J. Math. Soc. Japan
Vol. 13, No. 3, 1961

On the zeta-functions of the algebraic curves uniformized by certain automorphic functions

By Goro SHIMURA

(Received March 31, 1961)

Introduction. After Hasse and Weil, we can attach a zeta-function to every algebraic variety defined over an algebraic number field. In contrast with its importance, our knowledge of the zeta-function of this kind is little. At present, as far as I know, the zeta-function is determined only in the following two cases.

I) Abelian varieties with sufficiently many complex multiplications [**30, 3, 27**].

II) Algebraic curves uniformized by modular functions belonging to congruence-subgroups [**6, 22**].

Here we note that the determination of the zeta-function of a curve is essentially the same as the determination of the zeta-function of its jacobian. Now, in all these cases, the zeta-functions are meromorphic on the whole complex plane and satisfy functional equations, as conjectured by Hasse.

The purpose of the present paper is to supply a new class of algebraic curves, for which Hasse's conjecture is true, and of which the curves of II) are particular cases. Our principal result is as follows. Let Φ be an indefinite quaternion algebra over the rational number field $\boldsymbol{Q}$, and $\mathfrak{o}$ a maximal order in Φ. Take a positive integer N which is prime to the discriminant of Φ and denote by Γ_N the group of units γ of $\mathfrak{o}$, with positive reduced norm, such that $\gamma \equiv 1 \bmod. N\mathfrak{o}$. As Φ has a faithful representation by real matrices of degree 2, Γ_N is considered as a Fuchsian group on the upper half plane $\mathfrak{H}$. If Φ has no zero-divisor, $\Gamma_N \backslash \mathfrak{H}$ is compact, while if Φ is the total matric algebra of degree 2 over $\boldsymbol{Q}, \Gamma_N$ is nothing but the principal congruence-subgroup of SL$(2, \boldsymbol{Z})$ of level N. Now, according to Eichler [**7**], we can develop the theory of Hecke's operators for cusp-forms with respect to Γ_N. We obtain then Dirichlet-series $D(s)$, meromorphic on the whole plane, having Euler-products, and sa:isfying functional equations. Let $\mathfrak{K}_N$ be the field of automorphic functions with respect to Γ_N. We can find an algebraic curve $\mathfrak{C}_N$, defined over $\boldsymbol{Q}$, whose function-field is identified with $\mathfrak{K}_N$. Our main theorem asserts that the zeta-function of $\mathfrak{C}_N$ is determined by the Dirichlet-series $D(s)$ for cusp-forms of degree 2.

We shall now explain our method by giving a summary of the contents.[1] §§ 1.1~1.4 introduce the ring of modular correspondences for the group Γ_N; in § 1.5, we consider the representations of modular correspondences in the vector spaces of cusp-forms. Each representation yields a Dirichlet series $D(s)$ with an Euler-product. We can express $D(s)$ as a certain integral on the idèle-group of Φ; then the Poisson summation formula on the adèle-space lead to the functional equation for $D(s)$ (Theorem 1 of § 1.6). Now we consider the one-parameter system $\{A_z \mid z \in \mathfrak{H}\}$ of polarized abelian varieties of dimension 2, whose endomorphism-rings are isomorphic to $\mathfrak{o}$; such a system has been constructed in a previous paper [**23**] (quoted hereafter as [AF]). We have shown in [AF] that the moduli $f_i(z)$ of A_z, considered as functions of z, generate the field of automorphic functions $\mathfrak{K}_1$. We construct a quotient variety V_z of A_z by the automorphisms ± 1, which is called the Kummer variety of A_z, as well as a natural mapping h_z of A_z onto V_z with a suitable property. Then, t_z being a point on A_z of order N, the coordinates of $h_z(t_z)$, regarded as functions of z, give automorphic functions $g_j(z)$ with respect to Γ_N; the functions f_i and g_j generate over $\boldsymbol{C}$ the field $\mathfrak{K}_N$. These facts are proved in §§ 2.1~3.4. The field $\boldsymbol{Q}(f_i, g_j)$ is a Galois extension of $\boldsymbol{Q}(f_i)$; we determine in § 4.1 the Galois group. §§ 4.2~4.3 concern the relation of modular correspondences and isogenies of A_z. Taking a generic member A_z of our system, we consider the isogenies λ_ν of A_z onto other members A_{z_ν} whose kernels are isomorphic to $\mathfrak{o}/\mathfrak{q}$ for a given left $\mathfrak{o}$-ideal $\mathfrak{q}$. Then the correspondence $(f_i(z), g_j(z)) \rightarrow (f_i(z_\nu), g_j(z_\nu))$ determines an algebraic correspondence $X_\mathfrak{q}$ of the curve $\mathfrak{C}_N$. If $\mathfrak{o}/\mathfrak{q}$ is of order p^2 for a prime number p, and if p does not divide the discriminant of Φ, then, by the reduction modulo p, we obtain from the λ_ν one purely inseparable isogeny and p separable isogenies. This fact is the key to the congruence-relations for $X_\mathfrak{q}$, which are fundamental in our whole theory, and whose proof is the object of §§ 5.1~5.5. Our principal result is then easily derived from those relations. The idea is almost the same as [**22**], where the author treated the one-parameter system of elliptic curves. The present situation is, however, more complicated than [**22**], since the abelian varieties A_z are not necessarily defined over the field of moduli. We can overcome this difficulty by the use of "normalized Kummer variety".

The present investigation may be thus regarded as a continuation of [**22**] and [AF]. It is also considered as an example of a more general theory, which is definitely non-abelian in character, and which one may expect to be constructed in future; but as for this, I have only mentioned some related problems at

[1] Our results were partly announced in the memoir "Fonctions automorphes et correspondances modulaires", Proc. Int. Cong. Math. 1958, 330-338. In the last half of this article, the reader will also find a brief and easy account of the theory.

the end of the paper.

Notation. We shall use the same notation as in [AF]. In particular, we denote by $c(V)$ the Chow-point of an algebraic variety V. The notation concerning abelian varieties will be the same as Weil [**29**]; so, if λ is an isogeny of an abelian variety A, all being defined over a field k, we denote by $\nu_i(\lambda)$ and $\nu_s(\lambda)$ the inseparable and separable factors of the degree of $k(x)$ over $k(\lambda x)$, respectively, where x is a generic point of A over k.

§ 1. Analytic theory of modular correspondences.

1.1. Ring of transformations. We first recall the definition of ring of transformations introduced in [**24**, §7]. Let $\mathfrak{G}$ be a group; two subgroups G and G' of $\mathfrak{G}$ are called *commensurable* if the intersection $G \cap G'$ is of finite index in G and in G'. Fix a subgroup G of $\mathfrak{G}$; let $\tilde{G}$ be the set of all elements α of $\mathfrak{G}$ such that $\alpha^{-1}G\alpha$ is commensurable with G. It can be easily verified that $\tilde{G}$ is a subgroup of $\mathfrak{G}$ containing G. For every element α of G, we see easily that

$$(1) \qquad [G:G\cap\alpha^{-1}G\alpha]=[\alpha G\alpha^{-1}:\alpha G\alpha^{-1}\cap G]$$
$$=\text{the number of right cosets } G\beta \text{ contained in } G\alpha G;$$

and a similar equality holds for the left cosets in $G\alpha G$.

LEMMA 1.1. *If the number of right cosets in $G\alpha G$ is equal to the number of left cosets in $G\alpha G$, then there exists a common system of representatives for right and left cosets in $G\alpha G$.*

PROOF. Let $G\beta$ and γG be a right coset and a left coset contained in $G\alpha G$. As we have $G\beta G=G\alpha G=G\gamma G$, the intersection $G\beta\cap\gamma G$ is not empty. Taking an element δ in $G\beta\cap\gamma G$, we get $G\beta=G\delta$ and $\gamma G=\delta G$; our lemma is a consequence of this fact.

Now fix a sub-semi-group S of $\tilde{G}$ containing G; we can take for example $\tilde{G}$ itself as S. Let $\mathfrak{R}$ denote the free $\boldsymbol{Z}$-module generated by the $G\alpha G$ for $\alpha\in S$. We shall now define a law of multiplication on the module $\mathfrak{R}$. For any two elements α and β of S, let $\{G\alpha_i\}$ and $\{G\beta_k\}$ be the complete systems of right cosets contained in $G\alpha G$ and in $G\beta G$, respectively. γ being an element of S, we can easily verify that the number of (i,k) such that $G\alpha_i\beta_k=G\gamma$ depends only on $G\alpha G, G\beta G, G\gamma G$, and is independent of the choice of $\{\alpha_i\}$, $\{\beta_k\}$, and γ. Putting $\sigma=G\alpha G, \tau=G\beta G, \rho=G\gamma G$, we denote this number by $\mu(\sigma\cdot\tau;\rho)$. Define the product $\sigma\cdot\tau$ by

$$\sigma\cdot\tau=\sum\mu(\sigma\cdot\tau;\rho)\rho\,,$$

where the sum is extended over all the $\rho=G\gamma G$ contained in $G\alpha G\beta G$. We extend this by linearity to a law of multiplication on $\mathfrak{R}$; the module $\mathfrak{R}$

then becomes an associative ring; the identity element is the coset $G=G1G$. We denote this ring by $\mathfrak{R}(G,S)$ and call it the *ring of transformations of* G *with respect to* S. For every $\sigma=G\alpha G$, we denote by $\deg(\sigma)$ the number given by (1) and put for $\sigma_\nu=G\alpha_\nu G$ and for $c_\nu\in\boldsymbol{Z}$,

$$\deg(\sum_\nu c_\nu\sigma_\nu)=\sum_\nu c_\nu\deg(\sigma_\nu).$$

By our definition, we see easily, for every $\xi,\eta\in\mathfrak{R}$,

$$\deg(\xi+\eta)=\deg(\xi)+\deg(\eta),$$

$$\deg(\xi\cdot\eta)=\deg(\xi)\cdot\deg(\eta);$$

and, for $\sigma=G\alpha G=\bigcup G\alpha_i$, $\tau=G\beta G=\bigcup G\beta_k$, $\rho=G\gamma G$,

$$(2)\qquad \deg(\rho)\mu(\sigma\cdot\tau;\rho)=\text{the number of } (i,k) \text{ such that } G\alpha_i\beta_kG=G\gamma G.$$

PROPOSITION 1.2. *If there exists an anti-automorphism $\alpha\to\alpha^*$ of the semigroup S which maps $G\alpha G$ onto $G\alpha G$ itself for every $\alpha\in S$, then the ring $\mathfrak{R}(G,S)$ is commutative.*

PROOF. Considering the anti-automorphism on $G\alpha G$, we see that the number of left cosets in $G\alpha G$ and the number of right cosets in $G\alpha G$ are the same. Hence, by Lemma 1.1, for every $\alpha,\beta\in S$, we can find sets of elements $\{\alpha_i\}$ and $\{\beta_k\}$ such that $G\alpha G=\bigcup G\alpha_i=\bigcup\alpha_iG$, $G\beta G=\bigcup G\beta_k=\bigcup\beta_kG$ are disjoint sums. We have then $G\alpha G=\bigcup G\alpha_i^*$ and $G\beta G=\bigcup G\beta_k^*$. Put $\sigma=G\alpha G$, $\tau=G\beta G$. By the relation (2), we have, for every $\rho=G\gamma G$ contained in $G\alpha G\beta G$,

$$\deg(\rho)\mu(\sigma\cdot\tau;\rho)=\text{the number of } (i,k) \text{ such that } G\alpha_i\beta_kG=G\gamma G,$$

$$\deg(\rho)\mu(\tau\cdot\sigma;\rho)=\text{the number of } (k,i) \text{ such that } G\beta_k^*\alpha_i^*G=G\gamma G.$$

Applying the anti-automorphism $\alpha\to\alpha^*$ to each double coset, we observe that these two numbers coincide; so we have $\mu(\sigma\cdot\tau;\rho)=\mu(\tau\cdot\sigma;\rho)$. This proves our proposition.

