $G = PSL(2, \mathbb{R}) \times PSL(2, k_{\mathfrak{p}})$, where $\mathbb{R}$ and $k_{\mathfrak{p}}$ are the real number field and a $\mathfrak{p}$-adic number field respectively. Let Γ be a discrete subgroup of G such that the volume of $\Gamma\backslash G$ is finite and the projection of Γ in each component of G is dense. Y. Ihara has conjectured in [4] that such a group would describe a non-abelian class field theory over an algebraic function field of one variable with a finite constant field. Moreover, he has studied the zeta function of the group Γ and checked his conjecture in a special case. Therefore, we shall call such a group Γ an Ihara-group in this paper. Our object in this paper is also such a group Γ. Let B be an indefinite quaternion algebra over the rational number field $\mathbb{Q}$, $\mathfrak{O}$ a maximal order of B. Let p be a prime number not dividing the discriminant of B. Put $\Gamma(1) = \{\gamma \in \mathfrak{O} \mid N_{B/\mathbb{Q}}(\gamma) = 1\}$, $\Gamma(1, p) = \{\gamma \in \mathfrak{O} \otimes \mathbb{Z}^{(p)} \mid N_{B/\mathbb{Q}}(\gamma) = 1\}$, where $N_{B/\mathbb{Q}}(\gamma)$ is the reduced norm of γ and $\mathbb{Z}^{(p)} = \bigcup_{l=0}^{\infty} p^{-l}\mathbb{Z} \subset \mathbb{Q}$. If we fix an isomorphism $B \otimes_{\mathbb{Q}} \mathbb{R} \cong M_2(\mathbb{R})$, $\Gamma(1)$ and $\Gamma(1, p)$ can be considered as subgroups of $SL(2, \mathbb{R})$ and hence they operate on the complex upper half plane $\mathfrak{H} = \{ z \in \mathbb{C} \mid \mathrm{Im}\, z > 0 \}$ in the usual manner; $\mathfrak{H} \ni z \longmapsto \gamma z = \frac{az+b}{cz+d} \in \mathfrak{H}$, where $\gamma = \begin{pmatrix} a, & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{R})$. Moreover we can consider $\Gamma(1, p)$ as a discrete

subgroup of $G_0 = SL(2, \mathbb{R}) \times SL(2, \mathbb{Q}_p)$ such that the quotient space $\Gamma(1, p) \backslash G_0$ has a finite volume and that the projection of $\Gamma(1, p)$ in each component of G_0 is dense. Therefore $\Gamma(1, p)/\{\pm 1\}$ is an Ihara-group. This group is the main object in this paper. Put $E_p = \{ z \in \mathfrak{H} \mid$ the isotropy group $\Gamma(1, p)_z$ is infinite $\}$ and $P(\Gamma(1, p)) = \Gamma(1, p) \backslash E_p$ i.e. the set of $\Gamma(1, p)$ - equivalence classes of E_p. Then we can define the degree of $P \in P(\Gamma(1, p))$ in a certain manner (c.f. § 6). Let $\widetilde{\Gamma}(1, p)$ be the completion of $\Gamma(1, p)$ by the topology in which the set of all the congruence subgroups makes a fundamental system of neighbourhoods of the unity.

By the way, if B is $M_2(\mathbb{Q})$, then $\Gamma(1, p) = SL(2, \mathbb{Z}^{(p)})$. Ihara has checked hisconjectures about this group. Therefore we shall exclude this case and assume B is a division algebra. Then we have the following two theorems.

Theorem A. *There exist an algebraic function field K_p of one variable with the finite constant field $\mathbb{F}_{p^2}$ and a map ℓ_p from E_p to the set $P(K_p)$ of prime divisors of K_p which satisfy the following conditions.*

① *ℓ_p induces a degree preserving injective map from $P(\Gamma(1, p)) = \Gamma(1, p) \backslash E_p$ to $P(K_p)$.*

② *The set $P(K_p) - \ell_p\{ P(\Gamma(1, p))\}$ is a finite set. Moreover, all the element of it have degree one over the constant field $\mathbb{F}_{p^2}$.*

Theorem B. *There exist an infinite Galois extension K_p*

of K_p, an injection g_p from $\Gamma(1, p)/\{\pm 1\}$ to $\mathrm{Gal}(K_p/K_p)$ and a map L_p from E_p to the set $P(K_p)$ of prime divisors of K_p which is an extension of ℓ_p, satisfying the following conditions.

① g_p is continuous and induces an isomorphism from $\tilde{\Gamma}(1, p)/\{\pm 1\}$ to $\mathrm{Gal}(K_p/K_p)$.

② L_p satisfies $L_p(z)^{g(\gamma)} = L_p(\gamma(z))$ for all $z \in E_p$ and $\gamma \in \Gamma(1, p)$ i.e. L_p is compatible with the operations of $\Gamma(1, p)$.

③ Let $z \in E_p$. Then the decomposition group and the inertia group of $L(z)$ are given by $g_p(\Gamma(1, p)_z/\{\pm 1\})$ and $g_p(\Gamma(1)_z/\{\pm 1\})$ respectively.

④ Any prime divisor of K_p whose restriction to K_p does not belong to $\ell_p\{P(\Gamma(1, p))\}$ has degree on over F_{p^2}.

Theorem A describes how we can associate the group $\Gamma(1, p)$ with the algebraic function field K_p and Theorem B describes how we can know the decomposition law in the infinite Galois extension K_p/K_p by the group $\Gamma(1, p)$. These are the main results of this paper.

0-2. An outline of the proof. Y. Ihara has obtained the above theorems in the case of $B = M_2(Q)$ by using elliptic curves (c.f. [4], Chap. 5). His proof is base on the classifications of elliptic curves defined over finite fields which is due to M. Deuring (c.f. [1]) and the construction of moduli spaces for the families of elliptic curves which is due to J. Igusa (c.f. [21],

[22]). Our proof of the above theorems is a generalization of his methods.

Let N be a natural number, $\Gamma(N, p) = \{\gamma \in \Gamma(1, p) \mid \gamma \equiv 1 \mod^{\times} N\}$ and $\Gamma(N) = \{\gamma \in \Gamma(1) \mid \gamma \equiv 1 \mod^{\times} N\}$. G. Shimura has constructed in [10] and [23] a family of abelian varieties parametrized by $\Gamma(N)\backslash H$. Moreover he has shown in [11] that there is a complete non-singular curve V_N defined over $\mathbb{Q}(e^{\frac{2\pi i}{N}})$ which is biregularly equivalent to $\Gamma(N)\backslash H$ and which makes a moduli space of the family (we summarize these Shimura's results in §1). Now, our first task is to construct a reduction modulo p of V_N which is compatible with the property that V_N is the moduli space of the family. This is settled in §5 rather elementarily by using the Mumford's moduli theory and some properties of abelian varieties and Chow points of projective varieties (c.f. Theorem 4). Then the next task is to show that $V_N \mod p$ is a complete non-singular curve. This turns out to be the hardest point in our paper. In order to settle this task, we classify the family of abelian varieties defined over finite fields which are obtained as reduction modulo p of some members of the above family (we classify these abelian varieties in §4, Theorem 2 and Theorem 3 and reformulate it in §6, Theorem 5). By using this classification and the fact that $V_N \mod p$ is a moduli space for this family, we calculate the congruence zeta functions of the algebraic cycle $V_N \mod p$. It is expressed in a simple form by the zeta functions of the group $\Gamma(N, p)$, which was defined and calculated in Ihara, [4] (c.f.

§ 6, Theorem 5). Then we conclude from the form of the congruence zeta function that there is some model of V_N such that $\tilde{V}_N = V_N \bmod \mathfrak{p}$ ($\mathfrak{p}$ may be any prime ideal of $Q(e^{\frac{2\pi i}{N}})$ not dividing N and the discriminant of B) is a complete non-singular curve which is a moduli space for the family (c.f. § 6, Theorem 7). The last task is to show our theorems by using these facts. First, by using the classification of the members of the above family and the fact that $\tilde{V}_N$ is a moduli space for this family, we show some arithmetic properties of $\tilde{V}_N$ which describes in terms of the fixed points of $\Gamma(N, p)$ what and how many rational points are on $\tilde{V}_N$ (c.f. § 7, Main Theorem 1). Then, by using these properties, we descend the field of the rationality of $\tilde{V}_N$ to the finite field F_{p^2}. Let K_N be the function field of $\tilde{V}_N$ over F_{p^2}. Put $K_p = K_1$, $K_{\mathfrak{p}} = \bigcup_{(N,p)=1} K_N$. Then the arithmetic properties of $\tilde{V}_N$ are translated in the terms of the function fields as our theorem (c.f. § 7, Main Theorem 2).

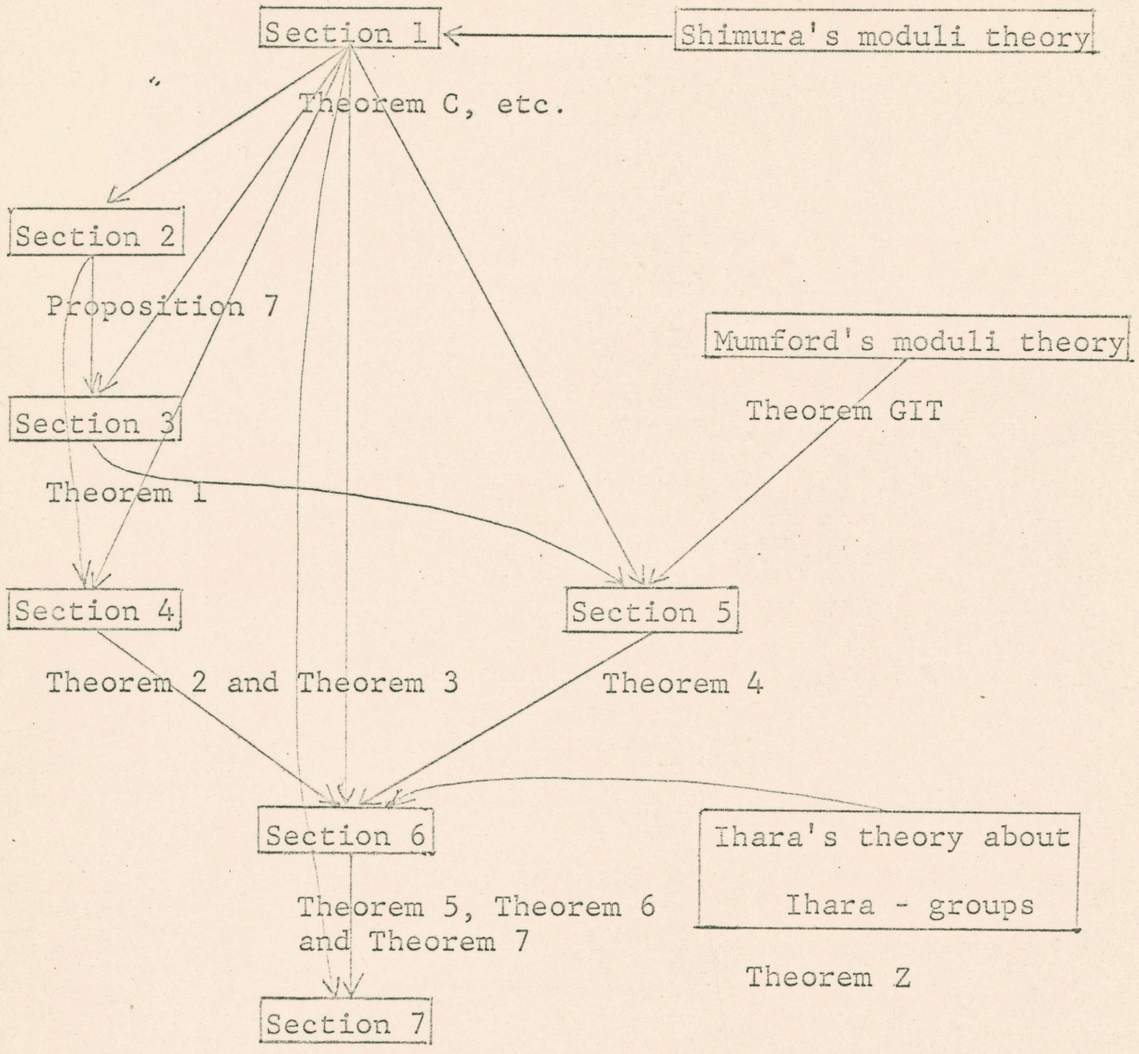
0-3. A few remarks. The classification of abelian varieties i.e. the results in § 4 is due to G. Shimura. Moreover, the author heard from him that he had proved our theorem for $\Gamma(1, p)$ for almost all p, using the theory of almost all $\mathfrak{p}$. Note that our theorem is not for almost all p but for all p (not dividing the discriminant of B). Y. Ihara gave me a comment that we should prove our theorem not for almost all p but all p and my starting point was this comment.

Lastly the author wants to thank Professor G. Shimura who informed the author of his unpublished results i.e. the results

of § 4 and Professor Y. Ihara who gave the author the above-mentioned valuable comment and some other remarks.

Contents

Interdependence of each section.



Main Theorem 1 and Main Theorem 2.

Notation. $\underset{\sim}{Z}$, $\underset{\sim}{Q}$, $\underset{\sim}{Z}_p$, $\underset{\sim}{Q}_p$, $\underset{\sim}{R}$, $\underset{\sim}{C}$, $\underset{\sim}{F}_q$ denote the ring of rational integers, the field of rational numbers, the ring of p-adic integers, the field of p-adic numbers, the field of real numbers, the field of complex numbers, the finite field with q elements respectively. Let S be an associative ring with an identity element. Then $M_n(S)$ denotes the ring of all matrices of size n with entries in S and $GL_n(S)$ the group of invertible elements of $M_n(S)$. In particular $S^\times$ denotes the group of invertible elements of S. Let G, G' be S-modules. Then $\mathrm{Hom}_S(G, G')$, $\mathrm{End}_S(G)$ denote the S-module of all the S-homomorphisms from G to G', the S-algebra of all the S-endomorphisms of G respectively. Let K be a field, k its subfield. Then $\mathrm{Aut}(K/k)$ denotes the group of all automorphism of K trivial on k. In particular, if K is a Galois extension of k, $\mathrm{Gal}(K/k)$ denotes the Galois group of K over k. Let k be an algebraic number field, K an abelian extension of k and $\mathfrak{a}$ a fractional ideal of k. Then $\left[K/k, \mathfrak{a}\right]$ is the Artin symbol (c.f. [C], §1). If $\mathfrak{a}$ is principal, we abbreviate it as $\left[K/k, a\right]$.$(a \in k)$. Let k be a field. Then $\bar{k}$ denotes the algebraic closure of k in some universal domain. Some other standard notations and terminologies are used.

§1. Families of abelian varieties defined over $\mathbb{C}$.

Let L be a semi-simple algebra over $\mathbb{Q}$. Then we call a structure $Q = (A, C, \theta : t_1, \cdots, t_s)$, formed by a polarized abelian variety (A, C), an isomorphism of L into $\mathrm{End}(A) \otimes \mathbb{Q}$, and points $t_1, \cdots, t_s$ of A of finite order, a PEL-structure. In this section, we shall construct a family of PEL-structures and its moduli space, following the methods which is used in G. Shimura [10], [11] and [23]. The notations and the results of this section are used in the following sections.

1-1. A construction of a family of PEL-structures.

First we shall construct a families of PEL-structure. Let B be an indefinite division quaternion algebra over $\mathbb{Q}$, D its discriminant, O a maximal order of B. Let $B \ni x \longmapsto x' \in B$ be the canonical involution of B, and $B \ni x \longmapsto x^{\rho} = v^{-1}x'v \in B$ $(v \in B)$ a positive involution of B. Let $\Phi : B \longrightarrow M_2(\mathbb{R})$ be an irreducible representation. For any $\alpha \in B$, let $N(\alpha) = N_{B/\mathbb{Q}}(\alpha)$ be the reduced norm of α. Put

$$B^+ = \left\{ \alpha \in B \,\middle|\, N(\alpha) > 0 \right\}.$$

Then B^+ operates on $H = \left\{ z \in \mathbb{C} \,\middle|\, \mathrm{Im}\, z > 0 \right\}$ as

$$B^+ \ni \alpha : H \ni z \longrightarrow \frac{az + b}{cz + d} \in H,$$

where

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \Phi(\alpha) \in M_2(\mathbb{R}).$$

Now we shall fix a natural number N and a prime number p

with $(N, p) = 1$. Put

$$U(N) = \{\alpha \in B^+ \mid \alpha \text{ is prime to } N\},$$

$$\Gamma(N) = \{\alpha \in \mathfrak{O} \mid N(\alpha) = 1,\ \alpha \equiv 1 \bmod^{\times} N\mathfrak{O}\},$$

$$\Gamma(N, p) = \{\alpha \in \bigcup_{n=0}^{\infty} p^{-n}\mathfrak{O} \subset B \mid N(\alpha)=1, \alpha \equiv 1 \bmod^{\times} N\mathfrak{O}\},$$

where we write $\alpha \equiv 1 \bmod^{\times} N\mathfrak{O}$ if and only if $\alpha - 1 \in N\mathfrak{O}$. Then, $U(N)$, $\Gamma(N)$ and $\Gamma(N, p)$ operate on $\mathfrak{H}$ as subgroups of B^+. It is well-known that $\Gamma(N)$ is a discrete subgroup of $SL(2, \underset{\sim}{R})$ with a compact quotient. Moreover, if we fix an isomorphism $B \otimes_{\underset{\sim}{Q}} \underset{\sim}{Q}_p \cong M_2(\underset{\sim}{Q}_p)$, we may regard $\Gamma(N, p)$ as a discrete subgroup of $G_0 = SL(2, \underset{\sim}{R}) \times SL(2, \underset{\sim}{Q}_p)$ such that the quotient space $\Gamma(N,p)\backslash G_0$ is compact and the projection of $\Gamma(N, p)$ in each component of G_0 is dense. Therefore, $\Gamma(N, p)/\{\pm 1\}$ is an Ihara-group (c.f. [CMP], Chap. 4). This property of $\Gamma(N, p)$ is essentially used in §6. Let t be an element of B satisfying $N^{-1}\mathfrak{O} = \mathfrak{O} + \mathfrak{O}t$. Let $s_1 = 1, s_2, s_3, s_4$ be a base of $\mathfrak{O}$ over $\underset{\sim}{Z}$. Put $t_i = s_i t$ for $i = 1, 2, 3, 4$. Then $\mathfrak{O}t = \sum_{i=1}^{4} \underset{\sim}{Z} t_i$. Let c be some element of $\underset{\sim}{Q}$ satisfying $c \cdot \mathrm{Tr}\{v \cdot \mathfrak{O} \cdot (\mathfrak{O})'\} = \underset{\sim}{Z}$, where $\mathrm{Tr} = \mathrm{Tr}_{B/\underset{\sim}{Q}}$ denotes the reduced trace of B over $\underset{\sim}{Q}$. Now the set of data $\Omega = \Omega_{N,t} = (B, \mathfrak{O}, \rho;$

cv, $\mathcal{O}$; $t_1, \cdots, t_4$) makes a PEL-type in the sense of G. Shimura (cf. [C], p. 89). The following results show how we can make a family of PEL-structures of type Ω. They are obtained in [C], p. 89 and p. 90.

Proposition 1. *There is a real analytic map*

$$\mathcal{Y} : (\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}) \times \mathcal{H} \longrightarrow \mathbb{C}^2$$

which satisfies the following conditions.

① *For any fixed* x, $\mathcal{Y}(x, z)$ *is a holomorphic map from* $\mathcal{H}$ *to* $\mathbb{C}^2$.

② *For* $z \in \mathcal{H}$, *put* $\mathcal{Y}_z(x) = \mathcal{Y}(x, z)$. *Then* $\mathcal{Y}_z$ *is an* R*-linear isomorphism from* $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R}$ *to* $\mathbb{C}^2$ *and satisfies*

$$\mathcal{Y}_z(ax) = \Phi(a)\mathcal{Y}_z(x) \qquad (a \in B).$$

③ *For* $z \in \mathcal{H}$, *put* $\mathcal{E}_z(u, v) = \mathrm{Tr}(\mathcal{Y}_z^{-1}(u) \cdot \mathrm{cv}\, \mathcal{Y}_z^{-1}(u)^{\rho})$ $(u, v \in \mathbb{C}^2)$. *Then* $\mathcal{E}_z$ *defines a Riemann form on the complex torus* $\mathbb{C}^2/\mathcal{Y}_z(\mathcal{O})$.

④ *For* $\alpha \in B^+$ *and* $z \in \mathcal{H}$, *there is a* C*-linear automorphism* $\Lambda(\alpha, z)$ *of* $\mathbb{C}^2$ *satisfying*

$$\Lambda(\alpha, z)\mathcal{Y}(x, z) = \mathcal{Y}(x\alpha, \alpha^{-1}(z)).$$

The results of the above proposition show that we can construct a family of abelian varieties parametrized by $\mathcal{H}$ as follows.

For any $z \in \mathfrak{H}$, let $A_z = \mathbb{C}^2/\mathfrak{y}_z(O)$, C_z be the polarization of A_z which corresponds to the Riemann form E_z on A_z, θ_z the injection

$$B \ni a \longmapsto \theta_z(a) \in \mathrm{End}(A_z) \otimes \mathbb{Q},$$

where $\theta_z(a)$ is the element of $\mathrm{End}(A_z) \otimes \mathbb{Q}$ which is induced by $\Phi(a) \in \mathrm{End}_R(O \otimes R)$, $t_{i,z} = \mathfrak{y}_z(t_i)$. Put

$$Q_z = (A_z, C_z, \theta_z; t_{1,z}, \cdots, t_{4,z}).$$

Then $\Sigma(\Omega_{N,t}) = \{ Q_z \mid z \in \mathfrak{H} \}$ is so-called a family of PEL-structures parametrized by $\mathfrak{H}$. Here, we note that A_z, C_z and θ_z does neither depend on N nor on t. We can define the isogenies and the isomorphisms between PEL-structures Q_z ($z \in \mathfrak{H}$) in a natural way as in [C], p. 92. Then we have the following proposition.

Proposition 2. Every isogenies between Q_z ($z \in \mathfrak{H}$) are obtained from $\Lambda(\alpha, z) \in \mathrm{End}_{\mathbb{C}}(\mathbb{C}^2)$ ($\alpha \in B^+$) and every isomorphisms between Q_z ($z \in \mathfrak{H}$) are obtained from $\Lambda(\alpha, z) \in \mathrm{End}_{\mathbb{C}}(\mathbb{C}^2)$ ($\alpha \in \Gamma(N)$).

Proof. This proposition is a special case of Proposition 4.2 of [D], II, p. 135 and Proposition 4.4 of [D], II, p. 136. Q.E.D.

We know from this proposition that the isomorphism classes of

members of $\Sigma(\Omega_{N,t})$ are parametrized by $\Gamma(N)\backslash\mathfrak{H}$. Using this fact, G. Shimura has constructed a moduli space for the family $\Sigma(\Omega_{N,t})$ (c.f. 1-3).

1-2. Studies of the endomorphism rings.

From now on, we assume $N = 1$. Therefore we shall write as $\Sigma(\Omega_1) = \Sigma(\Omega_{1,t})$. Now we shall study the endomorphism rings of the members of $\Sigma(\Omega_1)$.

Proposition 3. *If* $z \in \mathfrak{H}$ *is not fixed by any* $\alpha \in B^+ - Q$, *then* $Q_z \in \Sigma(\Omega_1)$ *satisfies*

① $\mathrm{End}(Q_z) \cong Z$,

② $\mathrm{End}(A_z) \cong \mathfrak{O}$.

Proof. ① is clear from Proposition 2. About ②, the result of ① shows that the center of $\mathrm{End}(A_z) \cong Z$, therefore $\mathrm{End}(A_z) \otimes Q \cong B$ (since $\mathrm{End}(A_z) \otimes Q$ is a subalgebra of $M_2(C)$). Therefore $\mathrm{End}(A_z)$ is an order of B containing $\mathfrak{O}$. Since $\mathfrak{O}$ is a maximal order, consequently we have $\mathrm{End}(A_z) \cong \mathfrak{O}$. Q.E.D.

Let M be a quadratic field, $Z + Z\omega$ the ring of integers of M. Let $\mathfrak{r} = Z + Z(f\omega)$ ($f \in Z$) be an arbitrary order of M. Then we call f the *conductor* of the order $\mathfrak{r}$. Let $\mathfrak{a}$ be a Z-lattice in M. If $\mathfrak{a} \otimes Z_\ell = a_\ell \cdot \mathfrak{r} \otimes Z_\ell$ ($a_\ell \in M \otimes Z_\ell$) for all prime number ℓ, we call $\mathfrak{a}$ a *proper ideal* of $\mathfrak{r}$ or a

proper $\mathfrak{r}$-ideal (c.f. [S], §2). We call the group $\{$ proper ideals of $\mathfrak{r}\}/\{$principal ideals of $\mathfrak{r}\}$ the proper $\mathfrak{r}$-ideal class group. We call its order the class number of proper ideals of $\mathfrak{r}$ or the class number of proper $\mathfrak{r}$-ideals (c.f. [S], §2).

Proposition 4. Let $z \in \mathfrak{H}$ be a fixed point of some $\alpha \in B^+ - Q$. Then, there is an imaginary quadratic number field $M \subset C$ which is a splitting field of B, and a Q-linear isomorphism f from M to B satisfying the following conditions.

① $\Lambda : \mathfrak{o} \cap f(M) \longrightarrow \mathrm{End}(Q_z)$

defines an isomorphism.

② $\mathrm{End}(A_z) \otimes Q \cong M_2(M)$.

Moreover, if we put $\mathfrak{r}_z = f^{-1}(\mathfrak{o} \cap f(M)) \cong \mathrm{End}(Q_z)$, $\mathfrak{r}_z$ is an order of M whose conductor $\mathfrak{f}_z$ is prime to D(the discriminant of B). Moreover

③ there are just two Q-linear isomorphisms satisfying the above conditions, and one is equal to the composite of the other and the canonical involution of B. We can choose one of them in a canonical way and call it a normalized embedding and write it as f_z (c.f. [C], p. 68). Then we have

④ $f_{\alpha^{-1}(z)}(x) = \alpha^{-1} \cdot f_z(x) \cdot \alpha$ for any $\alpha \in B^+$ and $x \in M$.

For any imaginary quadratic number field $M \subset C$ which is

a splitting field of B and for any order $\mathfrak{r}$ of M whose conductor is prime to D, there is a non-trivial fixed point z of B^+ such that $\mathfrak{r}_z = \mathfrak{r}$. Moreover, the number of $\Gamma(1)$-equivalence classes of such non-trivial B^+-fixed points i.e. the number of the isomorphism classes of Q_z $(z \in \mathfrak{H})$ which satisfies $\mathrm{End}(Q_z) \cong \mathfrak{r}_z$ are equal to $2^s h(\mathfrak{r})$, where s denotes the number of prime numbers which are ramified in B but are not ramified in M, and $h(\mathfrak{r})$ denotes the class number of the proper ideals of $\mathfrak{r}$.

Proof. ① is clear from Proposition 2 and results of [C], §2. Since $\mathrm{End}(A_z) \otimes \mathbb{Q}$ contains $B \otimes M \cong M_2(M)$ and the comutant of B in $\mathrm{End}(A_z) \otimes \mathbb{Q}$ is equal to M, $\mathrm{End}(A_z) \otimes \mathbb{Q} \subset M_2(\mathbb{C})$ is equal to $M_2(M)$. About ③ or ④, in spite of the fact that $\mathfrak{r}$ is not necessarily the maximal order of M, we can prove just by the same methods as in [C], §2 (c.f. [C], 2.7, [C], Proposition 2.12 and [C], Proposition 2.17). Q.E.D.

These results i.e. Proposition 3 and Proposition 4 are used in §4 and §6.

1-3. A moduli space for $\Sigma(\Omega_{N,t})$. Now let N be an arbitrary natural number. Then G. Shimura has constructed a moduli space for the family $\Sigma(\Omega_{N,t})$ by descending the field of the rationality of $\Gamma(N)\backslash\mathfrak{H}$.

Proposition 5. *There is a projective non-singular curve* $V = V_N$ *defined over* $\mathbb{Q}(e^{\frac{2\pi i}{N}})$ *and a family of PEL-structures* $\{Q_w = (A_w, C_w, \Theta_w; t_{1w}, \cdots, t_{4w})\}$ *parametrized by the* $\mathbb{C}$*-rational points of* V *satisfying the following conditions.*

① *There is a holomorphic map*

$$\varphi : \mathfrak{H} \longrightarrow V$$

which induces a biregular isomorphism between $\Gamma(N)\backslash\mathfrak{H}$ *and* V.

② $Q_z \cong Q_{\varphi(z)}$ *for all* $z \in \mathfrak{H}$. *Therefore* $Q_w \not\cong Q_{w'}$ $(w, w' \in V)$ *if and only if* $w = w'$.

③ *If* w *is a* $\mathbb{C}$*-rational point of* V, *then* $\mathbb{Q}(e^{\frac{2\pi i}{N}}, w)$ *is equal to the field of moduli of* Q_w i.e. $Q_w^{\sigma} = Q_w$ *if and only if* $\sigma =$ *identity on* $\mathbb{Q}(e^{\frac{2\pi i}{N}}, w)$, *for any automorphism* σ *of* $\mathbb{C}$. *Moreover, if* $N \geqq 3$, $\Gamma(N)$ *is torsion free. Then we may assume that* Q_w *is defined over* $\mathbb{Q}(e^{\frac{2\pi i}{N}}, w)$, *and that, if we specialize* w *to another point* $w' \in V$, *then* Q_w *has no defect at this reduction of the field of rationality and is reduced to* $Q_{w'}$.

Proof. This proposition is a special case of [M], p. 324, Theorem 5.3 and [M], p. 329, Theorem 6.2. Q.E.D.

Remark. This proposition shows that we may regard the complete non-singular curve V as a *moduli space for the family* $\Sigma(\Omega_{N,t})$.

In § 5 and § 6, we construct such a moduli space in characteristic p.

Now we shall construct certain biregular morphisms between V^{σ} ($\sigma \in Gal(\mathbb{Q}(e^{\frac{2\pi i}{N}})/\mathbb{Q})$). They describe the reicplocity law of certain class fields (c.f. 1-4).