1.2. Arithmetic of indefinite quaternion algebras. Let Φ be an indefinite quaternion algebra over $\boldsymbol{Q}$ (cf. [AF, § 5, no. 14]). We denote by $\alpha\to\alpha'$ the canonical involution of Φ and put $N(\alpha)=\alpha\alpha'$, $\mathrm{tr}(\alpha)=\alpha+\alpha'$. Let $\mathfrak{o}$ be a maximal order in Φ; put, for any base $\{u_i\}$ of $\mathfrak{o}$ over $\boldsymbol{Z}$,

$$d(\Phi)=|\det(\mathrm{tr}(u_iu_j))|^{1/2}.$$

This number is independent of the choice of $\mathfrak{o}$ and $\{u_i\}$; it is a square-free positive integer. Throughout the present paper, we shall use these notations always in this sense.

Now we fix once for all a maximal order $\mathfrak{o}$. For every integral right, left, two-sided $\mathfrak{o}$-ideal $\mathfrak{a}$, we denote by $N_1(\mathfrak{a})$ the number of elements in $\mathfrak{o}/\mathfrak{a}$ and put

$N(\mathfrak{a})=N_1(\mathfrak{a})^{1/2}$; we can define in a natural manner $N(\mathfrak{a})$ and $N_1(\mathfrak{a})$ for any $\mathfrak{o}$-ideal which is not necessarily integral. $N(\mathfrak{a})$ is a positive integer for any integral $\mathfrak{o}$-ideal $\mathfrak{a}$; and we have

$$N(\alpha\mathfrak{o})=N(\mathfrak{o}\alpha)=|N(\alpha)|.$$

The two-sided $\mathfrak{o}$-ideals form a commutative group, which is a direct product of the infinite cyclic groups generated by the prime ideals. Every prime ideal $\mathfrak{p}$ divides one and only one rational prime p; and we have

$$\mathfrak{p}=p\mathfrak{o} \quad \text{if} \quad p \nmid d(\Phi),$$

$$\mathfrak{p}^2=p\mathfrak{o} \quad \text{if} \quad p \mid d(\Phi).$$

Therefore, every integral two-sided $\mathfrak{o}$-ideal $\mathfrak{a}$ is written in the form

$$\mathfrak{a}=a_0\mathfrak{p}_1\cdots\mathfrak{p}_s, \tag{3}$$

where a_0 is a rational integer and the $\mathfrak{p}_i$ are distinct prime ideals dividing $d(\Phi)$. By Eichler [**5**], every one-sided $\mathfrak{o}$-ideal is principal. For our later use, we state here a lemma which is a particular case of Eichler [**4**, Satz 5].

LEMMA 1.3. *Let $\mathfrak{a}$ be an integral two-sided $\mathfrak{o}$-ideal; let β be an element of $\mathfrak{o}$ and b an element of $\boldsymbol{Z}$ such that $b\equiv N(\beta)$ mod. $\mathfrak{a}$. Then there exists an element β_0 of $\mathfrak{o}$ such that*

$$\beta_0\equiv\beta \text{ mod. } \mathfrak{a}, \quad N(\beta_0)=b.$$

Taking $\mathfrak{a}$ to be $\mathfrak{o}$, we obtain

LEMMA 1.4. *For every rational integer b, there exists an element β of $\mathfrak{o}$ such that $N(\beta)=b$.*

1.3. Ring of modular correspondences. We denote by Γ the group of all units γ of $\mathfrak{o}$ such that $N(\gamma)=1$. By Lemma 1.4, $\mathfrak{o}$ contains an element ε such that $N(\varepsilon)=-1$; for any such element ε, $\Gamma\cup\Gamma\varepsilon$ is the group of all units in $\mathfrak{o}$. Let $\mathfrak{a}=\alpha\mathfrak{o}$ be an integral two-sided $\mathfrak{o}$-ideal; we denote by $\Gamma_{\mathfrak{a}}=\Gamma_\alpha$ the subgroup of Γ consisting of the elements γ such that $\gamma\equiv 1$ mod. $\mathfrak{a}$.

PROPOSITION 1.5. *Let α be an element of $\mathfrak{o}$ such that $N(\alpha)=m\neq 0$. Then $\alpha^{-1}\Gamma\alpha$ contains Γ_m.*

PROOF. If γ is an element of Γ_m, we have

$$\alpha\gamma\alpha^{-1}=\alpha\gamma\alpha'm^{-1}\equiv 1 \text{ mod. } \alpha\mathfrak{o}\alpha'.$$

This shows that $\alpha\gamma\alpha^{-1}$ is contained in $\mathfrak{o}$. As we have $N(\alpha\gamma\alpha^{-1})=1, \alpha\gamma\alpha^{-1}$ is contained in Γ, so that $\gamma\in\alpha^{-1}\Gamma\alpha$, Q. E. D.

It follows from Proposition 1.5 that, for every regular element α of Φ, Γ and $\alpha^{-1}\Gamma\alpha$ are commensurable. Let Δ (resp. Δ_0) be the set of all the elements α of Φ (resp. $\mathfrak{o}$) such that $N(\alpha)>0$. Now we shall consider the ring $\mathfrak{R}(\Gamma,\Delta)$.

Our first task is to characterize the double cosets $\Gamma\alpha\Gamma$ by their "elementary divisors". For every rational prime number p, let $\boldsymbol{Q}_p$ and $\boldsymbol{Z}_p$ denote respectively the field of p-adic numbers and the ring of p-adic integers; and put

$$\Phi_p = \Phi \otimes_{\boldsymbol{Q}} \boldsymbol{Q}_p, \quad \mathfrak{o}_p = \mathfrak{o} \otimes_{\boldsymbol{Z}} \boldsymbol{Z}_p. \tag{4}$$

If $p \nmid d(\Phi)$, Φ_p is isomorphic to the total matric algebra $\boldsymbol{M}_2(\boldsymbol{Q}_p)$ over $\boldsymbol{Q}_p$ of degree 2; and for a suitable choice of isomorphism, $\mathfrak{o}_p$ corresponds to the ring $\boldsymbol{M}_2(\boldsymbol{Z}_p)$ of matrices with entries in $\boldsymbol{Z}_p$. If $p \mid d(\Phi)$, Φ_p is a division algebra over $\boldsymbol{Q}_p$. For each prime factor p of $d(\Phi)$, we fix a prime element π_p in $\mathfrak{o}_p$, which satisfies $N(\pi_p) = p$.

Let α be an element of Δ_0. We now define the elementary divisors of α. First consider a prime p which does not divide $d(\Phi)$. Then, regarding α as an element of $\boldsymbol{M}_2(\boldsymbol{Z}_p)$, we can find two units ε_1 and ε_2 of $\boldsymbol{M}_2(\boldsymbol{Z}_p)$ so that $\varepsilon_1 \alpha \varepsilon_2$ is of the following form:

$$\varepsilon_1 \alpha \varepsilon_2 = \begin{pmatrix} p^{c_1} & 0 \\ 0 & p^{c_2} \end{pmatrix},$$

where c_1 and c_2 are non-negative integers such that $c_1 \leqq c_2$. When p divides $d(\Phi)$, $\mathfrak{o}_p \alpha$ is a power $(\mathfrak{o}_p \pi_p)^c$. We call then

$$\{ \cdots, (p^{c_1}, p^{c_2}), \cdots, \pi_p^c, \cdots \}$$

the *elementary divisors* of α.

PROPOSITION 1.6. *Let α and β be two elements of Δ_0. Then the following four conditions are equivalent to each other.*

i) $\Gamma \alpha \Gamma = \Gamma \beta \Gamma$.

ii) *α and β have the same elementary divisors.*

iii) *$\mathfrak{o}/\mathfrak{o}\alpha$ and $\mathfrak{o}/\mathfrak{o}\beta$ are isomorphic as $\mathfrak{o}$-modules.*

iv) *There exists an element γ of Γ such that $\mathfrak{o}\alpha\gamma = \mathfrak{o}\beta$.*

PROOF. The equivalences i)$\Leftrightarrow$iv), ii)$\Leftrightarrow$iii) and the implication i)$\Rightarrow$ii) are obvious. Therefore our proposition is proved if we show ii)$\Rightarrow$iv). Suppose the condition ii) holds. Then, for each prime p, we can find two units $\varepsilon_1^{(p)}, \varepsilon_2^{(p)}$ of $\mathfrak{o}_p$ such that $\varepsilon_1^{(p)} \alpha \varepsilon_2^{(p)} = \beta$. We may assume, without loss of generality, that $N(\varepsilon_1^{(p)}) = N(\varepsilon_2^{(p)}) = 1$; put $q = N(\alpha)$; we have clearly $N(\beta) = q$. We can find two elements a_1 and a_2 of $\mathfrak{o}$ such that, for every prime factor p of q,

$$a_1 \equiv \varepsilon_1^{(p)}, \quad a_2 \equiv \varepsilon_2^{(p)} \quad \mathrm{mod.}\, q\mathfrak{o}_p.$$

This relation holds for any p, since if p does not divide q, we have $q\mathfrak{o}_p = \mathfrak{o}_p$. Hence we have

$$N(a_1) \equiv N(a_2) \equiv 1 \ \mathrm{mod.}\, (q).$$

Now by Lemma 1.3, there exist two elements γ_1 and γ_2 of $\mathfrak{o}$ such that

$$N(\gamma_1) = N(\gamma_2) = 1,$$

$$\gamma_1 \equiv a_1, \quad \gamma_2 \equiv a_2 \quad \text{mod.}\, q\mathfrak{o}\,.$$

We have then $\gamma_1\alpha\gamma_2 \equiv \beta$ mod. $q\mathfrak{o}$. It follows that $\mathfrak{o}\alpha\gamma_2 = \mathfrak{o}\beta$ since both $\mathfrak{o}\alpha\gamma$ and $\mathfrak{o}\beta$ contain $q\mathfrak{o}$. We have thus proved ii)$\Rightarrow$iv).