Let α be an element of B^{+} which is prime to N i.e. $\alpha \in U(N)$. Then there is $\beta \in O$ such that $\beta \equiv \alpha \bmod^{\times} NO$ (for the notation $\bmod^{\times} NO$, c.f. [S], § 2). Put $t' = t\beta$, then $N^{-1}O = O + Ot'$ and $t\alpha \equiv t' \bmod^{\times} O \otimes \mathbb{Z}_{\ell}$ for all prime number $\ell \mid N$. Then we put $\Omega_{N,t\alpha} = \Omega_{N,t'}$. We can construct a family of PEL-structures as before from these data. Then Proposition 1, 2 hold with the same y, Λ as in the case of $\Omega_{N,t}$. Therefore, $\Sigma(\Omega_{N,t\alpha}) = \{ Q_z = (A_z, C_z, \theta_z ; t_{1,z\alpha}, \cdots, t_{4,z\alpha}) \}_{z \in \mathfrak{H}}$, where A_z, C_z, θ_z are the same as in the case of $\Omega_{N,t}$ and $t_{i,z\alpha} = y(t_i\alpha, z)$. Moreover, Proposition 5 hold with the same V and φ as in the case of $\Omega_{N,t}$ (c.f. [C], p. 133 p. 134). Now we have the following proposition.

Proposition 6. Let α, $\Omega_{N,t\alpha}$, etc. be as above. Put $\sigma = [\mathbb{Q}(e^{\frac{2\pi i}{N}})/\mathbb{Q}, N(\alpha)]$. Then there is a biregular morphism

$$R_{\sigma}(\alpha) : V \longrightarrow V^{\sigma}$$

defined over $Q(e^{\frac{2\pi i}{N}})$. It satisfies the following condition.

Let τ be an automorphism of C whose restriction to $Q(e^{\frac{2\pi i}{N}})$ is equal to σ. Then

$$\varphi(z)^{\tau} = R_{\sigma}(\alpha) \quad [\varphi(z')] \qquad (z,\ z \in H)$$

if and only if

$$Q_z^{\tau} \cong Q_{z'} \ .$$

Proof. See [C], p. 134. Q.E.D.

Remark. Let notation be as in Proposition 6. Let $\tau \in \mathrm{Aut}(C)$ whose restriction to $Q(e^{\frac{2\pi i}{N}})$ is equal to σ. Then $\Sigma(\Omega_{N,t})^{\tau}$ $= \Sigma(\Omega_{N,t\alpha})$ (as a set of PEL-structures). By the way, $\Sigma(\Omega_{N,t})^{\tau}$ and $\Sigma(\Omega_{N,t\alpha})$ have V^{σ} and V as their moduli space. This proposition shows the relation between these two moduli spaces for the family $\Sigma(\Omega_{N,t})^{\tau} = \Sigma(\Omega_{N,t\alpha})$.

1-4. The canonical model of the arithmetic quotient $\Gamma(N)\backslash H$. Let $M \subset C$ be an imaginary quadratic number field, r an order of M, r_0 the maximal order of M and $f \in Z$ the conductor of r. Let a be any fractional r_0-ideal prime to f. Then $[a] = [a]_r = \bigcap_{p:\text{prime}} (a \otimes Z_{(p)} \cap M)$ defines a proper ideal of

$\mathfrak{r}$ (c.f., [S], p. 510). Moreover, if $\mathfrak{a}$ is an integral $\mathfrak{r}_0$-ideal prime to $\mathfrak{f}$, $[\mathfrak{a}]_{\mathfrak{r}} = \mathfrak{a} \cap \mathfrak{r}$. Let $I(N, \mathfrak{r})$ be the set of all the fractional ideal $\mathfrak{a}$ of M which is prime to $N\mathfrak{f}$ and which satisfies $[\mathfrak{a}]_{\mathfrak{r}} = v\mathfrak{r}$, $v \in M$, $v \equiv 1 \mod^{\times} N\mathfrak{r}$. Then $I(N, \mathfrak{r})$ form a ideal group of M (c.f. [S], p. 510). Let $C(N, \mathfrak{r})$ be the corresponding class field over M. With these notations, we can summarize the main results in [C] and [S] about the canonical model of the arithmetic quotient $\Gamma(N)\backslash H$.

Theorem C. Let N, V, φ, $R_\sigma(\alpha)$ be as before. Then the following conditions are satisfied.

① $R_\sigma(\alpha) = R_\sigma(\beta)$ if $\alpha \equiv \beta \mod^{\times} N\mathfrak{o}$.

② $R_\tau(\beta)^\sigma \circ R_\sigma(\alpha) = R_{\tau\sigma}(\beta\alpha)$.

③ $R_1(\gamma)[\varphi(z)] = \varphi(\gamma(z))$ if $\gamma \in \Gamma(N)$ and $z \in H$.

④ Let z be a non-trivial B^+-fixed point i.e. a fixed point of $B^+ - \mathbb{Q}$. Let M_z, $\mathfrak{r}_z$ f_z be as in Proposition 4. Let $C(N, \mathfrak{r}_z)$ be as above. Then the following conditions are satisfied.

ⓐ $M(e^{\frac{2\pi i}{N}}, \varphi(z)) = C(N, \mathfrak{r}_z)$,

ⓑ Let $\mathfrak{a}$ be a fractional ideal of M prime to $N\mathfrak{f}_z$. Then

there is $\alpha \in U(N)$ satisfying $O\alpha^{-1} = Of_z([a]_{r_z}^{-1})$.

Let $\tau = [C(N, r_z)/M, a]$, then

$$\varphi(z)^{\tau} = R_{\sigma}(\alpha)\,[\varphi(\alpha^{-1}(z)) \quad .$$

Remark. One of the main objects of this paper is to generalize this theorem for the case of arbitrary characteristic (c.f. § 7, Main Theorem 1).

Remark. This theorem can be proved by studying the special members of $\Sigma(\Omega_{N,t})$ and $\Sigma(\Omega_{N,t\alpha})$ (c.f. [C], § 9). But, in view of Proposition 5, we can regard that this theorem describes some arithmetic properties of the special members of $\Sigma(\Omega_{N,t})$ and $\Sigma(\Omega_{N,t\alpha})$. For example, let M_z, r_z, a, α, τ be as in Theorem C - ④. Then $Q_z^{\nu} = Q_{\alpha^{-1}(z)\cdot\alpha}$ holds true for any $\nu \in$ Aut(C) whose restriction on $C(N, r_z)$ coincides with τ. In particular $\mathrm{End}(A_z, \theta_z) \cong \mathrm{End}(A_{\alpha^{-1}(z)}, \theta_{\alpha^{-1}(z)})$.

§ 2. ℓ-ardic representations.

In this section, we shall study the Tate module $T_\ell(A_z)$ of $Q_z = (A_z, C_z, \theta_z) \in \Sigma(\Omega_1)$ and show that every homomorphism between A_z, $A_{z'}$ $(z, z' \in H)$ which preserves the operations of O also preserves the polarizations C_z, $C_{z'}$. All the results of this section are used only to prove Theorem 1 of § 3 and Theorem 2 and Theorem 3 of § 4. Therefore any reader who has no interest in the proof of them may skip this section.

Let A be a 2-dimensional abelian variety defined over a field k, ℓ a prime number which is prime to the characteristic of k. Let $T_\ell(A) = \varprojlim A_{\ell^n}$ be the Tate module of A. We assume that there is a monomorphism

$$\theta : O \longrightarrow \mathrm{End}(A),$$

where O is the maximal order of the indefinite division quaternion algebra B over Q and θ maps 1_O to 1_A. Then θ induces $\theta_\ell : O \otimes Z_\ell \longrightarrow \mathrm{End}(A) \otimes Z_\ell \subseteq \mathrm{End}(T_\ell(A))$ and $\theta_\ell : O \otimes Q_\ell \longrightarrow \mathrm{End}(T_\ell(A) \otimes Q_\ell)$. Since $O \otimes Q_\ell$ is a quaternion algebra over Q_ℓ and $T_\ell(A) \otimes Q_\ell$ is a 4-dimensional vector space over Q, the left $O \otimes Q_\ell$-module $T_\ell(A) \otimes Q_\ell$ is isomorphic to the left $O \otimes Q_\ell$-module $O \otimes Q_\ell$. Now, since $T_\ell(A)$ is a Z_ℓ-submodule of finite type of $T_\ell(A) \otimes Q$, we may regard $T_\ell(A)$ as a

Z_ℓ-lattice of $O \otimes Q_\ell$. Moreover θ_ℓ makes $O \otimes Z_\ell$ operate on $T_\ell(A)$. Therefore, since $O \otimes Z_\ell$ is a maximal order of $O \otimes Q_\ell$ whose class number is one, $T_\ell(A)$ is isomorphic to $O \otimes Z_\ell$ as left $O \otimes Z_\ell$-module.

Now, let $Q_z = (A_z, C_z, \theta_z ; t_{1,z}, \cdots, t_{4,z})$ $(z \in H)$ be as in Section 1. Then our above considerations can apply and therefore $T_\ell(A_z) \cong O \otimes_Z Z_\ell$ as left $O \otimes Z_\ell$-module. Moreover, since $\mathrm{Aut}_{O \otimes Z_\ell}(O \otimes Z_\ell) \cong (O \otimes Z_\ell)^\times$, we may assume that O operates on $T_\ell(A_z) \cong O \otimes Z_\ell$ by the operation of $\Lambda(\alpha, z)$ $(\alpha \in O)$ as the right multiplication of α.

Let $\hat{A}_z$ be the dual of A_z. Then θ determines an injective anti-homomorphism ${}^t\theta : O \longrightarrow \mathrm{End}(\hat{A}_z)$ with $\theta(\ |_O) = \ |_{\hat{A}_z}$. Therefore the above considerations show that we may assume that $T_\ell(\hat{A}_z) \cong O' \otimes Z_\ell$, where the operation of $\alpha \in O$ on $T_\ell(\hat{A}_z)$ by ${}^t\theta$ corresponds to the right multiplication of α' on $O' \otimes Z_\ell$ and the operation of $\alpha \in O$ on $T_\ell(\hat{A}_z)$ by ${}^t\Lambda(\alpha, z)$ corresponds to the left multiplication of α' on $O' \otimes Z_\ell$.

Now we shall study the isogeny $\varphi_X : A_z \longrightarrow \hat{A}_z$ $(X \in C)$, using the above canonical basis of ℓ-adic representations. Let P be the map $O \otimes Z_\ell = M_2(Z_\ell) \longrightarrow O' \otimes Z_\ell \cong M_2(Z_\ell)$ which represents φ_X. Then, since $\theta_z(v^{-1}\alpha' v) = \varphi_X^{-1} \circ {}^t\theta(\alpha) \circ \varphi_X$

$(\alpha \in O)$, we have $v^{-1}\alpha' v = P^{-1} \circ \alpha' \circ P$ $(\alpha \in O)$. Therefore $(P \circ v^{-1}) \circ \alpha' = \alpha' \circ (P \circ v^{-1})$. Therefore $\gamma \circ P \circ v^{-1}$: $O \otimes Q_\ell \longrightarrow O \otimes Q_\ell$ commutes with the left multiplications of any $\alpha \in B$, where γ denotes the canonical involution of $O \otimes_Q Q_\ell$.

Now let z be a generic point of $\Gamma \backslash H$ over Q. Then Proposition 3 of § 1 show that $\gamma \circ P \circ v^{-1}$ can be represented by a composition of two maps $O \otimes Z_\ell \ni x \longmapsto cx \in O \otimes Z_\ell$ $(c \in Q)$, since $\mathrm{End}(A_z, C_z, \theta_z) \otimes_Z Q \cong Q$. Therefore $\gamma \circ P$ can be represented by the left multiplication of cv, where $c \in Q$, v is an element of B which corresponds to the positive involution induced by φ_X.

Now let z' be any point of H or $\Gamma \backslash H$. Then we may assume $Q_{z'}$ is a reduction of Q_z. Then two isomorphisms $T_\ell(A_z) \tilde{=} O \otimes Z_\ell$ (as left $O \otimes Z_\ell$-module) and $T_\ell(\hat{A}_z) \tilde{=} O' \otimes Z_\ell$ (as right $O' \otimes Z_\ell$-module) reduce to $T_\ell(A_{z'}) \tilde{=} O \otimes Z_\ell$ (as left $O \otimes Z_\ell$-module) and $T_\ell(\hat{A}_z) \tilde{=} O \otimes Z_\ell$ (as right $O' \otimes Z_\ell$-module) respectively. Therefore, since $\varphi_{X'}$ $(X' \in C_{z'})$ can be taken as a reduction of φ_X $(X \in C_z)$, we see that $\varphi_{X'}$ can be represented by the composition of the left multiplication of cv and the canonical involution of $O \otimes Z_\ell$ if we use above basis of ℓ-adic representations. Therefore, all the homomorphisms between Q_z $(z \in H)$

which commute with the operations of O preserve the polarization.

Proposition 7. Let $Q = (A, C, \theta ; t_1, \cdots, t_4)$, $Q' = (A', C', \theta', t_1', \cdots, t_4')$ be two elements of $\Sigma(\Omega_{N,t})$ or some good reductions of two elements of $\Sigma(\Omega_{N,t})$ (the characteristic of the residue field may be either 0 or p). Then

① The Tate module $T_\ell(A)$ is isomorphic to $O \otimes_Z Z_\ell$ as left $O \otimes Z_\ell$ - module, where $O \otimes Z_\ell$ operates on $T_\ell(A)$ by θ,

② any homomorphisms between A and A' which commute with the operations of O preserve the polarizations.

Proof. If $Q_z \in \Sigma(\Omega_{N,t})$, we have already proved out theorem. Moreover, even in the case that Q_z is some reduction, we can prove in a quite similar way as the first case. Q.E.D.

§ 3. Good reduction of abelian varieties.

In this section, we shall show that every PEL-structure defined over $\bar{\mathbb{Q}}$, which was ~~defined~~ constructed in § 1, have good reduction at any place of $\bar{\mathbb{Q}}$. This result will be obtained by applying the criterion for good reduction of abelian varieties, which is due to Serre-Tate. The facts that ① $T_\ell(A) \otimes \mathbb{Q}_\ell \cong B_\ell$ (as left B_ℓ-module) and ② there is a prime number ℓ such that B_ℓ is division algebra and $(\ell, p) = 1$ are critical to obtain our result. This result will be used to show that our moduli space is proper reduced scheme over $\bar{\mathbb{F}}_p$ in § 6.

3-1. Main Lemma about ℓ-ardic representations. The main result of this section is based upon the following lemma.

Lemma 1.(Main Lemma). Let k be a $\mathfrak{p}$-adic number field, $\mathbb{Q}_\ell$ the ℓ-adic number field. We assume that the prime number ℓ is not divided by $\mathfrak{p}$. Let $\mathfrak{O}_\ell$ be the unique maximal order of the unique division quaternion algebra over $\mathbb{Q}_\ell$, $G = \mathrm{Gal}(\bar{k}/k)$ the Galois group of $\bar{k}/k$, T the inertia group. Then, for any continuous homomorphism

$$\rho : G \longrightarrow \mathfrak{O}_\ell^\times ,$$

$\rho(T)$ is a finite group.

Proof. We need two sublemmas to prove this lemma.

Sublemma 1. Let H be any pro-p-group. Then H does not contain any pro-ℓ-group $\neq \{1\}$, where we assume p and ℓ are mutually prime.

Proof of sublemma. Easy. Q.E.D.

Now let V be the subgroup of G which corresponds to the maximal tamely ramified extension of k. We see easily that V is a normal subgroup of G.

Sublemma 2 (A result about the local Galois group which is due to K. Iwasawa). G/V contains a dense subgroup H satisfying the following conditions.

① H is a group generated by α and β with the fundamental relation $\alpha\beta\alpha^{-1} = \beta^{q}$, where $q = N\mathfrak{p}$.

② β generates a dense subgroup of T/V.

③ α is a Frobenius element.

Proof. See K. Iwasawa, [5], p. 463, Theorem 2. Q.E.D.

Now we shall start the proof of our Main Lemma.

For any natural number n, put $\mathfrak{o}_n = \{a \in \mathfrak{o} \mid a \equiv 1 \mod \ell^n\mathfrak{o}\}$.

Then, we have a series of normal subgroups;

$$\mathfrak{o}^{\times} \rhd \mathfrak{o}_1 \rhd \cdots \rhd \mathfrak{o}_n \rhd \mathfrak{o}_{n+1} \rhd \cdots.$$

Here $\mathfrak{o}^{\times}/\mathfrak{o}_1 \cong F_{\ell^2}^{\times}$ (the multiplicative group of the finite field

with ℓ^2 elements), $O_n/O_{n+1} \cong O/\ell O \cong F_{\ell^2}$ (the additive group of the finite field with ℓ^2 elements) and $\bigcap_{n=1}^{\infty} O_n = \{1\}$ hold. Put $T_1 = \{t \in T \mid \rho(T) \in O_1\}$. Then T_1 is a normal subgroup of T. Moreover, since $O^\times/O_1$ is a finite group, $\rho(T)/\rho(T_1)$ is also a finite group. Therefore we have only to prove that $\rho(T_1)$ is a finite group. By the way, since O_1 is a pro-ℓ-group, the pro-p-group $\rho(T_1 \cap V)$ meets with O_1 only at $\{1\}$. Therefore ρ induces a continuous homomorphism from $T/T_1 \cap V$ to O_1.

Now we shall use the notations in the above sublemma. Since $\rho(T)/\rho(T_1)$ is a finite group, we can take a large natural number m so that $\rho(\alpha^m) = \xi$ and $\rho(\beta^m) = \eta$ belong to $\rho(T_1)$. Then we have $\xi\eta\xi^{-1} = \eta^{mq}$. Therefore η and η^{mq} belong to the same quadratic subfield $Q_\ell(\eta)$ of $O \otimes Q_\ell$, and are conjugate over Q_ℓ. Therefore $\eta = \eta^{mq}$ or $\eta \cdot \eta^{mq} = N(\eta) = N(\xi\eta\xi^{-1}) = N(\eta)^{mq}$ holds. Therefore $\eta^{(mq)^2-1} = 1$. Therefore $\rho(\beta^m) = \eta$ generates a finite subgroup of $O^\times$. Since β generates a dense subgroup of $T_1/T_1 \cap V$, the topological closure of the group generated by β^m is a subgroup of finite index of $T_1/T_1 \cap V$. Therefore the topological closure of the group generated

by $\rho(\beta^m) = \eta$, which is a finite group, is a subgroup of finite index of $\rho(T_1) = \rho(T_1/T_1 \cap V)$. Consequently $\rho(T_1)$ is a finite group. Q.E.D.

3-2. Good reduction of abelian varieties.

Lemma 2 (A riterion for good reduction of abelian varieties, due to Serre-Tate). Let k be a field, v a discrete valuation of k, $\tilde{k}$ the residue field of v. Let A be an abelian variety defined over k, l a prime number, $T_l(A)$ the Tate module of A. We assume that $\tilde{k}$ is perfect and the characteristic of $\tilde{k}$ is prime to l. Let k_s be the separable closure of k, $\mathrm{Gal}(k_s/k)$ the Galois group of k_s/k, T the inertia group of v. Let

$$\rho : \mathrm{Gal}(k_s/k) \longrightarrow \mathrm{End}(T_l(A))$$

be the continuous homomorphism induced by the natural action of $\mathrm{Gal}(k_s/k)$ on $T_l(A)$. Then A has good reduction at v if and only if $\rho(T)$ is a finite group.

Proof. See J. P. Serre and J. Tate, [15], p. 493, Theorem 1. Q.E.D.

Now we can obtain the main result of this section. It depends only on § 2, Proposition 7, ①, § 3 Lemma 1 and § 3 Lemma 2.

Theorem 1. Let $Q_z = (A_z, C_z, \theta_z; t_{1,z}, \cdots, t_{4,z})$ be any element of $\Sigma(\Omega_{N,t})$. We assume that Q_z is defined over a p-adic number field k and that p does not divide N. Then, there is a finite algebraic extension k' of k and a PEL-structure Q' defined over k' such that

① Q' is isomorphic to Q_z over k',

② Q' has good reduction at the discrete place p' which is the extension of p to k'.

Proof. Let ℓ be a prime number which divides D and which is prime to p. Let $T_\ell(A_z)$ is the Tate module of A_z. Then $T_\ell(A_z) \cong O \otimes_Z Z_\ell$ and $\theta_z(O)$ operates on $T_\ell(A_z)$ as the left multiplication. Therefore, any element of $\mathrm{End}_{Z_\ell}(T_\ell(A_z))$ which commutes with the operation of $\theta_z(O)$ is represented as the right multiplication of an element of O. Now, $\mathrm{Gal}(\bar{k}/k)$ operates on $T_\ell(A_z)$ as Z_ℓ-linear endomorphisms. Moreover, since any element of $\theta_z(O)$ is defined over k, the operation of $\mathrm{Gal}(\bar{k}/k)$ commutes with the operations of $\theta_z(O)$. Therefore, we have a homomorphism $\rho: \mathrm{Gal}(\bar{k}/k) \longrightarrow (O \otimes_Z Z_\ell)^\times$, where $g \in \mathrm{Gal}(\bar{k}/k)$ operates on $T_\ell(A_z) \cong O \otimes Z_\ell$ as the right multiplication of $\rho(g) \in O \otimes Z_\ell$. Moreover we see that above homomorphism is continuous.

Therefore, by Lemma 1, ρ maps the inertia group of $\mathfrak{p}$ onto a finite subgroup I of $(O \otimes Z_\ell)^\times$. Since $\rho(\mathrm{Gal}(\bar{k}/k))$ is a pro-finite group, we can take a open subgroup H of $G(\bar{k}/k)$ which meets with the inertia group of $\mathfrak{p}$ only at a subset of $\rho^{-1}(1)$. Let k' be the subfield of $\bar{k}/k$ which corresponds to $H \subset \mathrm{Gal}(\bar{k}/k)$. Then, the underlying abelian variety of the PEL-structure has good reduction at $\mathfrak{p}'$ (the extension of $\mathfrak{p}$ to k). Since the level is prime to $\mathfrak{p}$, the PEL-structure has good reduction at $\mathfrak{p}'$ (c.f. [S&T], p. 94, Proposition 12 and P. 98, Proposition 16). Q.E.D.

Remark. Let ℓ be a prime number, $\mathfrak{g} = \mathrm{GL}(n, Z_\ell)$. Put $\mathfrak{g}_\ell = \left\{ g \in \mathfrak{g} \;\middle|\; g \equiv 1 \begin{cases} \bmod \ell & \text{if } \ell \neq 2 \\ \bmod 4 & \text{if } \ell = 2 \end{cases} \right\}$. Then we see $\mathfrak{g}_\ell$, is torsion free. Therefore, if N is no less than 3, Q_z has good reduction over any $\mathfrak{p}$-adic fields over which it is defined. Moreover, since the automorphism group of the polarized abelian variety is a finite group, $P_z = (A_z, C_z; t_{1z}, \cdots, t_{4z})$ has no automorphisms. This fact will be used in §5.

§4. A classification of some kind of PEL-structures defined over finite fields.

In this section, we shall classify PEL-structures defined over finite fields which are obtained as reductions of some PEL-structures $(Q_z \in \Sigma(\Omega_1)$ defined over $\bar{Q}$. It is a generalization of the main results of M. Deuring [1], in which $\Sigma(\Omega_1)$ is the family of elliptic curves (we do not use the assumption $B \neq M_2(Q)$ in this section). Moreover, the method to obtain our results is almost the same as it of M. Deuring [1]. The results of this section is due to G. Shimura (he has informed me of these results by a letter). All the results of this section are used only to prove Theorem 5 of §6.

Let D be the discriminant of the indefinite quaternion algebra B over Q, p a prime number not dividing D, (P) an extension of p to a place of $\bar{Q}$. Let Q_z be an element of $\Sigma(\Omega_1)$ whose field of moduli is contained in $\bar{Q}$. Then we see Q_z can be defined over $\bar{Q}$ (c.f. e.g. [M], p. 324, Theorem 5.3). Therefore, we may say reduction modulo (P) of Q_z, etc. Note that the above condition is satisfied if z is a non- trivial fixed point of B^+ (c.f. Proposition 5 and Theorem C). Moreover, Theorem 1 of the

last section shows that Q_z has good reduction at $\mathfrak{P}$. Therefore we have PEL-structures

$$\tilde{Q}_z = (\tilde{A}_z, \tilde{C}_z, \tilde{\theta}_z) = (A_z \bmod \mathfrak{P}, C_z \bmod \mathfrak{P}, \theta_z \bmod \mathfrak{P})$$

defined over finite fields. In this section we shall classify the set of the $\bar{F}_p$-isomorphism classes of all the PEL-structures $\tilde{Q}_z$ which can be obtained as above.

Remark. If $B = M_2(\mathbb{Q})$, $Q_z/\bar{\mathbb{Q}}$ does not necessarily have good reduction. But, even in this case, if z is a non-trivial fixed point of B, it is O.K. (c.f. [15], p. 497, Corollary 1).

Remark. We need only to classify $\bar{F}_p$-isomorphism classes of the structure $(\tilde{A}_z, \tilde{\theta}_z)$ in view of Proposition 7 of § 2.

Remark. Let A, A' be ablian varieties defined over a finite field k. Then $\mathbb{Z}_\ell \otimes \mathrm{Hom}_k(A, A') \longrightarrow \mathrm{Hom}_{\mathrm{Gal}(\bar{k}/k)}(T_\ell(A), T_\ell(A'))$ is bijective. This is the Main Theorem of [E]. We shall use this theorem and its corollaries in 4-2 and 4-3 to classify PEL-structures of the above type.

4-1. Representations of endomorphism rings at tangent spaces of abelian varieties.

Now we shall study the representation δ of $\tilde{\theta}_z(O) \subset \mathrm{End}_k(A)$

on the tangent space $\tilde{D}_z$ of $\tilde{A}_z$. First we see that $p\tilde{\theta}_z(0) = \tilde{\theta}_z(p0)$ is mapped to 0 since $\delta(p 1_{\tilde{A}}) = p\delta(1_{\tilde{A}}) = 0$. Therefore, δ induces a homomorphism $0/p0 \cong \tilde{\theta}_z(0)/\tilde{\theta}_z(p0) \longrightarrow \mathrm{End}_{\tilde{F}_p}(\tilde{D}_z)$. By the way, since p is prime to D, $0/p0$ is isomorphic to $M_2(\tilde{F}_p)$. Moreover it is clear that $\delta(\tilde{\theta}(1_0)) = \delta(1_{\tilde{A}}) = 1_{\tilde{D}_z}$. Therefore $\delta\cdot\tilde{\theta}$ is equivalent to $0 \ni a \longmapsto a \bmod p0 \in 0/p0 \cong M_2(\tilde{F}_p)$ (note the fact that $\mathrm{End}_{\tilde{F}_p}(\tilde{D}_z) \cong M_2(\Omega)$, where Ω is the universal domain of characteristic p).

Proposition 8. *Let $\tilde{Q}_z$ be as before. Let δ be the representation of the endomorphism ring $\mathrm{End}_k(\tilde{A}_z)$ at the tangent $\tilde{D}_z \cong \Omega^2$ of $\tilde{A}_z$. Then the representation $\delta\cdot\tilde{\theta}_z : 0 \longrightarrow \mathrm{End}(\tilde{D}_z)$ is equivalent to $0 \ni a \longmapsto a \bmod p0 \in 0/p0 \cong M_2(\tilde{F}_p)$.*

From now on, we shall fix an isomorphism $0/p0 \cong M_2(\tilde{F}_p)$. We call a base of $\tilde{D}_z$ as a *canonical base* if $(\delta\circ\tilde{\theta}_z)(a)$ $(a \subset 0)$ is represented by this base as the left multiplication of $a \bmod p0$ on $0/p0 \cong M_2(\tilde{F}_p)$.

Corollary 1. *Let $\tilde{Q}_z$, $\tilde{Q}_{z'}$ be as before. Let δ be the representation of $\mathrm{Hom}(\tilde{A}_z, \tilde{A}_{z'})$ by the canonical bases of $\tilde{A}_z$ and $\tilde{A}_{z'}$. Then any element f of $\mathrm{Hom}(\tilde{A}_z, \tilde{A}_{z'})$ which preserves*

the operations of $\mathfrak{O}$ i.e. $f \circ \theta_z(a) = \theta_z(a) \circ f$ $(a \in \mathfrak{O})$ is represented by a scalar matrix.

Proof. Clear from Proposition 8. Q.E.D.

Corollary 2. Let $\tilde{Q}_z$, $\tilde{Q}_{z'}$, δ and f be as in Corollary 1. If f is not a separable isogeny, then $\delta f = 0$. Therefore, f is a compose of the Frobenius homomorphism from $\tilde{A}_z$ to $\tilde{A}_z^p$ and a homomorphism from $\tilde{A}_z^p$ to $\tilde{A}_{z'}$ which commutes with the operations $\tilde{\theta}_z^p(a)$ and $\tilde{\theta}_{z'}(a)$ $(a \in \mathfrak{O})$.

Proof. The first part is clear. For the second part (Therefore, f is ····), it is a corollary of [S & T], p. 16, Proposition 6. Q.E.D.

4-2. Super-singular cases. Now let $\tilde{Q}_z = (\tilde{A}_z, \tilde{C}_z, \tilde{\theta}_z)$ be as in 4-1. We assume that $\tilde{Q}_z$ is defined over the finite field F_q with q elements. Let π be the Frobenius automorphism of F_q. Then π induces an endomorphism of $\tilde{A}_z$. Clearly, only two cases may occur; ① some power of π belongs to $\mathfrak{O}$ (super-singular case), or ② no power of π belongs to $\mathfrak{O}$ (singular case).

Remark. We shall later see that $\tilde{Q}_z$ is super-singular if

and only if $\tilde{A}_z$ has no points of order p and that $\tilde{Q}_z$ is singular if and only if $\tilde{A}_z$ has just $p^2 - 1$ points of order p.

In the first case, we can take the field of the definition for $\tilde{Q}_z$ so large that $\pi = q^{\frac{1}{2}} \in \mathbb{Q}$.

Theorem 2 (A classification of super-singular PEL-structures). Assume some power of π belongs to $\mathbb{Q}$. Then $\tilde{A}_z$ is isogenous to a square E^2 of a super-singular elliptic curve E. Therefore $\mathrm{End}(\tilde{A}_z)\otimes_{\mathbb{Z}}\mathbb{Q} = \mathrm{End}(\tilde{A}_z)\otimes_{\mathbb{Z}}\mathbb{Q} \cong M_2(S)$, where S is the definite quaternion algebra over $\mathbb{Q}$ which ramifies only at p and the infinite place. Therefore the commutant of $\tilde{\theta}_z(B)$ in $\mathrm{End}(\tilde{A}_z)\otimes\mathbb{Q} \cong M_2(S)$ is isomorphic to the definite quaternion algebra G over $\mathbb{Q}$ which ramifies at finite places dividing pD and at the infinite place. Moreover, the commutant of $\tilde{\theta}_z(O)$ in $\mathrm{End}(\tilde{A}_z)$ is a maximal order $\mathfrak{o}$ of the quaternion algebra G. Still more, the number of the isomorphism classes of such $\tilde{Q}_z$ is equal to the class number of $\mathfrak{o}$, and the set of such $\tilde{Q}_z$ modulo isomorphisms is equal to the set of some $\mathfrak{a}$-transforms of a fixed such $\tilde{Q}_z$, where $\mathfrak{a}$ runs over a representative of the left ideal classes of $\mathfrak{o}$.