We call the elementary divisors of α also the *elementary divisors* of $\Gamma\alpha\Gamma$ or of the integral left $\mathfrak{o}$-ideal $\mathfrak{o}\alpha$. It is easy to see that α and α' have the same elementary divisors; so by Proposition 1.6, we have $\Gamma\alpha\Gamma = \Gamma\alpha'\Gamma$; this holds not only for $\alpha \in \Delta_0$ but also for every $\alpha \in \Delta$. Applying Proposition 1.2 to the present case, we obtain

PROPOSITION 1.7. *The ring $\mathfrak{R}(\Gamma, \Delta)$ is commutative.*

We shall now determime the structure of $\mathfrak{R}(\Gamma, \Delta_0)$. It is easy to see that $\Gamma\alpha \rightarrow \mathfrak{o}\alpha$ gives a one-to-one correspondence between the right cosets contained in Δ_0 and the integral left $\mathfrak{o}$-ideals. By Proposition 1.6, $\Gamma\alpha$ and $\Gamma\beta$ belongs to the same double coset $\Gamma\alpha\Gamma$ if and only if $\mathfrak{o}/\mathfrak{o}\alpha$ and $\mathfrak{o}/\mathfrak{o}\beta$ are isomorphic. Thus we observe that $\deg(\Gamma\alpha\Gamma)$ is equal to the number of integral left $\mathfrak{o}$-ideals $\mathfrak{b}$ such that $\mathfrak{o}/\mathfrak{b}$ is isomorphic to $\mathfrak{o}/\mathfrak{o}\alpha$. In particular, when $N(\alpha) = p$ is a prime number, we have

$$\deg(\Gamma\alpha\Gamma) = \begin{cases} p+1 & \text{if } \ p \mid d(\Phi)\,, \\ 1 & \text{if } \ p \nmid d(\Phi)\,. \end{cases}$$

PROPOSITION 1.8. *Put $\sigma = \Gamma\alpha\Gamma, \tau = \Gamma\beta\Gamma, \rho = \Gamma\gamma\Gamma$. Then $\mu(\sigma\cdot\tau\,;\rho)$ is equal to the number of integral left $\mathfrak{o}$-ideals $\mathfrak{b}$ such that*: i) $\mathfrak{b} \supset \mathfrak{o}\gamma$; ii) $\mathfrak{o}/\mathfrak{b}$ *is isomorphic to* $\mathfrak{o}/\mathfrak{o}\beta$; iii) $\mathfrak{b}/\mathfrak{o}\gamma$ *is isomorphic to* $\mathfrak{o}/\mathfrak{o}\alpha$.

PROOF. Let $\Gamma\alpha\Gamma = \bigcup\Gamma\alpha_i$ and $\Gamma\beta\Gamma = \bigcup\Gamma\beta_k$ be disjoint sums. Then $\mu(\sigma\cdot\tau\,;\rho)$ is the number of (i, k) such that $\Gamma\alpha_i\beta_k = \Gamma\gamma$. We note that, for each k, there exists only one or no i such that $\Gamma\alpha_i\beta_k = \Gamma\gamma$. Now if $\Gamma\alpha_i\beta_k = \Gamma\gamma$ holds, we have $\mathfrak{o} \supset \mathfrak{o}\beta_k \supset \mathfrak{o}\alpha_i\beta_k = \mathfrak{o}\gamma$; and $\mathfrak{o}/\mathfrak{o}\beta_k$ is isomorphic to $\mathfrak{o}/\mathfrak{o}\beta$, and $\mathfrak{o}\beta_k/\mathfrak{o}\gamma$ is isomorphic to $\mathfrak{o}/\mathfrak{o}\alpha$; so the integral left $\mathfrak{o}$-ideal $\mathfrak{o}\beta_k$ satisfies the conditions i, ii, iii). Conversely, suppose that an integral left $\mathfrak{o}$-ideal $\mathfrak{b}$ satisfies i, ii, iii). By ii), we have $\mathfrak{b} = \mathfrak{o}\beta_k$ for some k. Put $\gamma\beta_k^{-1} = \alpha_0$; we have then $\alpha_0 \in \Delta_0$, and, by virtue of iii), $\mathfrak{o}/\mathfrak{o}\alpha_0$ is isomorphic to $\mathfrak{o}/\mathfrak{o}\alpha$. We have therefore $\Gamma\alpha_0 = \Gamma\alpha_i$ for some i. It follows that $\Gamma\alpha_i\beta_k = \Gamma\gamma$. This proves our proposition.

PROPOSITION 1.9. *If $N(\alpha)$ and $N(\beta)$ are relatively prime,*

$$(\Gamma\alpha\Gamma)(\Gamma\beta\Gamma) = \Gamma\alpha\beta\Gamma\,.$$

PROOF. Using the same notation as in the preceding proposition, assume that $N(\alpha)$ and $N(\beta)$ are relatively prime. Let $\mathfrak{b}_1$ and $\mathfrak{b}_2$ be integral left $\mathfrak{o}$-ideals satisfying the conditions i, ii, iii). By ii), $\mathfrak{b}_1+\mathfrak{b}_2/\mathfrak{b}_2$ is isomorphic to a submodule of $\mathfrak{o}/\mathfrak{o}\beta$. On the other hand, $\mathfrak{b}_1/\mathfrak{b}_1\cap\mathfrak{b}_2$ is isomorphic to a submodule of $\mathfrak{o}/\mathfrak{o}\alpha$. Hence we must have $\mathfrak{b}_1+\mathfrak{b}_2 = \mathfrak{b}_2, \mathfrak{b}_1 = \mathfrak{b}_1\cap\mathfrak{b}_2$, namely, $\mathfrak{b}_1 = \mathfrak{b}_2$. This proves $\mu(\sigma\cdot\tau\,;\rho) = 1$ by virtue of Proposition 1.8. It is easy to see that, for every

$\alpha_1 \in \Gamma\alpha\Gamma$ and $\beta_1 \in \Gamma\beta\Gamma$, the element $\alpha_1\beta_1$ have the same elementary divisors as $\alpha\beta$. Hence $(\Gamma\alpha\Gamma)(\Gamma\beta\Gamma)$ has the only component $\Gamma\alpha\beta\Gamma$; this proves our proposition.

Now fix our attention to one prime number p. We observe that the $\Gamma\alpha\Gamma$, for which $N(\alpha)$ is a power of p, generate a subring of $\mathfrak{R}(\Gamma, \Delta_0)$, which we denote by $\mathfrak{R}_p$. Let $T(p^m)$ be the sum of $\Gamma\alpha\Gamma$ such that $N(\alpha)=p^m$. If p is a factor of $d(\Phi)$, we have $T(p^m)=T(p)^m$, so that the ring $\mathfrak{R}_p$ is the polynomial ring $\boldsymbol{Z}[T(p)]$. Now suppose that p does not divide $d(\Phi)$. Let $T(p^\lambda, p^\mu)$ denote the element $\Gamma\alpha\Gamma$ of $\mathfrak{R}_p$ whose elementary divisors are (p^λ, p^μ).

PROPOSITION 1.10. *If $p \nmid d(\Phi)$, the following relations hold.*

$$T(p,p)T(p^\lambda, p^\mu) = T(p^{\lambda+1}, p^{\mu+1}). \tag{5}$$

$$T(p)T(p^m) = T(1, p^{m+1}) + (p+1)T(p,p)T(p^{m-1}) \quad \textit{for} \quad m \geqq 1. \tag{6}$$

PROOF. The first equality is obvious. Let $c_{\lambda\mu}$ be the multiplicity of $T(p^\lambda, p^\mu)$ in the product $T(1,p)T(p^m)$. Fix an element $\alpha_{\lambda\mu}$ of $\mathfrak{o}$ whose elementary divisors are (p^λ, p^μ). Then, by Proposition 1.8, $c_{\lambda\mu}$ is the number of integral left $\mathfrak{o}$-ideals $\mathfrak{b}$ such that: i) $\mathfrak{b} \supset \mathfrak{o}\alpha_{\lambda\mu}$; ii) $\mathfrak{o}/\mathfrak{b}$ is isomorphic to $\mathfrak{o}/\mathfrak{o}\alpha_{01}$. If $1 \leqq \lambda \leqq \mu$, $\mathfrak{o}\alpha_{\lambda\mu}$ is contained in $p\mathfrak{o}$; so in this case, the condition i) is a consequence of ii), so that we have $c_{\lambda\mu}=p+1$. If $\lambda=0$, we have $\mu=m+1$; in this case, $\mathfrak{o}\alpha_{0\mu}$ is not contained in $p\mathfrak{o}$; hence we must have $\mathfrak{b}=\mathfrak{o}\alpha_{0\mu}+p\mathfrak{o}$. This implies $c_{0\mu}=1$. The relation (6) follows from these facts.

We can also verify that

$$T(1,p)T(1,p^m) = T(1,p^{m+1}) + \begin{cases} pT(p,p^m) & (m>1), \\ (p+1)T(p,p) & (m=1), \end{cases}$$

$$\deg(T(1,p^m)) = p^{m-1}(p+1) \qquad (m \geqq 1);$$

and the ring $\mathfrak{R}_p$ is the polynomial ring $\boldsymbol{Z}[T(1,p), T(p,p)]$. It follows that the ring $\mathfrak{R}(\Gamma, \Delta)$ is an integral domain.

PROPOSITON 1.11. *Let $T(n)$ be the sum of $\Gamma\alpha\Gamma$ for $\alpha \in \Delta_0$, $N(\alpha)=n$. Then, the formal Dirichlet-series $\sum_{n=1}^{\infty} T(n)n^{-s}$ is decomposed into an Euler-product:*

$$\sum_{n=1}^{\infty} T(n)n^{-s} = \prod_{p \mid d(\Phi)} [1-T(p)p^{-s}]^{-1} \prod_{p \nmid d(\Phi)} [1-T(p)p^{-s}+T(p,p)p^{1-2s}]^{-1}.$$

PROOF. By Proposition 1.9, we have $\sum_{n=1}^{\infty} T(n)n^{-s} = \prod_p (\sum_{m=0}^{\infty} T(p^m)p^{-ms})$. If p is a factor of $d(\Phi)$, we have

$$\sum_{m=0}^{\infty} T(p^m)p^{-ms} = \sum_{m=0}^{\infty} (T(p)p^{-s})^m = [1-T(p)p^{-s}]^{-1}.$$

Now suppose that p does not divide $d(\Phi)$; putting $X=p^{-s}$, we observe

$$\sum_{m=0}^{\infty} T(p^m)X^m = 1+\sum_{m=1}^{\infty} T(1,p^m)X^m + T(p,p)X^2 \sum_{\nu=0}^{\infty} T(p^\nu)X^\nu .$$

Then, by Proposition 1.10, we can easily verify

$$[1-T(1,p)X+pT(p,p)X^2]\sum_{m=0}^{\infty} T(p^m)X^m = 1 .$$

Our proposition is thereby proved.

By Proposition 1.11, we see easily

(7) $$\deg T(n) = \sum{}' d ,$$

where the sum is extended over all positive divisors d of n which are prime to $d(\Phi)$.

1.4. Congruence-subgroups of Γ. We begin with

PROPOSITION 1.12. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be integral two-sided $\mathfrak{o}$-ideals which are relatively prime. Then we have $\Gamma = \Gamma_{\mathfrak{a}}\Gamma_{\mathfrak{b}}$.*

PROOF. Let α be an element of Γ. We can find an element β of $\mathfrak{o}$ such that $\beta \equiv 1 \bmod. \mathfrak{b}$ and $\beta \equiv \alpha \bmod. \mathfrak{a}$. We have then $N(\beta) \equiv 1 \bmod. \mathfrak{a}\mathfrak{b}$. By Lemma 1.3, there exists an element γ of Γ such that $N(\gamma)=1$ and $\gamma \equiv \beta \bmod. \mathfrak{a}\mathfrak{b}$. As $\gamma \equiv \beta \equiv 1 \bmod. \mathfrak{b}, \gamma$ is contained in $\Gamma_{\mathfrak{b}}$; and as $\gamma \equiv \alpha \bmod. \mathfrak{a}, \alpha\gamma^{-1}$ is contained in $\Gamma_{\mathfrak{a}}$. We have therefore $\alpha = \alpha\gamma^{-1}\cdot\gamma \in \Gamma_{\mathfrak{a}}\Gamma_{\mathfrak{b}}$; this proves our proposition.

Now we fix an integral two-sided $\mathfrak{o}$-ideal $\mathfrak{a}$.

PROPOSITION 1.13. *Let α and β be two elements of Δ_0 whose norms are prime to $\mathfrak{a}$. Then we have $\Gamma_{\mathfrak{a}}\alpha = \Gamma_{\mathfrak{a}}\beta$ if and only if $\Gamma\alpha = \Gamma\beta$ and $\alpha \equiv \beta$* mod. $\mathfrak{a}$.

This is an easy consequence of the definition of $\Gamma_{\mathfrak{a}}$.

PROPOSITION 1.14. *Let α be an element of Δ_0 such that $N(\alpha)$ is prime to $\mathfrak{a}$. Then the following assertions hold.*

i) $\Gamma\alpha\Gamma = \Gamma\alpha\Gamma_{\mathfrak{a}} = \Gamma_{\mathfrak{a}}\alpha\Gamma$.

ii) $\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}} = \{\beta \mid \beta \in \Gamma\alpha\Gamma, \beta \equiv \alpha \bmod. \mathfrak{a}\}$.

iii) *If $\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}} = \bigcup_{\nu} \Gamma_{\mathfrak{a}}\alpha_\nu$ is a disjoint sum, then $\Gamma\alpha\Gamma = \bigcup_{\nu} \Gamma\alpha_\nu$ is a disjoint sum.*

PROOF. By Propositions 1.5 and 1.12 we have $\Gamma = (\Gamma \cap \alpha^{-1}\Gamma\alpha)\Gamma_{\mathfrak{a}}$. Multiplying by $\alpha^{-1}\Gamma\alpha$, we obtain $\alpha^{-1}\Gamma\alpha\Gamma = \alpha^{-1}\Gamma\alpha\Gamma_{\mathfrak{a}}$, so that $\Gamma\alpha\Gamma = \Gamma\alpha\Gamma_{\mathfrak{a}}$; the relation $\Gamma\alpha\Gamma = \Gamma_{\mathfrak{a}}\alpha\Gamma$ is similarly proved. The assertions ii, iii) follow from this and Proposition 1.13.

Now let $\Delta_{\mathfrak{a}}$ be the subset of Δ_0 consisting of the elements whose norms are prime to $\mathfrak{a}$. Assume that $\mathfrak{a}$ *is prime to $d(\Phi)$*. Then we have $\mathfrak{a} = a\mathfrak{o}$ for a positive integer a; and $\mathfrak{o}/\mathfrak{a}$ is isomorphic to the total matric ring of degree 2 over $\boldsymbol{Z}/a\boldsymbol{Z}$. Identifying $\mathfrak{o}/\mathfrak{a}$ with the matric ring, let $\Delta_{\mathfrak{a}}^{*}$ be the set of elements α in $\Delta_{\mathfrak{a}}$ such that

$$(8) \qquad \alpha \equiv \begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix} \quad \text{mod. } \mathfrak{a}.$$

If the relation (8) holds, we have clearly $N(\alpha) \equiv c$ mod. $\mathfrak{a}$.

PROPOSITION 1.15. *Notations and assumptions being as above, the correspondence $\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}} \rightarrow \Gamma\alpha\Gamma$ gives a surjective isomorphism of $\mathfrak{R}(\Gamma_{\mathfrak{a}}, \Delta_{\mathfrak{a}}^{*})$ onto $\mathfrak{R}(\Gamma, \Delta_{\mathfrak{a}})$*

PROOF. Denote by φ the linear mapping of $\mathfrak{R}(\Gamma_{\mathfrak{a}}, \Delta_{\mathfrak{a}}^{*})$ into $\mathfrak{R}(\Gamma, \Delta)$ given by the correspondence. First we prove that φ is surjective. Let α be an element of $\Delta_{\mathfrak{a}}$; put $N(\alpha) = c$. As c is prime to $\mathfrak{a}$, there exists an integer b such that $bc \equiv 1$ mod. $\mathfrak{a}$. Let β be an element of $\mathfrak{o}$ such that $\beta \equiv \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix}$ mod. $\mathfrak{a}$. Then we have $N(\alpha\beta) \equiv 1$ mod. $\mathfrak{a}$. By Lemma 1.3, there exists an elemet γ of Γ such that $\gamma \equiv \alpha\beta$ mod. $\mathfrak{a}$. We have then $\gamma^{-1}\alpha \equiv \begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix}$ mod. $\mathfrak{a}$, so that $\gamma^{-1}\alpha$ is contained in $\Delta_{\mathfrak{a}}^{*}$. This proves that φ is surjective. Suppose that $\Gamma\alpha\Gamma = \Gamma\beta\Gamma$ for two elements α, β of $\Delta_{\mathfrak{a}}^{*}$. Since $N(\alpha)$ is equal to $N(\beta)$, we get $\alpha \equiv \beta$ mod. $\mathfrak{a}$, so that by ii) of Proposition 1.14, we obtain $\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}} = \Gamma_{\mathfrak{a}}\beta\Gamma_{\mathfrak{a}}$; this proves that φ is one-to-one. Now let $\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}} = \bigcup \Gamma_{\mathfrak{a}}\alpha_i$ and $\Gamma_{\mathfrak{a}}\beta\Gamma_{\mathfrak{a}} = \bigcup_{k} \Gamma_{\mathfrak{a}}\beta_k$ be disjoint sums for $\alpha, \beta \in \Delta_{\mathfrak{a}}^{*}$. We have then $\Gamma\alpha\Gamma = \bigcup \Gamma\alpha_i$ and $\Gamma\beta\Gamma = \bigcup \Gamma\beta_k$; and these are disjoint sums by virtue of iii) of Proposition 1.14. The product $(\Gamma\alpha\Gamma)(\Gamma\beta\Gamma)$ in the ring $\mathfrak{R}(\Gamma, \Delta_{\mathfrak{a}})$ is a linear combination of the $\Gamma\alpha_i\beta_k\Gamma$. Fix a pair (λ, ν) and put $\gamma = \alpha_\lambda\beta_\nu$. If we have $\Gamma_{\mathfrak{a}}\alpha_i\beta_k = \Gamma_{\mathfrak{a}}\gamma$, then obviously $\Gamma\alpha_i\beta_k = \Gamma\gamma$. Conversely, suppose that $\Gamma\alpha_i\beta_k = \Gamma\gamma$. As $\alpha_i \equiv \alpha_\lambda$ and $\beta_k \equiv \beta_\nu$ mod. $\mathfrak{a}$, we have $\alpha_i\beta_k \equiv \gamma$ mod. $\mathfrak{a}$. Hence by Proposition 1.13, we obtain $\Gamma_{\mathfrak{a}}\alpha_i\beta_k \equiv \Gamma_{\mathfrak{a}}\gamma$. This proves that φ is an isomorphism.

The ring $\mathfrak{R}(\Gamma, \Delta)$ was first introduced by Hecke [**12**] in the case where Φ is the total matric ring $\boldsymbol{M}_2(\boldsymbol{Q})$; this is generalized by Eichler [**7**] to the case of quaternion algebra. Recently, Tamagawa [**26**] has given a theory for arbitrary division algebras over $\boldsymbol{Q}$. The result of §§ 1.3-4 is essentially contained in these works. Hecke considered, in the case $\Phi = \boldsymbol{M}_2(\boldsymbol{Q})$, the representation of $T(n)$ by modular forms and constructed Dirichlet-series whose coefficients are those representations of $T(n)$; the series have Euler-products and satisfy functional equations; this work was completed by Petersson [**17**]. Eichler [**7**] and Selberg (unpublished?) considered a similar problem in the case of quaternion algebras. Tamagawa treated the case of general division algebras; his work is, however, concerned with automorphic "functions" but not with "forms". On the other hand, Godement [**10**] gave a fairly general theory of zeta-functions attached to division algebras, which is applicable to both the cases "functions" and "forms"; but in this work, there remain unexplained some essential aspects in the case of automorphic forms. Therefore, we shall now give a treatment in the case of automorphic forms attached to quaternion algebras.