Proof. Take F_q so large as $\pi = q^{\frac{1}{2}} \in \mathbb{Q}$. Then, $\tilde{A}_z$ is isogenous

to a square of a super-singular elliptic curve by [E], Theorem 2. Therefore $\mathrm{End}(\tilde{A}_z) \otimes \mathbb{Q} \cong M_2(S)$. Therefore the commutant of $\tilde{\theta}_2(B) \cong B$ in $M_2(S)$ is the indefinite quaternion algebra G over $\mathbb{Q}$ which ramifies at pD and the infinite place. Now we shall show that the commutant of $\tilde{\theta}_z(0) \cong \mathcal{O}$ in $\mathrm{End}(\tilde{A}_z)$ is its maximal order.

Lemma 3. *A_0, A_1 be 2-dimensional abelian varieties over $\mathbb{F}_q$ which have an injective homomorphisms $\theta_i : \mathcal{O} \longrightarrow \mathrm{End}_{\mathbb{F}_q}(A_i)$ with $\theta_i(1_{\mathcal{O}}) = 1_{A_i}$ $(i = 1, 2)$. We assume their Frobenius endomorphisms π_i over $\mathbb{F}_q$ is equal to $q^{\frac{1}{2}} \in \mathbb{Q}$. Moreover we assume that the commutant of $\theta_0(\mathcal{O})$ in $\mathrm{End}(A_0)$ is a maximal order $\mathfrak{o}$ (c.f. above). Let $f : A_0 \longrightarrow A_1$ be any homomorphism which commutes with the operations of $\mathcal{O}$ by θ_i $(i = 1, 2)$. Then there is a left ideal $\mathfrak{a}$ of $\mathfrak{o}$ and an $\mathfrak{a}$-multiplication $\lambda : A_0 \longrightarrow A_{0,\mathfrak{a}}$, such that f is a compose of λ and an isomorphism from $A_{0,\mathfrak{a}}$ to A_1 which preserves the operations of $\mathcal{O}$. In particular, the commutant of $\theta_1(\mathcal{O})$ in $\mathrm{End}(A_1)$ is also a maximal order.*

Remark. Let $\mathfrak{a}$ be a left ideal of $\mathfrak{o}$ and $\lambda : A_0 \longrightarrow A_{0,\mathfrak{a}}$ be an $\mathfrak{a}$-multiplication as above. Then there is an injective homomorphism $\theta_{0,\mathfrak{a}} : \mathcal{O} \longrightarrow \mathrm{End}(A_{0,\mathfrak{a}})$ with $\theta_{0,\mathfrak{a}}(1_{\mathcal{O}}) = 1_{A_{0,\mathfrak{a}}}$,

since $\mathcal{O}$ and $\mathfrak{o}$ commute. Moreover we may take $\theta_{0,\mathfrak{a}}$ so that λ is a homomorphism from (A_0, θ_0) to $(A_{0,\mathfrak{a}}, \theta_{0,\mathfrak{a}})$ i.e. $\lambda \circ \theta_0(a) = \theta_{0,\mathfrak{a}}(a) \circ \lambda$ $(a \in \mathfrak{o})$. This statement can be proved easily from the construction of the $\mathfrak{a}$-multiplication (c.f. [S & T], p. 53, Proposition 7).

Proof of Lemma 3. Let $p\mathfrak{o} = \mathfrak{p}^2$. Then the results of 4 - 1 show that the representaion of $\mathfrak{o}$ at the tangent space of A_0 is equivalent to

$$\mathfrak{o} \ni \alpha \longmapsto \begin{pmatrix} \alpha \bmod \mathfrak{p} & 0 \\ 0 & \alpha \bmod \mathfrak{p} \end{pmatrix} \in \mathfrak{o}/\mathfrak{p} \cong F_{p^2}.$$

Therefore the Frobenius tranform A_0^p of A_0 is isomorphic to $A_{0,\mathfrak{p}}$. Therefore, Corollary 2 of Proposition 8 shows that f is a compose of the $\mathfrak{p}^n$-transform and a separable isogeny. Therefore we may assume that f is a separable isogeny.

Since $p\mathfrak{o} = \mathfrak{p}^2$, A_0 has no point of order p. Let l be a prime number with $(l, p) = 1$. Then the results of § 2 shows: The Tate module $T_l(A_i)$ $(i = 0, 1)$ is isomorphic to $\mathfrak{o} \otimes_Z Z_l$ and we may assume that $\theta_i(\mathfrak{o})$ operates on $\mathfrak{o} \otimes_Z Z_l$ as the left multiplications. Therefore, $a \in \mathfrak{o}$ operates on $\mathfrak{o} \otimes_Z Z_l$ as the right multiplication of some element $i_l(a) \in \mathfrak{o} \otimes_Z Z_l$. In this

manner, we have an anti-isomorphism $\mathfrak{o} \otimes_{Z} Z_\ell \ni a_\ell \longmapsto i_\ell(a_\ell) \in \mathfrak{O} \otimes_{Z} Z_\ell$. Then, any homomorphism f from A_0 to A_1 which commutes with the operations of $\mathfrak{O}$ is represented by the Tate module as a right multiplication of $i_\ell(a_\ell)$ $(a_\ell \in \mathfrak{o} \otimes_{Z} Z_\ell)$. Therefore, we can take a left $\mathfrak{o}$-ideal $\mathfrak{a}$ which is prime to p so that the kernals of f and it of the $\mathfrak{a}$-multiplication $\lambda_{\mathfrak{a}}$ are the same. Since f and $\lambda_{\mathfrak{a}}$ are both separable isogeny, we see that f is a compose of the $\mathfrak{a}$-multiplication and an isomorphism. Lemma 3 Q.E.D.

Now we shall go on our proof of Theorem 2. Put $\tilde{A}_z = A_1$, $\tilde{\theta}_z = \theta_1$. Let $\mathfrak{f}$ be the conductor of the order $\mathfrak{o} = \{ a \in \mathrm{End}(\tilde{A}_z) \mid a \circ \tilde{\theta}_z(b) = \tilde{\theta}_z(b) \circ a \text{ for all } b \in \mathfrak{O} \}$. Let $g : A_1 \longrightarrow A_0$ be the $\mathfrak{f}$-multiplication. Put $\theta_0(a) = g \circ \theta_1(a) \circ g^{-1}$ $(a \in B)$. Since $\mathfrak{O}$ and $\mathfrak{o}$ commute, θ_0 defines an injective homomorphism $\mathfrak{O} \longrightarrow \mathrm{End}(A_0)$ with $1_{\mathfrak{O}} = 1_{A_0}$. Moreover, $\{ a \in \mathrm{End}(A_0) \mid a \circ \theta_0(b) = \theta_0(b) \circ a \ (b \in \mathfrak{O}) \}$ is a maximal order since the left order of $\mathfrak{f}$ is a maximal order. Let f be the homomorphism from A_0 to A_1, where $f \circ g = n 1_{A_1}$ for some natural number n. Then $f : (A_0, \theta_0) \longrightarrow (A_1, \theta_1)$ satisfies the conditions in Lemma 3. Therefore $\mathfrak{o}$ is a maximal order.

Now we shall fix a $\tilde{Q}_z = (\tilde{A}_z, \tilde{C}_z, \tilde{\theta}_z)$ and take another $\tilde{Q}_{z'}$ $= (\tilde{A}_{z'}, \tilde{C}_{z'}, \tilde{\theta}_{z'})$. Take $\mathbb{F}_q$ sufficiently large so that $\tilde{A}_z$ and $\tilde{A}_{z'}$ have the same Frobenius endomoephism $\pi = q^{\frac{1}{2}} \in \mathcal{O}$. Then $\mathrm{Hom}_{\mathbb{F}_q}(\tilde{A}_z, \tilde{A}_{z'}) \otimes \mathbb{Q}_\ell \cong \mathrm{Hom}(T_\ell(\tilde{A}_z), T_\ell(\tilde{A}_{z'})) \cong \mathrm{Hom}(\mathcal{O} \otimes \mathbb{Z}_\ell, \mathcal{O} \otimes \mathbb{Z}_\ell)$. Therefore, there is a $f_\ell \in \mathrm{Hom}_{\mathbb{F}_q}(\tilde{A}_z, \tilde{A}_{z'}) \otimes \mathbb{Q}$ which commutes with the operations of $\mathcal{O}$. Therefore we can take $f \in \mathrm{Hom}_{\mathbb{F}_q}(\tilde{A}_z, \tilde{A}_{z'})$ which preserves the operations of $\mathcal{O}$. Now put $(\tilde{A}_z, \tilde{\theta}_z) = (A_0, \theta_0)$, $(\tilde{A}_{z'}, \tilde{\theta}_{z'}) = (A_1, \theta_1)$ and $f : (A_0, \theta_0) \longrightarrow (A_1, \theta_1)$. Then Lemma 3 shows that (A_1, θ_1) is isomorphic to $\mathfrak{a}$-transform of (A_0, θ_0) with some $\mathcal{O}$-ideal $\mathfrak{a}$. Moreover, in this case, (A_1, θ_1) is isomorphic to (A_0, θ_0) if and only if $\mathfrak{a}$ is a principal left $\mathcal{O}$-ideal. Let z be a non-trivial fixed point of B^+ on H such that r_z is a maximal order of a imaginary quadratic number field in which p is ramified. Then we see easily $\tilde{Q}_z = (\tilde{A}_z, \tilde{C}_z, \tilde{\theta}_z)$ is super singular (consider the prime ideal decomposition of the Frobenius endomorphism). Moreover, for any $\mathcal{O}$-ideal $\mathfrak{a}$, we can find $\alpha \in B^+$ such that $\tilde{Q}_{\alpha^{-1}(z)}$ is isomorphic to the $\mathfrak{a}$-transform of $\tilde{Q}_z$ just in the same manner as in the proof of Lemma 3. Therefore, we have completed the

proof of Theorem 3. Q.E.D.

4-3. Singular cases. Now we shall study the second case, namely singular case.

Theorem 3. (A classification of singular PEL-structures) We assume that no power of π belongs to Q. Then $\tilde{A}_z$ is isogenous to the square E^2 of a singular elliptic curve E. Therefore $\mathrm{End}(\tilde{A}_z) \otimes Q \cong M_2(M)$, where $M = Q(\pi)$ is an imaginary quadratic number field in which B splits and p is decomposed. Now, let $\mathfrak{r}$ be the center of $\mathrm{End}(\tilde{A}_z)$, namely the commutant of $\tilde{\theta}_z(O)$ in $\mathrm{End}(\tilde{A}_z)$ i.e. $\mathrm{End}(\tilde{Q}_z)$. Then the conductor of $\mathfrak{r}$ is prime to pD. Moreover the number of such $\tilde{Q}_z = (\tilde{A}_z, \tilde{C}_z, \tilde{\theta}_z)$ wiht $\mathrm{End}(\tilde{Q}_z) \cong \mathfrak{r}$ is equal to $2^s h(\mathfrak{r})$, where s is the number of prime numbers which are ramified in B but are not ramified in M, $h(\mathfrak{r})$ is the number of the proper ideal classes of $\mathfrak{r}$. Still more, let $\{Q_z\}$ be a representative of the isomorphism classes of members of $\Sigma(\Omega_1)$ with $\mathrm{End}(Q_z) \cong \mathfrak{r}$ (c.f. § 1, Proposition 4). Then $\{\tilde{Q}_z\}$ constitutes a representative of the isomorphism classes with $\mathrm{End}(\tilde{Q}_z) \cong \mathfrak{r}$.

Proof. We shall prove this theorem in three steps.

First step; studies of $Q(\pi)$.

We note that $Q(\pi)$ is a commutative semi-simple algebra of dimension no greater than 4 (c.f. [E], Theorem 2). Therefore $[Q(\pi) : Q] = 1, 2, 3, 4$. We shall exclude the case $[Q(\pi) : Q] = 1, 3, 4$ and show $[Q(\pi) : Q] = 2$. Now let $[Q(\pi) : Q] = 1$. Then $\pi \in Q$, which is a contradiction. Now let $[Q(\pi) : Q] = 4$. Then $\mathrm{End}(\tilde{A}_z) \otimes Q = Q(\pi)$ (c.f. [E], Theorem 2). Since $Q(\pi)$ is commutative, $\mathrm{End}(\tilde{A}_z) \otimes Q$ can not contain non-comutative algebra B, which is a contradiction. Now let $[Q(\pi) : Q] = 3$. Suppose that $\tilde{A}_z$ is F_q-simple. Then $\mathrm{End}_{F_q}(\tilde{A}_z) \otimes Q$ is a simple algebra over Q. Therefore, by considering the ℓ-adic representation, we see the comutant of the commutative semi-simple algebra $Q(\pi) \otimes Q_\ell$, in $M_4(Q_\ell)$ is the simple algebra $\mathrm{End}_{F_q}(\tilde{A}_z) \otimes Q_\ell$ (c.f. [E], Lemma 4). Therefore $[Q(\pi) : Q] = [Q(\pi) \otimes Q_\ell : Q_\ell]$ divides 4 (c.f. [E], Theorem 2), which is a contradiction. Therefore, if $[Q(\pi) : Q] = 3$, then $\tilde{A}_z$ is not F_q-simple. Therefore $\tilde{A}_z \sim E_1 \times E_2$ (F_q-isogenous), where E_i ($i = 1, 2$) is some elliptic curve. If $E_1 \sim E_2$ (F_q-isogenous), then $\mathrm{End}_{F_q}(\tilde{A}_z) \otimes Q$ is a simple algebra over Q. Therefore we have a contradiction as in the above way. If E_1 is not F_q-isogenous to E_2, then $\mathrm{End}_{F_q}(\tilde{A}_z) \otimes Q$

$= \mathrm{End}(E_1) \otimes \mathbb{Q} \oplus \mathrm{End}(E_2) \otimes \mathbb{Q}$. If $\mathrm{End}_{\mathbb{F}_q}(\tilde{A}_z) \otimes \mathbb{Q}$ contains the simple algebra B, then B is contained in $\mathrm{End}(E_1) \otimes \mathbb{Q}$ or $\mathrm{End}(E_2) \otimes \mathbb{Q}$. Since B is an indefinite quaternion over $\mathbb{Q}$, this is a contradiction to the results of the classification of elliptic curves (c.f. M. Deuring, [1]). Therefore $[\mathbb{Q}(\pi) : \mathbb{Q}]$ must equal to 2.

We see above that $\mathbb{Q}(\pi)$ is a quadratic number field or $\mathbb{Q} \oplus \mathbb{Q}$. If $\mathbb{Q}(\pi) = \mathbb{Q} \oplus \mathbb{Q}$, then $\tilde{A}_z \sim E_1 \times E_2$ ($\mathbb{F}_q$-isogenous), where E_1 and E_2 are super-singular elliptic curves with $E_1 \not\sim E_2$ (not $\mathbb{F}_q$-isogenous). Then this assumption leads to a contradiction as above. Therefore $\mathbb{Q}(\pi)$ is a quadratic number field. If $\mathbb{Q}(\pi)$ is a real quadratic number field, then $\pi = \pm q^{\frac{1}{2}} \in \mathbb{Q}$, which is a contradiction. Therefore $\mathbb{Q}(\pi)$ is an imaginary quadratic number field. Therefore we put $M = \mathbb{Q}(\pi)$.

Now we shall show $\mathrm{End}(\tilde{A}_z) \otimes \mathbb{Q} \cong M_2(M)$. Since M is contained in the center of $\mathrm{End}(\tilde{A}_z) \otimes \mathbb{Q}$, $\mathrm{End}(\tilde{A}_z) \otimes \mathbb{Q} \supset B \otimes M$. Since M is an imaginary quadratic number field, $B \otimes_{\mathbb{Q}} M \otimes_{\mathbb{Q}} R = B \otimes_{\mathbb{Q}} C$ splits. Since $B \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong M_2(\mathbb{Q}_p)$, $B \otimes M \otimes \mathbb{Q}_p$ splits. Therefore, since $B \otimes M \otimes \mathbb{Q}_\ell$ ($\ell \neq p$) splits always, $B \otimes M$ splits. Therefore M is a splitting field of B and $B \otimes M \cong M_2(M)$. Therefore

$\mathrm{End}(\tilde{A}_z) \otimes \mathbb{Q} \supset M_2(M)$. Taking a ℓ-adic representation of $\tilde{A}_z$ where ℓ is a prime number which is prime to p and decomposed in M, we see easily that $\mathrm{End}(\tilde{A}_z) \otimes \mathbb{Q} = M_2(M)$ (c.f. [E], Lemma 4).

Second step; studies of (r).

Now, we shall show that p is decomposed in M and that, if we write $p = (p)(\bar{p})$, $(p) \neq (\bar{p})$, then the principal ideal (π) is equal to some power of (p) or $(\bar{p})$. Then, since $\pi \in (r)$, the conductor of (r) must be prime to p.

Suppose that $p = (p)$ or $(p)^2$ in M. Then, since $\pi\bar{\pi} = q =$ a power of p, (π) is equal to a power $(p)^\alpha$ of (p). Well, $(\tilde{\pi})$ is also equal to $(p)^\alpha$. Therefore $\pi/\bar{\pi}$ is a unit of M. Since M is an imaginary quadratic number field, $\pi/\bar{\pi}$ is a root of unity. Therefore, there is a natural number β such that $\pi^\beta = \bar{\pi}^\beta$. Then $\pi^\beta \in \mathbb{Q}$, which is a contradiction. Therefore p is decomposed in M. Moreover, above considerations show that, if $p = (p)(\bar{p})$, $(p) \neq (\bar{p})$, then $(\pi) = (p)^\alpha (\bar{p})^\beta$ with $\alpha \neq \beta$.

Now we shall show that α or $\beta = 0$. Let (f) be the conductor of (r) and A_0 be the (f)-transform of $\tilde{A}_z$. Since (r) is contained in the center of $\mathrm{End}(\tilde{A}_z) \otimes \mathbb{Q}$, there is an injection

$\theta_0 : \mathcal{O} \longrightarrow \mathrm{End}(A_0)$. Moreover, since $\tilde{A}_z$ and A_0 is isogenous, we may take sufficiently large F_q so that $\tilde{A}_z$ and A_0 are F_q-isogenous and θ_0 induces an injection $\mathcal{O} \longrightarrow \mathrm{End}_{F_q}(A_0)$. Then $\mathrm{End}(A_0) \otimes \mathbb{Q} = M_2(M)$ and the center of $\mathrm{End}(A_0) \otimes \mathbb{Q}$ is the maximal order $\mathfrak{r}_0$. Since $\tilde{A}_z$ and A_0 is F_q-isogenous, they have the same Frobenius endomorphism π (c.f. [E], Theorem 1). Now, consider the representation δ of $\mathfrak{r}_0$ at the tangent space of A_0. Then Corollary 1 of Proposition 8 shows that the image of δ is contained in $\bar{F}_p$. Therefore the kernel of δ is a prime ideal of $\mathfrak{r}$. Since $\delta(p\mathfrak{r}_0) = 0$, the kernel of δ is $\mathfrak{p}$ or $\bar{\mathfrak{p}}$. Therefore one of $\mathfrak{p}$ or $\bar{\mathfrak{p}}$ multiplication is a separable isogeny and the other is a purely inseparable isogeny. Therefore, since $(\pi) = \mathfrak{p}^{\alpha}\bar{\mathfrak{p}}^{\beta}$ is purely inseparable isogeny, α or β must be equal to 0. Consequently we have $(\pi) = \mathfrak{p}^{\alpha}$ or $\bar{\mathfrak{p}}^{\beta}$.

Now we shall show that the conductor of $\mathfrak{r}$ is prime to D. For this purpose, take any prime number ℓ which divides D. Since p is prime to D, $T_\ell(\tilde{A}_z) = \mathcal{O} \otimes \mathbb{Z}_\ell$. Moreover, since $\mathcal{O}$ is a maximal order, $\mathcal{O} \otimes \mathbb{Z}_\ell$ is the unique maximal order of the unique division quaternion algebra over $\mathbb{Q}_\ell$. Since $\mathfrak{r} \otimes \mathbb{Z}_\ell$

is optimally imbedded in $\mathfrak{O} \otimes \mathbb{Z}_\ell$ (c.f. [E], Main Theorem), $\mathfrak{r} \otimes \mathbb{Z}_\ell$ is the maximal order of $M \otimes \mathbb{Q}_\ell$.

Remark. Let M, $\mathfrak{r}$, π be as above. Then there is a singular elliptic curve E whose Frobenius endomorphism is equal to some power of π (c.f. M. Deuring [1]). Therefore $\tilde{A}_z$ must be isogenous to the square E^2 (c.f. [E], Theorem 1).

Third step; a classification of isomorphism classes.

At first, we shall consider the representation δ of $\mathfrak{r}$ at the tangent space of $\tilde{A}_z$. Since $(\pi) = \mathfrak{p}^\alpha$ (if $(\pi) = \bar{\mathfrak{p}}^\beta$, then replace $\mathfrak{p}$ with $\bar{\mathfrak{p}}$), we see from Corollary 1 of Proposition 8 that δ is equivalent to

$$\mathfrak{r} \ni \alpha \longmapsto \begin{pmatrix} \alpha \bmod \mathfrak{p} & 0 \\ 0 & \alpha \bmod \mathfrak{p} \end{pmatrix}.$$

Therefore, π is purely inseperable and $\bar{\pi}$ is separable. Therefore $T_p(\tilde{A}_z) = \varprojlim A_{p^n} \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$ and $\mathfrak{r}$ operates on $T_p(\tilde{A}_z) \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$ by the multiplications of $\mathfrak{r} \subset \mathfrak{r}_\mathfrak{p} \cong \mathbb{Z}_p$. Now let us fix an isomorphism $\mathfrak{O} \otimes \mathbb{Z}_p \cong M_2(\mathbb{Z}_p)$. Then, as in § 2, we see that there is a $M_2(\mathbb{Z}_p)$ unit γ_z such that $\mathfrak{O}$ operates on $T_p(\tilde{A}) \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$ as the left multiplication of $\gamma_z^{-1} M_2(\mathbb{Z}_p) \gamma_z$. Let $\tilde{Q}_z$

and $\tilde{Q}_{z'}$ be two such PEL-structures. Then we see that any elements of $\mathrm{Hom}(\tilde{A}_z, \tilde{A}_{z'})$ which preserve the operation of O are represented on p-adic representations as the left multiplications of some elements of $\gamma_z^{-1} Z_p \gamma_{z'}$.

Now we shall show three facts:

① If $\mathrm{End}(Q_z) \cong \mathfrak{r}$, then $\mathrm{End}(\tilde{Q}_z) \cong \mathfrak{r}$, where $\mathfrak{r}$ be as in before.

② If $\mathrm{End}(Q_z)$, $\mathrm{End}(Q_{z'}) \cong \mathfrak{r}$ and $Q_z \neq Q_{z'}$, then $\tilde{Q}_z \neq \tilde{Q}_z$.

③ If $\mathrm{End}(\tilde{Q}_z) \cong \mathfrak{r}$, we can find z' so that $\mathrm{End}(Q_{z'}) \cong \mathfrak{r}$ and $\tilde{Q}_{z'} \cong \tilde{Q}_z$.

Let z be a non-trivial B^+-fixed point such that $\mathrm{End}(Q_z) \cong \mathfrak{r}$. Let $\tilde{Q}_z$ be the reduction of Q_z. We see easily that $\mathrm{End}(\tilde{Q}_z) \otimes \underset{\sim}{Q} \cong \mathrm{End}(Q_z) \otimes \underset{\sim}{Q}$ from the classification of $\mathrm{End}(\tilde{Q}_z)$ which was obtained in Theorem 2, the first and the step of the proof of this theorem. Moreover $\mathrm{End}(\tilde{Q}_z) \otimes \underset{\sim}{Z}_\ell \cong \mathrm{End}(Q_z) \otimes \underset{\sim}{Z}_\ell$ for all $\ell \nmid p$, since the ℓ-adic representations of endomorphisms of $T_\ell(\tilde{A}_z)$ and $T_\ell(A_z)$ is equivalent and $\mathrm{End}(\tilde{Q}_z) \otimes \underset{\sim}{Z}_\ell$ and $\mathrm{End}(Q_z) \otimes \underset{\sim}{Z}_\ell$ are optimally embedded in $\mathrm{End}(T_\ell(\tilde{A}_z))$ and $\mathrm{End}(T_\ell(A_z))$ (c.f. [E], Main Theorem). Moreover $\mathrm{End}(\tilde{Q}_z) \otimes \underset{\sim}{Z}_p \cong \mathrm{End}(Q_z) \otimes \underset{\sim}{Z}_p \cong \mathfrak{r} \otimes \underset{\sim}{Z}_p$, since $\mathfrak{r} \otimes \underset{\sim}{Z}_p$ is the maximal order.

Therefore, $\mathrm{End}(\tilde{Q}_z) \cong \mathrm{End}(Q_z) = r$. In general, if the conductor of $\mathrm{End}(Q_z)$ is not necessary prime to p, then $\mathrm{End}(\tilde{Q}_z) = \bigcap_{l \nmid p}$ $(\mathrm{End}(Q_z) \otimes \mathbb{Q} \cap \mathrm{End}(\tilde{Q}_z) \otimes \mathbb{Z}_l) \cap$ (the maximal order of $\mathrm{End}(Q_z) \otimes \mathbb{Q}_p$). So we have proved ①.

Now let z, z' be two non-trivial B^+-fixed points which have the same $M \cong \mathrm{End}(Q_z) \otimes \mathbb{Q} \cong \mathrm{End}(Q_{z'}) \otimes \mathbb{Q}$, where M be as before. Then $\mathrm{Hom}(Q_z, Q_{z'}) \otimes \mathbb{Q} \cong \mathrm{Hom}(\tilde{Q}_z, \tilde{Q}_{z'}) \otimes \mathbb{Q}$. Now we assume that there is an isomorphism $f : \tilde{Q}_z \cong \tilde{Q}_{z'}$. Then there is $\alpha \in B^+$ such that $z' = \alpha^{-1}(z)$ and f is represented on the l-adic representations (l may be any prime number, $\neq p$) as $O \otimes \mathbb{Z}_l \ni x \longmapsto x \cdot \alpha \in (O \otimes \mathbb{Z}_l) \cdot \alpha$ (c.f. § 2). Since f is an isomorphism, $(O \otimes \mathbb{Z}_l) \cdot \alpha$ must be equal to $O \otimes \mathbb{Z}_l$ for all $l \nmid p$. Therefore, z and z' are equivalent by $\Gamma(1, p) = \{\alpha \in \bigcup_{n=0}^{\infty} p^{-n} O \subset B \mid N_{B/\mathbb{Q}}(\alpha) = 1\}$.

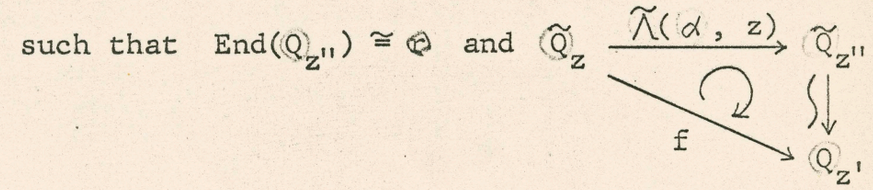
Remark. Let z, $z' \in H$ are B^+-fixed points such that p decompose in $M_z = M_{z'}$. Let Q_z, $Q_{z'} \in \Sigma(\Omega_{N,t})$ with $(N,p) = 1$. Assume $\tilde{Q}_z = \tilde{Q}_{z'}$. Then z and z' are equivalent by $\Gamma(N, p) = \{\alpha \in \Gamma(1, p) \mid \alpha \equiv 1 \bmod^{\times} N O\}$. We can prove this statement by using l-adic representaions.

Now we assume that $\mathrm{End}(Q_z) \cong \mathrm{End}(Q_{z'}) \cong \mathfrak{r}$, where $\mathfrak{r}$ be as before. We see that there is a proper $\mathfrak{r}$-ideal $\mathfrak{a}$ prime to p and an integral two sided $\mathfrak{O}$-ideal $\mathfrak{B}$ where $N_{B/Q}(\mathfrak{B})$ is square free and divisible only by primes which are ramified in B and are not ramified in M, such that $\Lambda(\alpha, z) \in \mathrm{Hom}(Q_z, Q_{z'})$ where $\mathfrak{B}^{-1} f(\mathfrak{a})^{-1} = \mathfrak{O}\alpha^{-1}$ $(\alpha \in B^+)$. Moreover Q_z and $Q_{z'}$ are isomorphic if and only if $\mathfrak{B} = \mathfrak{O}$ and $\mathfrak{a}$ is principal (all of these facts can be proved just in the same manner as in [C] § 2, where $\mathfrak{r}$ is assumed to be the maximal order). Therefore, $\tilde{\Lambda}(\alpha, z)$ is a compose of an element of $\mathrm{End}(Q_z)$ and an isomorphism. Considering the degree, we see that $\mathfrak{B} = \mathfrak{O}$. Moreover, since $\mathrm{End}(\tilde{Q}_z) \cong \mathrm{End}(Q_z) \cong \mathfrak{r}$ amd $\Lambda(\alpha, z)$ is $\mathfrak{a}$-multiplication, $\mathfrak{a}$ is a principal ideal of $\mathfrak{r}$. Therefore $Q_z \cong Q_{z'}$ and we have shown ②.

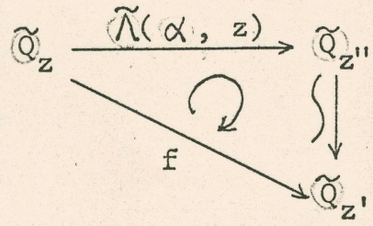
Remark. The above proof of ② can easily generalized to the case that Q_z and $\tilde{Q}_z$ have level structure by using ℓ-adic representations.