REMARK. Prof. Eichler kindly communicated to the author that $\mathrm{tr}(T(n))$ in the case of division quaternion algebra is a linear combination of similar traces in the classical case; this would be another way to Theorem 1 of §1.6.

1.5. Cusp-forms. Let $\mathfrak{H}$ denote the upper half-plane. For every matrix $x=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with real entries and for $z\in \boldsymbol{C}$, we shall put

$$j(x, z)=cz+d\,.$$

And when $\det x\neq 0$, we put

$$x[z]=\frac{az+b}{cz+d}\,;$$

we have then, if $\det x\neq 0$ and $\det y\neq 0$,

$$j(xy, z)=j(x, y[z])j(y, z)\,.$$

If $\det x>0, z\rightarrow x[z]$ gives an analytic automorphism of $\mathfrak{H}$.

Fix once for all a faithful representation χ of Φ by real matrices of degree 2. We identify every element ξ of Φ with the matrix $\chi(\xi)$; then the notation $\xi[z]$ does not contradict the one introduced in [AF, no. 21].

$\Gamma_{\mathfrak{a}}$ being as in § 1.2, we call as usual a function $f(z)$ on $\mathfrak{H}$ a *cusp-form of degree* κ *with respect to* $\Gamma_{\mathfrak{a}}$, where κ is a positive integer, if:

i) *$f(z)$ is holomorphic on* $\mathfrak{H}$;

ii) *$f(\sigma[z])j(\sigma, z)^{-\kappa}=f(z)$ for every $\sigma\in\Gamma_{\mathfrak{a}}$*;

iii) *$f(z)$ vanishes at every cusp of $\Gamma_{\mathfrak{a}}$.*

We denote by $S_{\kappa}(\Gamma_{\mathfrak{a}})$ the set of such $f(z)$. Let $\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}}=\bigcup\Gamma_{\mathfrak{a}}\alpha_{\nu}$ be a disjoint expression of an element of $\mathfrak{R}(\Gamma_{\mathfrak{a}}, \Delta)$. For every $f\in S_{\kappa}(\Gamma_{\mathfrak{a}})$, we define a function g by

$$g(z)=N(\alpha)^{\kappa-1}\sum_{\nu} f(\alpha_{\nu}[z])j(\alpha_{\nu}, z)^{-\kappa}\,.$$

It can be easily verified that g is an element of $S_{\kappa}(\Gamma_{\mathfrak{a}})$ and does not depend on the choice of $\{\alpha_{\nu}\}$. We denote by $(\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}})_{\kappa}$ the linear mapping $f\rightarrow g$ of $S_{\kappa}(\Gamma_{\mathfrak{a}})$ into itself thus obtained, and write $g=f\,|\,(\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}})_{\kappa}$. By our definition of $\mathfrak{R}(\Gamma_{\mathfrak{a}}, \Delta)$ we can conclude that $\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}}\rightarrow(\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}})_{\kappa}$ is a representation of the ring $\mathfrak{R}(\Gamma_{\mathfrak{a}}, \Delta)$ in the vector space $S_{\kappa}(\Gamma_{\mathfrak{a}})$. We shall give another expression for $(\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}})_{\kappa}$. Put $\alpha_{\nu}'=\beta_{\nu}$ for each ν. We have then $\Gamma_{\mathfrak{a}}\alpha'\Gamma_{\mathfrak{a}}=\bigcup_{\nu}\beta_{\nu}\Gamma_{\mathfrak{a}}$; and as $\alpha_{\nu}=N(\alpha)\beta_{\nu}^{-1}$, we get $f(\alpha_{\nu}[z])=f(\beta_{\nu}^{-1}[z])$ and $j(\alpha_{\nu}, z)=N(\alpha)j(\beta_{\nu}^{-1}, z)$. Hence,

$$f\,|\,(\Gamma_{\mathfrak{a}}\alpha\Gamma_{\mathfrak{a}})_{\kappa}=N(\alpha)^{-1}\sum_{\nu} f(\beta_{\nu}^{-1}[z])j(\beta_{\nu}^{-1}, z)^{-\kappa}\,. \tag{9}$$

If b is a positive integer, we see easily

$$f\,|\,(\Gamma_{\mathfrak{a}}b\Gamma_{\mathfrak{a}})_{\kappa}=b^{\kappa-2}f\,. \tag{10}$$

Let $\{f_1, \cdots, f_m\}$ be a base of $S_\kappa(\Gamma_\mathfrak{a})$ over $\boldsymbol{C}$ and $\boldsymbol{f}$ be the column-vector whose components are $f_1, \cdots, f_m$. Then, for every element $\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a}$ of $\mathfrak{R}(\Gamma_\mathfrak{a}, \Delta)$, we obtain a matrix $\mathfrak{T}_\kappa(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})$ with entries in $\boldsymbol{C}$ such that

$$(11) \qquad \boldsymbol{f} \,|\, (\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})_\kappa = \mathfrak{T}_\kappa(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})\boldsymbol{f}\,.$$

Restricting α to Γ, we observe that $\alpha \rightarrow \mathfrak{T}_\kappa(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})$ gives a representation of Γ, whose kernel contains $\Gamma_\mathfrak{a}$; we denote $\mathfrak{T}_\kappa(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})$ simly by $L(\alpha)$ for every $\alpha \in \Gamma$.

Now suppose that $\mathfrak{a}$ is prime to $d(\Phi)$. For every integer b which is prime to $\mathfrak{a}$, we can find, by Lemma 1.3, an element γ of Γ such that $\gamma \equiv \begin{pmatrix} b^{-1} & 0 \\ 0 & b \end{pmatrix} \bmod. \mathfrak{a}$; and $L(\gamma)$ is determined only by b; so we put

$$(12) \qquad R_\kappa(b\,;\mathfrak{a}) = L(\gamma)\,.$$

$T(n)$ and $T(p,p)$ being as in § 1.3, let $T(n\,;\mathfrak{a})$ and $T(p,p\,;\mathfrak{a})$ be the elements of $\mathfrak{R}(\Gamma_\mathfrak{a}, \Delta_\mathfrak{a}^*)$ corresponding to $T(n)$ and $T(p,p)$ by the isomorphism of Proposition 1.15. Denote by $\mathfrak{T}_\kappa(n\,;\mathfrak{a})$ and $\mathfrak{T}_\kappa(p,p\,;\mathfrak{a})$ the matrices determined for $T(n\,;\mathfrak{a})$ and $T(p,p\,;\mathfrak{a})$ as in (11). If γ is an element of Γ such that $\gamma \equiv \begin{pmatrix} p^{-1} & 0 \\ 0 & p \end{pmatrix} \bmod. \mathfrak{a}$, we have $p\gamma = \begin{pmatrix} 1 & 0 \\ 0 & p^2 \end{pmatrix} \bmod. \mathfrak{a}$, so that $T(p,p\,;\mathfrak{a}) = \Gamma_\mathfrak{a} p\gamma \Gamma_\mathfrak{a}$. Using the relations (10) and (12), we obtain $\mathfrak{T}_\kappa(p,p\,;\mathfrak{a}) = p^{\kappa-2}R_\kappa(p\,;\mathfrak{a})$. Therefore, by Propositions 1.11 and 1.15, we get (formally for the moment)

$$(13) \qquad \textstyle\sum' \mathfrak{T}_\kappa(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})N(\alpha)^{-s} = \displaystyle\sum_{(n,\mathfrak{a})=1} \mathfrak{T}_\kappa(n\,;\mathfrak{a})n^{-s}$$
$$= \prod_{p\,|\,d} [1 - \mathfrak{T}_\kappa(p\,;\mathfrak{a})p^{-s}]^{-1} \prod_{p \nmid d\mathfrak{a}} [1 - \mathfrak{T}_\kappa(p\,;\mathfrak{a})p^{-s} + R_\kappa(p\,;\mathfrak{a})p^{\kappa-1-2s}]^{-1}\,,$$

where $d = d(\Phi)$, and the first sum is extended over all $\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a}$ with $\alpha \in \Delta_\mathfrak{a}^*$. In order to examine the convergence, define, for every $f \in S_\kappa(\Gamma_\mathfrak{a})$, a function f^* on $G_0 = \mathrm{SL}(2, \boldsymbol{R})$ by $f^*(u) = f(u[i])j(u, i)^{-\kappa}$, where $i = \sqrt{-1}$. Then, we can easily verify $f^*(\gamma u) = f^*(u)$ for every $\gamma \in \Gamma_\mathfrak{a}$; and if $g = f \,|\, (\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})_\kappa$, we have

$$(14) \qquad g^*(u) = N(\alpha)^{\kappa-1} \sum_\nu f^*(\alpha_\nu u)\,,$$

the α_ν being as above. We may consider f^* as function on $\Gamma_\mathfrak{a}\backslash G_0$. Since $\Gamma_\mathfrak{a}\backslash G_0$ is compact, f^* attains its maximum at some point of G_0. Hence, using the relation (14), we observe that the absolute values of the characteristic roots of $\mathfrak{T}_\kappa(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})$ do not exceed $N(\alpha)^{\kappa-1} \deg(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})$. As we shall see a little later, for a suitable base of $S_\kappa(\Gamma_\mathfrak{a})$, the $\mathfrak{T}_\kappa(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})$ become diagonal matrices. Therefore, on account of (7), the Dirichlet-series (13) converges absolutely for $\mathrm{Re}(s) > \kappa + 1$.

For our later use, it is necessary to consider an operator defined by an element with negative norm. Let ε be a unit of $\mathfrak{o}$ such that $N(\varepsilon) = -1$. For every $f \in S_\kappa(\Gamma_\mathfrak{a})$, define $g = f \,|\, T(\varepsilon)_\kappa$ by

$$(15) \qquad g(z) = \overline{f(\varepsilon[\bar{z}])}\,j(\varepsilon, z)^{-\kappa}\,,$$

where bars indicate the complex conjugate. It can be easily verified that $T(\varepsilon)_\kappa$ is an $\boldsymbol{R}$-linear mapping of $S_\kappa(\Gamma_\mathfrak{a})$ onto itself satisfying $(af)\,|\,T(\varepsilon)_\kappa = \bar{a}(f\,|\,T(\varepsilon)_\kappa)$ for $a \in \boldsymbol{C}$. When $\mathfrak{a}$ is prime to $d(\Phi)$, we can take ε so that $\varepsilon \equiv \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \bmod. \mathfrak{a}$. Then we have $\varepsilon^2 \in \Gamma_\mathfrak{a}, \varepsilon^{-1}\alpha\varepsilon \equiv \alpha \bmod. \mathfrak{a}$ for every $\alpha \in \varDelta_\mathfrak{a}^*$. Therefore, $T(\varepsilon)_\kappa^2 = 1$ and $T(\varepsilon)_\kappa$ commutes with $(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})_\kappa$ for every $\alpha \in \varDelta_\mathfrak{a}^*$.