Now we fix a non-trivial B^+-fixed point with $\mathrm{End}(Q_z) \cong \mathfrak{r}$. Let $\tilde{Q}_{z'}$ be any PEL-structure with $\mathrm{End}(\tilde{Q}_{z'}) \cong \mathfrak{r}$. Let F_q be a sufficiently large finite field. Then $\tilde{Q}_z$ and $\tilde{Q}_{z'}$ have

the same Frobenius endomorphisms over F_q (c.f. the second step). Therefore there is a F_q-isogeny $f : \tilde{Q}_z \longrightarrow \tilde{Q}_{z'}$. Now we shall show that there is a non-trivial B^+-fixed point z'' and an element α of B^+ such that $\mathrm{End}(Q_{z''}) \cong \mathfrak{o}$ and



is a commutative diagram. Since $\mathfrak{p}$-transform of $\tilde{Q}_z$ is isomorphic to $\tilde{Q}_z^p$ and $\mathfrak{p}$-transform of Q_z is the same type as Q_z, we may assume f is a separable isogeny. Moreover, taking some $\mathfrak{p}$'s power transform of $\tilde{Q}_z$, we may assume the degree of f is prime to p (c.f. the representation of $\mathfrak{r}$ on $T_p(\tilde{A}_z)$ at the first of the third step). Now we shall consider the ℓ-adic representation of f. We see that f is represented as the right multiplication of some element of $\mathfrak{o} \otimes Z_\ell$ on $\mathfrak{o} \otimes Z_\ell$. Since the narrow class number of $\mathfrak{o}$ is equal to 1, we may take $\alpha \in B^+$ so that α is $\mathfrak{o} \otimes Z_p$ unit and $\tilde{\Lambda}(\alpha, z)$ and f has the same kernel. Then



is a commutative diagram,

where $z'' = \alpha^{-1}(z)$. Moreover, we see easily that the condition

$\mathrm{End}(Q_z) \cong \mathfrak{r}$ is satisfied (consider how M is embedded in B). So we have proved ③ and consequently proved Theorem 3. Q.E.D.

Remark. In this section, we have classified the structure $(\tilde{A}_z, \tilde{\theta}_z)$. We note that we have not used that $(\tilde{A}_z, \tilde{\theta}_z)$ is a reduction of some (A_z, θ_z) which is defined over $\bar{\mathbb{Q}}$. We have only used the facts that $\dim \tilde{A}_z = 2$ and $\tilde{\theta}_z$ is an injective homomorphism of $\mathfrak{O}$ into $\mathrm{End}(\tilde{A}_z)$ with $\tilde{\theta}_z(1_{\mathfrak{O}}) = 1_{\tilde{A}_z}$.

Remark. Let z be any non-trivial B^+-fixed point. Let M_z be as in §1. Since $\mathrm{End}(A_z) \otimes \mathbb{Q} \subseteq \mathrm{End}(\tilde{A}_z) \otimes \mathbb{Q}$, we have the followings.

① If p is decomposed in M_z, then $\tilde{Q}_z$ be as in Theorem 3.

② If p is not decomposed in M_z, then $\tilde{Q}_z$ be as in Theorem 2.

This remark is used in section 6.

§5. A construction of a moduli space.

In this section, we shall construct a moduli space for some families of PEL-structures by using the results of §1 and the theory of moduli spaces for abelian varieties which is due to D. Mumford. We shall show in this section only that our moduli space is one dimensional cycle. But we shall show in the next section also that our moduli space has good algebraic geometrical properties. The only result in this section which is used in the following sections is Theorem 4.

5-1. Some results of Mumford. Now we shall quote some results from [GIT]. Let S be a locally noetherian scheme, X a group scheme over S. Let $\pi : X \longrightarrow S$ be the structure morphism, $\varepsilon : S \longrightarrow X$ the section which defines the unit element. If the morphism π is smooth, proper and, for any algebraically closed field Ω and for any Ω-valued point s of S (we call such a point a geometric point), the fibre $\pi^{-1}(s)$ (we call such a fibre a geometric fibre) is connected, then we call X an abelian scheme over S. We note that, if S is $\mathrm{Spec}(k)$, where k is a field, then an abelian scheme over S means an abelian variety defined over k. Now let X be an abelian scheme

over S. We say X is g-dimensional if any geometric fibre of X/S is a g-dimensional abelian variety. For any abelian scheme X over S, there is an abelian scheme $\hat{X}$ over S such that, for any geometric point s of S, the geometric fibre $\hat{X}_s$ is the Picard variety of the geometric fibre X_s. We call $\hat{X}$ the Picard scheme of X. Now let $\omega : X \longrightarrow \hat{X}$ be a surjective S-morphism such that, for any geometric point s, $\omega_s : X_s \longrightarrow \hat{X}_s$ coincides with an isogeny $\varphi_{D_s} : X_s \longrightarrow \hat{X}_s$, where D_s is a positive non-degenerate divisor on X_s and φ_{D_s} is the well-known homomorphism induced by D_s (c.f. A. Weil, [18]). We call such an S-homomorphism ω a polarization of X/S. If the direct image $\omega_*(\mathcal{O}_X)$ is a locally free sheaf of rank d^2, we say that the degree of the polarization ω is d^2.

Now let N be an natural number. We assume that the residue characteristic of any geometric point of S is prime to N. Let $\sigma_1, \cdots, \sigma_{2g}$ be sections of X/S and $\psi_N : X \longrightarrow X$ be the homomorphism which represents N-times addition on X. We say $(\sigma_1, \cdots, \sigma_{2g})$ is a level N structure on X if, for any geometric point s of S, $\sigma_1(s), \cdots, \sigma_{2g}(s)$ give a generator of the group of the points of order N on X_s and $\psi_N \circ \sigma_i = \varepsilon$.

From now on, we shall call a set $\{X, \omega, \{\sigma_i\}\}$ a PL-structure of type (g, d, N) on S if S is a locally noetherian scheme, X is a g-dimensional abelian scheme over S, ω is a polarization on X/S of degree d^2 and $\{\sigma_i\}$ is a level N structure on X/S.

Now S be any locally noetherian scheme, we denotes by $\mathfrak{M}(S) = \mathfrak{M}_{g,d,N}(S)$ the set of all the isomorphism classes of all the PL-structures of type (g,d, N) on S. Then $\mathfrak{M}$ defines a contravariant functor from the category of all the locally noetherian schemes to the category of sets. In [GIT], Mumford has proved the following theorem.

Theorem GIT. *We assume* $N > N_0 = 6^g d\sqrt{g!}$. *Then* $\mathfrak{M}_{g,d,N}$ *is represented by a scheme which is quasi projective over* $\mathrm{Spec}(\mathbb{Z})$. *In other word, there is a subscheme* $M = M_{g,d,N} \subset P_r(\mathrm{Spec}(\mathbb{Z}))$ *of finite type, and a PL-structure* $(Z, \Omega, \{\Sigma_i\})$ *of type* (g,d, N) *on* M *such that, for any locally noetherian scheme* S *and for any PL-structure* $(X, \omega, \{\sigma_i\})$ *of type* (g, d, N) *on* S, *there is a unique morphism*

$$f : S \longrightarrow M$$

such that $(X, \omega, \{\sigma_i\})$ *is isomorphic (as PL-structures of*

type (g, d, N) on S) to the pull back $(Z, \Omega, \{\Sigma_i\}) \times_M S = (Z \times_M S, \Omega \times_M S, \{\Sigma_i \times S\})$ of $(Z, \Omega, \{\Sigma_i\})$, by the morphism f.

For some time, we shall fix g, d, $N > N_0 = 6^g \cdot d \cdot \sqrt{g!}$, and call any PL-structure of type (g, d, N) simply a PL-structure. Now let S, T be locally noetherian schemes. Let $\pi : T \longrightarrow S$ be a morphism and $\{X, \omega, \{\sigma_i\}\}$ a PL-structure on S. Then, we can determine a morphism $f : S \longrightarrow M$ as in Theorem GIT. Then $(X, \omega, \{\sigma_i\}) \times_S T = (X \times_S T, \omega \times_S T, \{\sigma_i \times_S T\})$ gives a PL-structure. We see the morphism which corresponds to this PL-structure as in Theorem GIT is $f \circ \pi : T \longrightarrow M$. In particular, taking as S a noetherian valuation ring and as T the quotient field or the residue field of S, we obtain the following corollary of Theorem GIT.

Corollary 1. Notations be as in Theorem GIT. Let P be a PL-structure of type (g, d, N) over a field K; $\mathfrak{p}$ a discrete place of K such that the residue characteristic of $\mathfrak{p}$ does not divide N. Let A be the underlying abelian variety of the PL-structure P. If A has good reduction at $\mathfrak{p}$, P mod $\mathfrak{p}$ is also a PL-structure of type (g, d, N). Moreover the $\mathfrak{p}(K)$-valued

point of M which corresponds to (P) mod (p) is the reduction mod (p) of the K-valued point which corresponds to (P).

Proof. The first assertion is well-known (c.f. [S & T], Chap. 3 and some others). The second assertion is clear from what we have considered before. Q.E.D.

Now let $S = T = K$ be a field and (σ) an automorphism of K. Then the above considerations show the following.

Corollary 2. Notations be as in Theorem GIT. Let (P) be a PL-structure over a field K and (σ) an automorphism of K. Then the K-valued point which corresponds to (P^{σ}) is the transform by σ of the K-valued point which corresponds to (P).

5-2. An imbedding of the moduli space. Now, we shall construct an imbedding of the moduli space which was constructed in Proposition 5 into the Mumford's moduli space. Let N be a natural number. Here after, we shall use the notation in §1. We assume that N is so large that $(\Gamma(N))$ is torsion free. Then we can apply Proposition 5. Let $V = V_N$ be as in Proposition 5. Let z be a generic point of V over $\underset{\sim}{Q}(e^{\frac{2\pi i}{N}})$, $X_z \in (C_z)$ an ample divisor rational over $\underset{\sim}{Q}(e^{\frac{2\pi i}{N}}, z)$. For any $z' \in V$, we denotes by $X_{z'}$ the divisor which is obtained by the specialization of

X_z over $z \longrightarrow z'$. Let $g = 2$, d^2 = degree of φ_{3X_z} and $N = N$. Then $P_{z'} = (A_{z'}, \varphi_{3X_{z'}}, t_{1z'}, \cdots, t_{4z'})$ is a PL-structure of type (g, d, N) rational over $Q(e^{\frac{2\pi i}{N}}, z')$. Now we assume that N is greater than $N_0 = 6^2\sqrt{2!}\, d$. Then, since $N \geqq 3$, $\Gamma(N)$ is torsion free. Therefore, we can use Theorem GIT and Proposition 5.

Let $Z^{(N)} = \bigcup_{\ell=0}^{\infty} N^{-\ell} Z \subset Q$. We note that M is a subscheme of $P_r(\mathrm{Spec}(Z^{(N)})) \subset P_r(\mathrm{Spec}(Z))$. Let $R = Z[e^{\frac{2\pi i}{N}}] \subset Q(e^{\frac{2\pi i}{N}})$, $R^{(N)} = \bigcup_{\ell=0}^{\infty} N^{-\ell} R \subset Q(e^{\frac{2\pi i}{N}})$. Then $M \times_{\mathrm{Spec}(Z)} \mathrm{Spec}(R)$ is a subscheme of $P_r(\mathrm{Spec}(R^{(N)}))$.

Let z be as before (i.e. a generic point of V over $Q(e^{\frac{2\pi i}{N}})$). Then we have a $Q(e^{\frac{2\pi i}{N}}, z)$-valued point w of $M_{\mathrm{red}} \times_{\mathrm{Spec}(Z)} \mathrm{Spec}(Q(e^{\frac{2\pi i}{N}})) \subset M \times_{\mathrm{Spec}(Z)} \mathrm{Spec}(R^{(N)}) \subset P_r(\mathrm{Spec}(R^{(N)}))$, which corresponds to $P_z = (A_z, \varphi_{3X_z}, t_{1z}, \cdots, t_{4z})$ as in Theorem GIT. Let W_0 be the locus of w over $Q(e^{\frac{2\pi i}{N}})$ in the locally closed set $M_{\mathrm{red}} \times_{\mathrm{Spec}(Z)} \mathrm{Spec}(Q(e^{\frac{2\pi i}{N}})) \subset P_r(C)$. Then W_0 is an algebraic curve defined over $Q(e^{\frac{2\pi i}{N}})$. Let W be the Zariski-closure of W_0 in $P_r(\mathrm{Spec}(R^{(N)}))$. Let $k = Q(e^{\frac{2\pi i}{N}}, w) \subset$

$Q(e^{\frac{2\pi i}{N}}, z)$. Let $\mathfrak{p}$ be any C-valued place of k, trivial on $k \cap Q(e^{\frac{2\pi i}{N}})$. Let $\mathfrak{P}$ be any extension of $\mathfrak{p}$ as a place of $Q(e^{\frac{2\pi i}{N}}, z)$, trivial on $Q(e^{\frac{2\pi i}{N}})$. Since $k \supset Q(e^{\frac{2\pi i}{N}})$ (c.f. [D], II, p. 128), there are some such $\mathfrak{P}$. Then, $\mathfrak{P}$ is induced by some specialization $z \longrightarrow z'$ $(z, z' \in V)$, since z is a generic point of the complete non-singular curve V. In particular, $\mathfrak{P}$ is a discrete place or an isomorphism of fields. By Proposition 5, $\mathfrak{Q}_z$ has good reduction at $\mathfrak{P}$ and $\mathfrak{Q}_z \bmod \mathfrak{P} = \mathfrak{Q}_{z'}$. Therefore, $\mathfrak{P}_z$ has good reduction at $\mathfrak{P}$ and $\mathfrak{P}_z \bmod \mathfrak{P} = \mathfrak{P}_{z'}$. Therefore $w \bmod \mathfrak{p} = w \bmod \mathfrak{P}$ is a C-valued point of $W_0 \subset M \times_{\mathrm{Spec}(Z)} \mathrm{Spec}(R^{(N)})$ which corresponds to $\mathfrak{P}_{z'}$ (c.f. corollaries of Theorem GIT). Therefore, W_0 is a projective algebraic curve defined over $Q(e^{\frac{2\pi i}{N}})$, and, for any C-valued point w' of W_0, there is some C-valued points z' of V such that w' corresponds to $\mathfrak{P}_{z'}$ as in Theorem GIT.

Now we shall prove W is a projective scheme over $\mathrm{Spec}(R^{(N)})$. Put $M \times_{\mathrm{Spec}(Z)} \mathrm{Spec}(R^{(N)}) = S - B$, where S, B be projective schemes over $\mathrm{Spec}(R^{(N)})$. Let p be any prime number which is prime to N, $\mathfrak{P}$ any extension of p as a place of $\bar{Q}$, R_p the

valuation ring of $\mathfrak{P}$ and $\mathfrak{p} = \mathfrak{P} \mid \underset{\sim}{Q}(e^{\frac{2\pi i}{N}})$. Let w' be any $\bar{\underset{\sim}{Q}}$-valued point of W_0. Let $z' \in V$ and $\mathfrak{P}_{z'}$ be as above. By Theorem 1, $\mathfrak{P}_{z'}$ has good reduction at $\mathfrak{P}$. Therefore $w' \bmod \mathfrak{P}$ determines an $\bar{\underset{\sim}{F}}_p$-valued point of $M \times_{\underset{\sim}{Spec}(\underset{\sim}{Z})} Spec(R^{(N)})$.