After Petersson [**17**], we define the inner product of the elements f and g of $S_\kappa(\Gamma_\mathfrak{a})$ by

$$(f, g) = \int_D f(z)\overline{g(z)}\,\mathrm{Im}\,(z)^{\kappa-2}\,|\,dzd\bar{z}\,|\,,$$

where D is a fundamental domain for $\Gamma_\mathfrak{a}$. Then, by Proposition 2 of [**24**], $T^* = (\Gamma_\mathfrak{a}\alpha'\Gamma_\mathfrak{a})_\kappa$ is the adjoint of $T = (\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})_\kappa$; namely, we have $(f\,|\,T, g) = (f, g\,|\,T^*)$. Let α be an element of $\varDelta_\mathfrak{a}^*$; put $N(\alpha) = b$. Let γ be an element of Γ such that $\gamma \equiv \begin{pmatrix} b^{-1} & 0 \\ 0 & b \end{pmatrix} \bmod. \mathfrak{a}$. We have then $\alpha'\gamma \equiv \gamma\alpha' \equiv \alpha \bmod. \mathfrak{a}$, so that

$$\mathfrak{T}_\kappa(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a}) = R_\kappa(N(\alpha)\,;\mathfrak{a})\mathfrak{T}_\kappa(\Gamma_\mathfrak{a}\alpha'\Gamma_\mathfrak{a}) = \mathfrak{T}_\kappa(\Gamma_\mathfrak{a}\alpha'\Gamma_\mathfrak{a})R_\kappa(N(\alpha)\,;\mathfrak{a})\,. \tag{16}$$

If follows that $(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})_\kappa$ commutes with its adjoint. Therefore, the operators $(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})_\kappa$ for $\alpha \in \varDelta_\mathfrak{a}^*$ form a commutative ring of normal operators. Therefore, we can find a base of $S_\kappa(\Gamma_\mathfrak{a})$ with respect to which $(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})_\kappa$ is represented by a diagonal matrix for every $\alpha \in \varDelta_\mathfrak{a}^*$. By Theorem 3 of [**24**], the characteristic roots of $(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})_\kappa$ are algebraic integers for every even κ and every $\alpha \in \varDelta_0$; they are totally real if $\mathfrak{a} = \mathfrak{o}$. Furthermore, we can find a base $\{f_1, \cdots, f_m\}$ of $S_\kappa(\Gamma_\mathfrak{a})$ whose members are invariant under $T(\varepsilon)_\kappa$. With respect to this base, *the* $(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})_\kappa$ *are represented by real matrices for all* $\alpha \in \varDelta_\mathfrak{a}^*$.

1.6. Functional equations for Dirichlet-series. Our method is the one due to Iwasawa-Tate; besides we shall use the ideas of Fujisaki [**9**], Godement [**10**] and Tamagawa [**26**].

We assume, until the end of this §, that Φ is a division algebra. Let $\mathfrak{A}$ and $\mathfrak{J}$ denote respectively the adèle-ring and the idèle-group of the quaternion algebra Φ; we identify, in the usual manner, Φ with a subring of $\mathfrak{A}$ and the multiplicative group Φ^* of Φ with a subgroup of $\mathfrak{J}$. For every $x \in \mathfrak{A}$, we denote by x_p the p-component of x; in particular, x_∞ will denote the component at the infinite prime. Let $\mathfrak{d}_p$ be the different of $\mathfrak{o}_p$ with respect to $\boldsymbol{Z}_p$. Define a Haar measure dm_p of the additive group Φ_p by the condition $m_p(\mathfrak{o}_p) = N_1(\mathfrak{d}_p)^{-\frac{1}{2}}$ for each finite prime p, where $N_1(\mathfrak{d}_p)$ denotes the number of elements in $\mathfrak{o}_p/\mathfrak{d}_p$; and define a Haar measure dm_∞ of $\Phi_\infty = \boldsymbol{M}_2(\boldsymbol{R})$ by the usual Euclidean volume element. Then the product $dm(x) = \prod_p dm_p(x)$ gives a Haar measure on $\mathfrak{A}$ satisfying $m(\mathfrak{A}/\Phi) = 1$. For every element a of $\mathfrak{J}$, we define a positive number $|\,a\,|$ by

$$dm(ax) = |\,a\,|^2 dm(x)\,.$$

$|a|$ is also given by $|a|=\prod_p |N(a_p)|_p$, where N denotes as before the reduced norm. Let U_p be the group of units of $\mathfrak{o}_p$; define a Haar measure dm_p^* of the multiplicative group Φ_p^* by $m_p^*(U_p)=1$. Take and fix any Haar measure dm_∞^* on $\Phi_\infty^*=\mathrm{GL}(2, \boldsymbol{R})$; then the product $dm^*(x)=\prod_p dm_p^*(x_p)$ gives a Haar measure on $\mathfrak{J}$ and we have $dm^*(x)=c\,|x|^{-2}dm(x)$ for a suitable constant c. We shall write

$$\begin{aligned} &G=\mathrm{GL}(2, \boldsymbol{R}),\\ &G_+=\{x \mid x\in \mathrm{GL}(2, \boldsymbol{R}), \det x>0\},\\ &K=\mathrm{SO}(2, \boldsymbol{R}),\\ &U=U_0\times G;\quad U_0=\prod_{p\,;\,\text{finite}} U_p\,. \end{aligned}$$

We want to express the Dirichlet-series (13) by an integral on the idèle-group $\mathfrak{J}$. Let $\mathfrak{a}$ be an integral two-sided $\mathfrak{o}$-ideal which is prime to $d(\Phi)$. We denote by $\mathfrak{G}_\mathfrak{a}$ the group of regular elements of the ring $\mathfrak{o}/\mathfrak{a}$ and by $\mathfrak{S}_\mathfrak{a}$ the subgroup of $\mathfrak{G}_\mathfrak{a}$ consisting of the residue-classes of the elements α such that $N(\alpha)\equiv 1 \bmod \mathfrak{a}$. Let $U_\mathfrak{a}$ be the subgroup of U consisting of the elements u such that $u_p\equiv 1 \bmod \mathfrak{a}_p$, where $\mathfrak{a}_p=\mathfrak{o}_p\mathfrak{a}$. Then, $U/U_\mathfrak{a}$ is canonically isomorphic to $\mathfrak{G}_\mathfrak{a}$; and as $\mathfrak{a}$ is prime to $d(\Phi)$, $\mathfrak{G}_\mathfrak{a}$ is isomorphic to the group of matrices with entries in $\boldsymbol{Z}/(\boldsymbol{Z}\cap\mathfrak{a})$. Fixing such an isomorphism, let $\mathfrak{K}$ denote the subgroup of $\mathfrak{G}_\mathfrak{a}$ consisting of the elements of the form $\begin{pmatrix} c & 0\\ 0 & 1\end{pmatrix}$. Then every element x of $\mathfrak{G}_\mathfrak{a}$ is written uniquely in the following form:

(17) $$x=x_1x_2,\quad x_1\in\mathfrak{S}_\mathfrak{a},\quad x_2\in\mathfrak{K}\,.$$

Fix a unit ε of $\mathfrak{o}$ such that $N(\varepsilon)=-1$ and $\varepsilon\equiv\begin{pmatrix} -1 & 0\\ 0 & 1\end{pmatrix} \bmod \mathfrak{a}$. Let $\{f_1,\cdots,f_m\}$ be a base of $S_\kappa(\Gamma_\mathfrak{a})$ over $\boldsymbol{C}$ whose members are invariant under $T(\varepsilon)_\kappa$; and denote by $\boldsymbol{f}$ the column-vector with the components $f_1,\cdots,f_m$. Then, as is seen in the preceding section, we obtain a representation $L(\gamma)$ of Γ by $\boldsymbol{f}(\gamma[z])j(\gamma, z)^{-\kappa}=L(\gamma)\boldsymbol{f}$; and $L(\gamma)=1$ for $\gamma\in\Gamma_\mathfrak{a}$. Now by Lemma 1.3, $\Gamma/\Gamma_\mathfrak{a}$ is canonically isomorphic to $\mathfrak{S}_\mathfrak{a}$. Hence we can consider L as a representation of $\mathfrak{S}_\mathfrak{a}$; so, for every element x of $\mathfrak{G}_\mathfrak{a}$ of the form (17), we define $L^*(x)$ by

$$L^*(x)=L(x_1)^{-1}.$$

Furthermore, using the isomorphism $u\to x$ of $U/U_\mathfrak{a}$ onto $\mathfrak{G}_\mathfrak{a}$, we define

$$L^*(u)=L^*(x)\,.$$

$L^*(u)$ is not necessarily a representation of U; only we have

(18) $$L^*(\gamma u)=L^*(u)L(\gamma)^{-1}$$

for every $\gamma\in\Gamma$. Define a column-vector function $\boldsymbol{f}_0$ on U by

$$\boldsymbol{f}_0(u)=\begin{cases} L^*(u)\boldsymbol{f}(u_\infty[i])j(u_\infty,i)^{-\kappa} & \text{if } \det(u_\infty)>0\,, \\ L^*(\varepsilon u)\boldsymbol{f}(\varepsilon u_\infty[i])j(\varepsilon u_\infty,i)^{-\kappa} & \text{if } \det(u_\infty)<0\,. \end{cases}$$

Then, on account of (18), we have, for every unit γ of $\mathfrak{o}$,

(19) $$\boldsymbol{f}_0(\gamma u)=\boldsymbol{f}_0(u)\,.$$

As every right $\mathfrak{o}$-ideal is principal, we have

(20) $$\mathfrak{J}=\Phi^*U\,.$$

Therefore, on account of (19), we can define a function $F(x)$ on $\mathfrak{J}$ by

$$F(\alpha u)=\boldsymbol{f}_0(u) \text{ for } \alpha\in\Phi^*,\quad u\in U\,.$$

We have then, for every $\alpha\in\Phi^*$,

(21) $$F(\alpha x)=F(x)\,.$$

Define a function $\varphi(x)=\prod_p\varphi_p(x)$ on $\mathfrak{A}$ as follows.

i) For every finite prime p,

$$\varphi_p(x_p)=\begin{cases} 1, \text{ if } x_p\in\mathfrak{o}_p \text{ and } x_p\equiv\begin{pmatrix} c & 0\\ 0 & 1\end{pmatrix} \text{mod.}\, \mathfrak{a}_p, (c,\mathfrak{a}_p)=1\,, \\ 0, \text{ otherwise.}\end{cases}$$

ii) $\varphi_\infty(w)=j(w,i)^\kappa\exp\{-\pi\,\mathrm{tr}\,(w{}^tw)\}$, where ${}^tw$ denotes the transpose of w.

We need furthermore a function $\psi_k(x)$ on $\mathfrak{J}$, for any integer k, defined by $\psi_k(x)=(x_\infty[i])^k$.

Now consider the integral

$$\zeta(s,\boldsymbol{f},\varphi,k,y)=\int_{\mathfrak{J}}F(yx)\psi_k(x)\varphi(x)\,|\,x\,|^s dm^*(x)\,,$$

where y is an element of $\mathfrak{J}$ such that $y_p=1$ for all finite p and $\det(y_\infty)>0$. As $F(x)=O(|\,x\,|^{-\kappa/2})$, we observe that this integral converges absolutely for large $\mathrm{Re}(s)$; first we transform it as follows.

$$\zeta(s,\boldsymbol{f},\varphi,k,y)=\int_{\mathfrak{J}}F(x)\psi_k(y^{-1}x)\varphi(y^{-1}x)\,|\,y^{-1}x\,|^s dm^*(x)$$
$$=\sum_{\{\alpha\}}\int_{\alpha U}\,,$$

where the sum is extended over the representatives α for $\Phi^*/(\Gamma\cup\Gamma\varepsilon)$; we may take α so that $N(\alpha)>0$. By the relation (21),

$$\int_{\alpha U}=\int_U F(x)\psi_k(y^{-1}\alpha x)\varphi(y^{-1}\alpha x)\,|\,y^{-1}x\,|^s dm^*(x)$$
$$=B(\alpha)\int_{G_+}+B'(\alpha)\int_{\varepsilon^{-1}G_+}\,,$$

where

$$B(\alpha)=\prod_p\int_{U_p}\varphi_p(\alpha x_p)L^*(x_p)dm^*(x_p),\quad B'(\alpha)=\prod_p\int_{U_p}\varphi_p(\alpha x_p)L^*(\varepsilon x_p)dm^*(x_p)\,.$$

By our definition of $\varphi_p, B(\alpha)$ does not vanish only when $\alpha \in \mathfrak{o}$ and α is prime to $\mathfrak{a}$. If that is so, we can find an element γ of Γ so that $\alpha\gamma \equiv \begin{pmatrix} c & 0 \\ 0 & 1 \end{pmatrix}$ mod. $\mathfrak{a}$. Therefore, taking $\alpha\gamma$ in place of α, we have only to consider $B(\alpha)$ and $B'(\alpha)$ for the elements α satisfying $\alpha \equiv \begin{pmatrix} c & 0 \\ 0 & 1 \end{pmatrix}$ mod. $\mathfrak{a}$. Then, recalling the definition of L^* and our choice of ε, we get

$$B(\alpha) = B'(\alpha) = e(\mathfrak{a})1_m,$$

where $e(\mathfrak{a})$ is a positive number depending only on $\mathfrak{a}$.

Now the integral on G_+ is equal to

$$N(\alpha)^{-s}\int_{G_+} \boldsymbol{f}(w[i])j(y^{-1}\alpha, w[i])^{\kappa}(y^{-1}\alpha w[i])^{k} \times \\ \exp\{-\pi\,\mathrm{tr}\,({}^t(y^{-1}\alpha)(y^{-1}\alpha)w{}^tw)\} \cdot \det(y^{-1}\alpha w)^s dm^*(w).$$

We observe that the integrand is invariant under the right multiplication of the elements of K; so it is considered as a function on G_+/K. By the correspondence $w \to w{}^tw$, G_+/K is identified with the space P of positive symmetric matrices of degree 2. Let $g(Y)$ be a function on P defined by

$$g(w{}^tw) = \boldsymbol{f}(w[i])j(y^{-1}\alpha, w[i])^{\kappa}(y^{-1}\alpha w[i])^{k} \qquad \text{for} \quad w \in G_+.$$

Then the above integral is equal to

$$(22) \qquad N(\alpha)^{-s}\int_P g(Y)\exp\{-\pi\,\mathrm{tr}\,(A^{-1}Y)\}\det(A^{-1}Y)^{s/2}dY,$$

where $A = (\alpha^{-1}y){}^t(\alpha^{-1}y)$. We have $Dg = 0$ for any invariant differential operator D on $P = G/K$, so that by virtue of the result of Selberg [18, pp. 58-59], (20) is equal to

$$c_1 N(\alpha)^{-s}\pi^{-s}\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s-1}{2}\right)g(A)$$

$$= c_1\pi^{-s}\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s-1}{2}\right)N(\alpha)^{-s}i^k\boldsymbol{f}(\alpha^{-1}y[i])j(\alpha^{-1}, y[i])^{-\kappa}j(y, i)^{-\kappa},$$

where c_1 is a constant depending only upon our choice of invariant measure of $P = G/K$. The integral on $\varepsilon^{-1}G_+$ is transformed by $w \to \varepsilon^{-1}w$ to the integral

$$(23) \qquad \int_{G_+} \boldsymbol{f}(w[i])j(y^{-1}\alpha\varepsilon^{-1}, w[i])^{\kappa}(y^{-1}\alpha\varepsilon^{-1}w[i])^{k} \times \\ \exp\{-\pi\,\mathrm{tr}\,({}^t(y^{-1}\alpha\varepsilon^{-1})(y^{-1}\alpha\varepsilon^{-1})w{}^tw)\}\det(y^{-1}w)^s dm^*(w).$$

We note that $\det(y^{-1}\alpha\varepsilon^{-1}) < 0$; so take an element u such that $u{}^tu = 1$, $\det u = -1$. Let $g'(Y)$ be a function on P defined by

$$g'(w{}^tw) = \boldsymbol{f}(w[i])j(y^{-1}\alpha\varepsilon^{-1}, w[i])^{\kappa}(y^{-1}\alpha\varepsilon^{-1}w[i])^{k} \qquad \text{for} \quad w \in G_+$$

Then the integral (23) is equal to

$$N(\alpha)^{-s}\int_P g'(Y)\exp\{-\pi\,\mathrm{tr}\,(B^{-1}Y)\}\det(B^{-1}Y)^{s/2}dY\,,$$

where $B=(\varepsilon\alpha^{-1}yu)^t(\varepsilon\alpha^{-1}yu)$. Then, by the same reason as above, this is equal to

$$c_1\pi^{-s}\Gamma\Big(\frac{s}{2}\Big)\Gamma\Big(\frac{s-1}{2}\Big)N(\alpha)^{-s}g'(B)$$

$$=c_1\pi^{-s}\Gamma\Big(\frac{s}{2}\Big)\Gamma\Big(\frac{s-1}{2}\Big)N(\alpha)^{-s}(-i)^k\boldsymbol{f}(\varepsilon\alpha^{-1}y[-i])j(\varepsilon\alpha^{-1},y[-i])^{-\kappa}j(y,-i)^{-\kappa}.$$

Put now

$$\xi(s)=(2\pi)^{-s}\Gamma(s),\quad c_2=2\sqrt{\pi}\;c_1e(\mathfrak{a})\,.$$

For any point z on the upper half plane $\mathfrak{H}$, we can find an element $y\in G_+$ such that $y[i]=z$ and $j(y,i)=1$. For such y, the above calculation shows that

$$\zeta(s,\boldsymbol{f},\varphi,k,y)$$
$$=c_2\xi(s-1)\sum_{\{\alpha\}}N(\alpha)^{-s}\{i^k\boldsymbol{f}(\alpha^{-1}[z])j(\alpha^{-1},z)^{-\kappa}+(-i)^k\boldsymbol{f}(\varepsilon\alpha^{-1}[\bar{z}])j(\varepsilon\alpha^{-1},\bar{z})^{-\kappa}\}\,.$$

Define the matrix $\mathfrak{T}_\kappa(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})$ as in (11) of § 1.5. By our choice of $\boldsymbol{f}$, the $\mathfrak{T}_\kappa(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})$ are real matrices for every $\alpha\in\varDelta_\mathfrak{a}^*$. Hence, using the relation (9) of § 1.5, we obtain

$$\zeta(s,\boldsymbol{f},\varphi,k,y)=c_2\xi(s-1)\sum_{\alpha\in\varDelta_\mathfrak{a}^*}\mathfrak{T}_\kappa(\Gamma_\mathfrak{a}\alpha\Gamma_\mathfrak{a})N(\alpha)^{1-s}\,\mathrm{Re}\,(i^k\boldsymbol{f}(z))\,.\tag{24}$$

We shall now consider the functional equation. Let $\hat{\varphi}(x)=\Pi_p\hat{\varphi}_p(x)$ be the Fourier-transform of φ. We can easily verify that: i) the support of $\hat{\varphi}_p$ is contained in $(\mathfrak{d}_p\mathfrak{a}_p)^{-1}$; ii) $\hat{\varphi}_\propto(w)=i^\kappa\varphi_\propto({}^tw)$. Hence, if $\det(w)\neq0$, we get

$$\hat{\varphi}_\infty(w')=(w[i])^\kappa\varphi_\infty(w)\,,\tag{25}$$

where w' denotes as before the transform of w by the canonical involution. Now by the Poisson summation formula, we get, for every x and y of $\mathfrak{J}$,

$$\sum_{\alpha\in\Phi}\varphi(y^{-1}\alpha x)=|\,yx^{-1}\,|^2\sum_{\alpha\in\Phi}\hat{\varphi}(x^{-1}\alpha y)\,.$$

As we have $\varphi(0)=\hat{\varphi}(0)=0$ and as Φ is a division algebra,

$$\sum_{\alpha\in\Phi^*}\varphi(y^{-1}\alpha x)=|\,yx^{-1}\,|^2\sum_{\alpha\in\Phi^*}\hat{\varphi}(x^{-1}\alpha y)\,.\tag{26}$$