Let $W_p = W \times_{Spec(R^{(N)})} Spec(R^{(N)} \bmod \mathfrak{p})$. We see that $W_p = W_0 \bmod \mathfrak{p}$ form the definition of W (c.f. [I], Chap. 2. § 8). Moreover it is known that any $\bar{\underset{\sim}{F}}_p$-valued point of the reduced variety W_p is some reduction of $\bar{\underset{\sim}{Q}}$-valued point of W_0 (c.f. ibid.). Therefore, above remark shows that any $\bar{\underset{\sim}{F}}_p$-valued point of W_p determines an $\bar{\underset{\sim}{F}}_p$-valued point of $M \times_{\underset{\sim}{Spec}(\underset{\sim}{Z})} Spec(R^{(N)})$. Now, assume that W is not projective. Then W and B must intersect at a non-empty locally closed set of $P_r(Spec(R^{(N)}))$ defined over $R^{(N)}$. Therefore W must have some $\bar{\underset{\sim}{Q}}$ or $\bar{\underset{\sim}{F}}_p$-valued points which do not determine any $\bar{\underset{\sim}{Q}}$ or $\bar{\underset{\sim}{F}}_p$-valued point of $M \times_{\underset{\sim}{Spec}(\underset{\sim}{Z})} Spec(R^{(N)})$, which contradicts to what we have seen above. Therefore W is projective.

5-3. A construction of a moduli space. In 5-2, we have constructed a moduli space W of PL-structures. Now we shall construct such a finite covering of W that makes a moduli space of PEL-structures.

Let $(x_i)_{i\in I}$ be any transcendental basis of C/Q. Let $(y_{p,i})_{i\in I}$ be a set of elements of the universal domain Ω_p of characteristic p, where $y_{p,i}$ is algebraically independent over F_p. Let $\mathfrak{P}_p$ be the Ω_p-valued place of C which induces $\mathfrak{P}_p : x_i \longrightarrow y_{p,i}$. Let w' be any C-valued point of W_0. Then, there is a C-valued point z' of V such that w' corresponds to $\mathfrak{P}_{z'}$. Since W is projective over $\mathrm{Spec}(R^{(N)})$, $w' \bmod \mathfrak{P}_p$ is a Ω_p-valued point of W. Therefore it is a Ω_p-valued point of $M \times_{\mathrm{Spec}(Z)} \mathrm{Spec}(R^{(N)})$. Therefore $\mathfrak{P}_{z'}$ has good reduction at $\mathfrak{P}_p$ and $w' \bmod \mathfrak{P}_p$ is the corresponding point of PL-structure $\mathfrak{P}_{z'} \bmod \mathfrak{P}_p$. In the following, we shall fix for sometime the place $\mathfrak{P}_p$ and the universal domain Ω_p. Moreover, we assume $\Omega_p = C \bmod \mathfrak{P}_p$ (since the residue field of a valuation ring whose quotient field is algebraically closed is also algebraically closed). Let

$$\mathfrak{S}_0 = \{\mathfrak{Q}_z \mid z \in V\},$$

$$\mathfrak{S}_p = \{\mathfrak{Q}_z \bmod \mathfrak{P}_p \text{ (modulo isomorphisms)} \mid z \in V\}$$

and

$$\mathfrak{S} = \mathfrak{S}_0 \cup \bigcup_{p\nmid N} \mathfrak{S}_p .$$

We shall construct a moduli space for the family $\mathfrak{S}$ of PEL-structures.

Now let $(Z, \Omega, \{\Sigma_i\})$ be as in Theorem GIT. Let $(X, \omega, \{\sigma_i\})$ be the pull back of $(Z, \Omega, \{\Sigma_i\})$ by the morphism $W \longrightarrow M \times_{\mathrm{Spec}(\underset{\sim}{C})} \mathrm{Spec}(R^{(N)}) \longrightarrow M$. Then for any $\underset{\sim}{C}$ or Ω_p-valued point of W, the fibre of $(X, \omega, \{\sigma_i\})$ at this point is isomorphic to the PL-structure which correspond to this point as described before (c.f. Theorem GIT).

Lemma 4. *There is an open covering $\{U_i\}_{i \in I}$ of W with the following properties.*

① *There is an embedding $\phi_i : X \times_C U_i \subset P_m(U_i)$, where $m = 6^g.d - 1$ and $P_m(U_i)$ is the projective space over U_i.*

② *There are $g_{ij} \in \mathrm{PGL}(m)(U_i \cap U_j)$ $(i, i \in I)$ such that g_{ij} induce isomorphism $\phi_i(X \times_C U_i) \xrightarrow{\sim} \phi_j(X \times_C U_j)$, where $\mathrm{PGL}(m)(U_i \cap U_j)$ are the sets of all the $U_i \cap U_j$-valued points of the group scheme $\mathrm{PGL}(m)$ and operate on $U_i \cap U_j$ in the natural way.*

Proof. This is a special case of [GIT], p. 136, Proposition 7.5.

Q.E.D.

Remark. Since $\mathrm{Spec}(R^{(N)})$ is quasi compact and W is finite type over $\mathrm{Spec}(R^{(N)})$, W is quasi compact. Therfore we may assume the above covering $\{U_i\}_{i \in I}$ is a finite affine covering.

In the following, we take $\{U_i\}_{i\in I}$ with such properties.

Now let z be a generic point of V over $\underset{\sim}{Q}(e^{\frac{2\pi i}{N}})$, w the generic point of W which corresponds to the PL-structure $P_z = (A_z, \varphi_{3X_z}, t_{1z}, \cdots, t_{4z})$. Let $r_1 = 1, r_2, r_3, r_4$ be a $\underset{\sim}{Z}$-basis of O. We shall fix it hereafter. Let $R_\ell = \theta_z(r_\ell) \in \mathrm{End}(A_z)$ $(\ell = 1, 2, \cdots, 4)$. Let $\bar{\phi}_i : A_z \hookrightarrow P_m(U_i \times \mathrm{Spec}(C))$ be the embedding induced by $\phi_i : X \times_c U_i \hookrightarrow P_m(U_i)$ on the fibre of the $\underset{\sim}{C}$-valued point $w : \mathrm{Spec}(\underset{\sim}{Q}(e^{\frac{2\pi i}{N}}, w)) \longrightarrow U_i$. Using this embedding, we transfer all the structures of P_z to the variety $\bar{\phi}_i(A_z)$. In particular, let $R_{\ell,i}$ be the image of R_ℓ by $\bar{\phi}_i$ and $c_{\ell,i}$ be the Chow point of the graph of $R_{\ell,i}$. (Since $P_{m_1} \times \cdots \times P_{m_k}$ can be embedded canonically into a large P_m over $\mathrm{Spec}(\underset{\sim}{Z})$ by the Segre's morphism, we can define the Chow point of a subvariety of $P_{m_1} \times \cdots \times P_{m_k}$ by the Chow point of the embedded subvariety of P_m.) In view of Lemma 4, the degree d_ℓ of the graph of $R_{\ell,i}$ does not depend on i. By the definition of the Chow point, $c_{\ell,i}$ is the coefficient of some homogenous polynomial $F_{w,\ell,i}(u^{(0)}, u^{(1)})$ of the degree d_ℓ. Therefore we can take $c_{\ell,i}$ as a $\mathrm{Spec}(\underset{\sim}{Q}(e^{\frac{2\pi i}{N}}, z))$-valued point of a

large projective space $P_{L(\ell)}(\mathrm{Spec}(R^{(N)}))$, where $L(\ell)$ depends only on m and d_ℓ. Now S_i be the Zariski-closure of $c_{1,i} \times \cdots \times c_{4,i} \times w$ in $P_{L(1)}(\mathrm{Spec}(R^{(N)})) \times \cdots \times P_{L(4)}(\mathrm{Spec}(R^{(N)})) \times U_i$.

Lemma 5. Let K be a field, V a variety in a projective space defined over K. Then the Chow point $c(V)$ of V is K-rational. Moreover the map

$$V \longmapsto c(V)$$

commutes with every operations of any discrete place of K or any automorphism of K.

Proof. The first part is well known. For the second part, it can be proved easily by using the definition of Chow points (c.f. e.g. H. Hironaka, [3]). Q.E.D.

By this lemma and by the fact that every endomorphisms of an abelian variety has good reduction (i.e. its graph is reduced to a graph of an endomorphism of the reduced abelian variety) whenever the abelian variety has good reduction (c.f. [S & T], p. 94, Proposition 12), we can prove the following Proposition 9.

Proposition 9. Every C or Ω_p-valued point of S_i is obtained

as $c'_{1,i} \times \cdots \times c'_{4,i} \times w'$ or $c'_{1,i} \times \cdots \times c'_{4,i} \times w' \bmod \mathfrak{P}_p$, where $c'_{1,i} \times \cdots \times w'$ or $c'_{1,i} \times \cdots \times w' \bmod \mathfrak{P}_p$ is made from $\mathfrak{Q}_{z'}$ or $\mathfrak{Q}_{z'} \bmod \mathfrak{P}_p$ ($z' \in V$, i.e. z' is a $\underset{\sim}{C}$-valued point of V) as we have made $c_{1,i} \times \cdots \times w$ from $\mathfrak{Q}_z$. Moreover, this correspondence $c'_{1,i} \times \cdots \times w'$ or $c'_{1,i} \times \cdots \times w' \bmod \mathfrak{P}_p \longmapsto \mathfrak{Q}_{z'}$ or $\mathfrak{Q}_{z'} \bmod \mathfrak{P}_p$ commutes with every operations of $\underset{\sim}{C}$ or $\mathfrak{Q}_p$-valued discrete places and automorphisms of $\underset{\sim}{C}$ or $\mathfrak{Q}_p$.

Proof. Do similarly as we have done about W. Q.E.D.

Since the operation of PGL(m) on P_m induces an operation on the spaces of Chow points of subvarieties of P_m, $g_{ij} \in \mathrm{PGL}(m)$ $(U_i \cap U_j)$ induces a biregular morphism $G_{i,j} : S_i \times_{U_i} (U_i \cap U_j) \longrightarrow S_j \times_{U_j} (U_i \cap U_j)$. By using this biregular morphism, we can paste up S_i $(i \in I)$ and make a scheme S over $\mathrm{Spec}(R^{(N)})$. Moreover, it is clear that S is irreducible and proper over $\mathrm{Spec}(R^{(N)})$, since W is so over $\mathrm{Spec}(R^{(N)})$. We see easily that this pasting is compatible with the correspondence $c'_{1,i} \times \cdots \times w'$ or $c'_{1,i} \times \cdots \times w' \bmod \mathfrak{P}_p \longmapsto \mathfrak{Q}_{z'}$ or $\mathfrak{Q}_{z'} \bmod \mathfrak{P}_p$. Therefore, we have a correspondence s' or $s' \bmod \mathfrak{P}_p \longmapsto \mathfrak{Q}_{z'}$ or $\mathfrak{Q}_{z'} \bmod \mathfrak{P}_p$ where s' or $s' \bmod \mathfrak{P}_p$ is a $\underset{\sim}{C}$ or $\mathfrak{Q}_p$-valued

point of S. From Proposition 5 and Theorem 1, the image of this correspondence is (S). Since $N > N_0 = 6^2\sqrt{2}\,d > 3$, $(P_{z'}$ or $(P_{z'}$ mod $(P_p$ has no automorphism (c.f. the last remark of §3). Therefore to determine a PEL-structure on a given PL-structure $(P_{z'}$ or $(P_{z'}$ mod $(P_p$ is equivalent to determine the endomorphisms of $A_{z'}$ or $A_{z'}$ mod $(P_p$ which correspond to $r_1 = 1, r_2, r_3, r_4 \in (O)$. Therefore, from the construction of S, this correspondence is injective. Therefore we have a one-to-one correspondence $(\psi : (Q_{s'} \longmapsto s'$ between (S) and the set of all the $\underset{\sim}{C}$ or $(\Omega_p$-valued point of S. Clearly this correspondence commutes with every operations of $\underset{\sim}{C}$ or $(\Omega_p$-valued places or automorphisms of $\underset{\sim}{C}$ or $(\Omega_p$.

Now let $(Q_{s'} \in (S)$ and $(\sigma \in \mathrm{Aut}(\underset{\sim}{C}/\underset{\sim}{Q}(e^{\frac{2\pi i}{N}}))$ or $\mathrm{Aut}((\Omega_p/\underset{\sim}{F}_p(e^{\frac{2\pi i}{N}}))$. Then $(Q_{s'})^{\sigma} \cong (Q_{s'}$ if and only if $(s')^{\sigma} = s'$. Therefore, if the field of moduli of $(Q_{s'}$ is perfect, the coordinates of s' generate over $\underset{\sim}{Q}(e^{\frac{2\pi i}{N}})$ or $\underset{\sim}{F}_p(e^{\frac{2\pi i}{N}})$ the field of moduli of $(Q_{s'}$. Therefore we have obtained the following theorem.

Theorem 4. *Let $N > N_0 = 6^2\sqrt{2}\,d > 3$ be a natural number, $R^{(N)} = \bigcup_{l=0}^{\infty} N^{-l}\underset{\sim}{Z}[e^{\frac{2\pi i}{N}}] \subset \underset{\sim}{Q}(e^{\frac{2\pi i}{N}})$. Let*

$$S = \{ Q_{s'} = Q_{z'} \text{ or } Q_z \bmod P_p \}$$

be the set of PEL-structures which was defined before. Then there is a proper irreducible scheme S over $\mathrm{Spec}(R^{(N)})$ and a bijective map ψ between S and the set of all the C or Ω_p-valued point of S, which satisfy the following conditions.

① $S_0 = S \times_{\mathrm{Spec}(R^{(N)})} \mathrm{Spec}(Q(e^{\frac{2\pi i}{N}}))$ is an absolutely irreducible curve and there is a birational one-to-one morphism

$$f : V \longrightarrow S_0$$

such that $\psi(Q_z) = f(z)$.

② $S_p = S \times_{\mathrm{Spec}(R^{(N)})} \mathrm{Spec}(F_p(e^{\frac{2\pi i}{N}}))$ $(p \nmid N)$ is a reduction modulo P_p of S_0.

③ ψ commutes with every operation of C or Ω_p-valued discrete places and automorphisms of C or Ω_p.

④ For any $Q \in S$ whose field of moduli is perfect, the coordinates of $\psi(Q)$ generate over $Q(e^{\frac{2\pi i}{N}})$ or $F_p(e^{\frac{2\pi i}{N}})$ the field of moduli of the PEL-structure Q.

Proof. Except ①, this theorem has already proved. Therefore we shall show ①. We define a rational map $f : V \longrightarrow S_0$ by $f(z) = \psi(Q_z)$. Since the map $z \longmapsto Q_z \longmapsto \psi(Q_z)$ commutes with

every operation of $\underset{\sim}{C}$-valued discrete places of $\underset{\sim}{Q}(e^{\frac{2\pi i}{N}}, z)$ trivial on $\underset{\sim}{Q}(e^{\frac{2\pi i}{N}})$ and automorphisms of $\underset{\sim}{C}$ over $\underset{\sim}{Q}(e^{\frac{2\pi i}{N}})$, $f(z') = \psi(Q_{z'})$ hold for all C-valued point of V. Moreover, since $f(z') = f(z'') \Longleftrightarrow Q_{z'} \cong Q_{z''} \Longleftrightarrow z' = z''$, f is injective. Since the surjectivity of f is clear (every element of S defined over $\underset{\sim}{C}$ are $Q_{z'}$, (z' is a $\underset{\sim}{C}$-valued points of V)), we have proved Theorem 4. Q.E.D.

Remark. In this section, we have used the assumption that S is our special family of PEL-structures only as Theorem 1. Therefore, for any family of PEL-structures, we can construct a moduli space over a ring as in our case if we remove the condition that S is proper over $\mathrm{Spec}(R^{(N)})$.