By virtue of (21), we have

$$\zeta(s,\boldsymbol{f},\varphi,0,y)=\int_{\Phi^*\backslash\mathfrak{J}}F(x)\,|\,y^{-1}x\,|^s\sum_{\alpha\in\Phi^*}\varphi(y^{-1}\alpha x)dm^*(x)\,.$$

Then, the usual technique decomposing this into two parts for $|\,x\,|\geqq1$ and $|\,x\,|\leqq1$, together with the formula (26), shows that the function $\zeta(s,\boldsymbol{f},\varphi,0,y)$ can be holomorphically prolongated on the whole s-plane and is equal to

$$\int_\mathfrak{J}F(x^{-1})\,|\,yx\,|^{2-s}\hat{\varphi}(xy)dm^*(x)\,.$$

Now y being such that $y_p=1$ and $\det(y_\infty)>0$, transform this by the canonical involution $x\rightarrow x'$. By our definition of F, we have

$$F(x'^{-1})=|x|^\kappa F(x),$$

and by (25),

$$\hat{\varphi}_\infty(x'y)=(y'x[i])^\kappa\varphi_\infty(y'x),$$

so that

$$\zeta(s,\boldsymbol{f},\varphi,0,y)=\int_{\mathfrak{J}}F(x)\,|x|^{2+\kappa-s}\,|y|^{2-s}\psi_\kappa(y'x)\varphi_1(y'x)dm^*(x),$$

where $\varphi_1(x)=\Pi_p\varphi_{1p}(x_p)$ is defined by: i) $\varphi_{1p}=\hat{\varphi}_p$ for every finite p; ii) $\varphi_{1\infty}=\varphi_\infty$. Transform x into $y'^{-1}x$ and observe that

$$F(y'^{-1}x)=|y|^\kappa F(yx).$$

We obtain then

$$\zeta(s,\boldsymbol{f},\varphi,0,y)=\zeta(2+\kappa-s,\boldsymbol{f},\varphi_1,\kappa,y),\tag{27}$$

which is the functional equation for the Dirichlet-series (13).

In order to find a more explicit form, we restrict ourselves to the case $\mathfrak{a}=\mathfrak{o}$. Since the group Γ contains -1, the vector space $S_\kappa(\Gamma)$ reduces to $\{0\}$ if κ is odd; so we assume henceforth κ is *even*. Put $D(s)=\sum_{n=1}^{\infty}\mathfrak{T}_\kappa(n;\mathfrak{a})n^{-s}$. By (24),

$$\zeta(s,\boldsymbol{f},\varphi,0,y)=c_2\xi(s-1)D(s-1)\operatorname{Re}(\boldsymbol{f}(z)).$$

As φ_p is a characteristic function of $\mathfrak{o}_p$, we have

$$\varphi_{1p}(x_p)=\hat{\varphi}_p(x_p)=\begin{cases} N_1(\mathfrak{d}_p)^{-1/2} & \text{if} \quad x_p\in\mathfrak{d}_p^{-1}, \\ 0 & \text{if} \quad x_p\notin\mathfrak{d}_p^{-1}. \end{cases}$$

Hence we obtain

$$\zeta(s,\boldsymbol{f},\varphi_1,\kappa,y)=c_2(-1)^{\kappa/2}N_1(\mathfrak{d})^{-1/2}\xi(s-1)\sum\mathfrak{T}_\kappa(\Gamma\alpha\Gamma)N(\alpha)^{1-s}\operatorname{Re}(\boldsymbol{f}(z)),\tag{28}$$

where the sum is extended over all the $\Gamma\alpha\Gamma$ such that $\alpha\in\mathfrak{d}^{-1}$, $N(\alpha)>0$. Let δ be an element of $\mathfrak{o}$ such that $\mathfrak{o}\delta=\mathfrak{d}$ and $N(\delta)>0$. Then,

$$N(\delta)^2=N_1(\mathfrak{d})=d(\Phi)^2=\prod_{p|d(\Phi)}p^2,$$

$$\mathfrak{T}_\kappa(\Gamma\delta\Gamma)=\prod_{p|d(\Phi)}\mathfrak{T}_\kappa(p;\mathfrak{o}).$$

If p is a prime factor of $d(\Phi)$, we have

$$\mathfrak{T}_\kappa(p;\mathfrak{o})^2=\mathfrak{T}_\kappa(\Gamma p\Gamma)=p^{\kappa-2}1_m.$$

Therefore $\mathfrak{T}_\kappa(\Gamma\delta\Gamma)$ is invertible; and (28) is equal to

$$c_2(-1)^{\kappa/2}N_1(\mathfrak{d})^{-1/2}\xi(s-1)N(\delta)^{s-1}\mathfrak{T}_\kappa(\Gamma\delta\Gamma)^{-1}D(s-1)\operatorname{Re}(\boldsymbol{f}(z)).$$

Putting

$$\Lambda_\kappa=d(\Phi)^{\kappa/2-1}\mathfrak{T}_\kappa(\Gamma\delta\Gamma)^{-1},$$

the functional equation (27) is now written in the following form.

$$d(\Phi)^{s/2}\xi(s)D(s)=(-1)^{\kappa/2}d(\Phi)^{(\kappa-s)/2}\xi(\kappa-s)\Lambda_{\kappa}D(\kappa-s).$$

We state the result as

THEOREM 1. *Let* $\mathfrak{a}$ *be an integral two-sided* $\mathfrak{o}$*-ideal which is prime to* $d(\Phi)$. *Let* $\mathfrak{T}_{\kappa}(n;\mathfrak{a})$ *be the representation of the operators* $T(n;\mathfrak{a})$ *in the vector space* $S_{\kappa}(\Gamma_{\mathfrak{a}})$ *of cusp-forms of degree* κ *with respect to* $\Gamma_{\mathfrak{a}}$ (cf. § 1.5). *Then the Dirichlet series* $\sum_{(n,\mathfrak{a})=1}\mathfrak{T}_{\kappa}(n;\mathfrak{a})n^{-s}$ *converges absolutely for* $\mathrm{Re}(s)>\kappa+1$ *and has an Euler-product:*

$$\sum_{(n,\mathfrak{a})=1}\mathfrak{T}_{\kappa}(n;\mathfrak{a})n^{-s}=\prod_{p\mid d}[1-\mathfrak{T}_{\kappa}(p;\mathfrak{a})p^{-s}]^{-1}\prod_{p\nmid d\mathfrak{a}}[1-\mathfrak{T}_{\kappa}(p;\mathfrak{a})p^{-s}+R_{\kappa}(p;\mathfrak{a})p^{\kappa-1-2s}]^{-1},$$

where $d=d(\Phi)$. *Put*

$$H_{\kappa}(s;\mathfrak{a})=d(\Phi)^{s/2}(2\pi)^{-s}\Gamma(s)\sum_{(n,\mathfrak{a})=1}\mathfrak{T}_{\kappa}(n;\mathfrak{a})n^{-s}.$$

Then, $H_{\kappa}(s;\mathfrak{a})$ *is a holomorphic function on the whole s-plane, and satisfies the functional equation* (27). *When* $\mathfrak{a}=\mathfrak{o}$, *the functional equation is written in the form*

$$H_{\kappa}(s;\mathfrak{o})=\Lambda H_{\kappa}(\kappa-s;\mathfrak{o}),$$

where

$$\Lambda=(-1)^{\kappa/2}\prod_{p\mid d(\Phi)}p^{\kappa/2-1}\mathfrak{T}_{\kappa}(p;\mathfrak{o}).$$

We note that $\Lambda^2=1$. If we transform the $\mathfrak{T}_{\kappa}(n;\mathfrak{o})$ into diagonal matrices, then the diagonal elements of $\sum_{n=1}^{\infty}\mathfrak{T}_{\kappa}(n;\mathfrak{o})n^{-s}$ are Dirichlet series which belong to the type $\{\lambda,k,\gamma\}$ of Hecke [11] for $\lambda=d(\Phi)^{1/2}, k=\kappa$.

As in the classical case, we may conjecture that the absolute values of the characteristic roots of $\mathfrak{T}_{\kappa}(p;\mathfrak{a})$ do not exceed $2p^{(\kappa-1)/2}$. We shall show in § 6.2 that, if $\kappa=2$, this is true for almost all p.

§ 2. Kummer varieties.

2.1. Quotient of an abelian variety. Let A be an abelian variety and G a finite group of automorphisms of A; let k be a field of definition for A and for the elements of G. Then, we can construct a couple (V,h) formed by a projective variety V and a rational mapping h of A onto V, both defined over k, satisfying the following conditions.

(Q1) h is everywhere defined on A.

(Q2) $h(u)=h(v)$ if and only if there exists an element $\gamma\in G$ such that $\gamma(u)=v$.

(Q3) If h' is a rational mapping of A into a variety V' satisfying $h'\circ\gamma=h'$ for every $\gamma\in G$, then there exists a rational mapping g of V into V' such that $h'=g\circ h$ and g is defined at a point $h(x)$ whenever h' is defined at a point

$x \in A$.

A proof following Serre's idea is given in [**25**] (cf. also Matsusaka [**15**], Serre [**20**], Weil [**31**]). (V, h) is uniquely determined by these conditions up to biregular birational mappings; we call (V, h) a *quotient of A by G*, defined over k. We note that in the condition (Q3), if k' is a field of definition for V' and h' containing k, then g is defined over k'.

2.2. Normalized Kummer varieties. Let $\mathfrak{r}$ be a ring having a finite basis over $\boldsymbol{Z}$ and $\mathcal{P}=(A, \mathcal{C}, \theta)$ a polarized abelian variety of type $\mathfrak{r}$ (cf. [AF, no. 3]). For the sake of simplicity, we assume always that the ring $\mathfrak{r}$ has an identity element 1 and $\theta(1)$ is the identity element of $\mathcal{A}(A)$. Let Ω denote the group of automorphisms of $\mathcal{P}$; then Ω is a subgroup of the group of automorphisms of $(A, \mathcal{C})$. Hence by [**15**] and [**31**], Ω is a finite group. We can therefore construct a quotient of A by Ω. Let K be the field of moduli of $\mathcal{P}$. We call a quotient (V_0, h_0) of A by Ω a *normalized Kummer variety* of $\mathcal{P}$ if it satisfies the following conditions.

(K1) *V_0 is defined over K.*

(K2) *If k is a field of definition for $\mathcal{P}$ containing K, h_0 is defined over k.*

(K3) *k being as in* (K2), *if σ is an isomorphism of k into the universal domain leaving invariant the elements of K, then we have*

$$h_0^\sigma \circ \xi = h_0$$

for every isomorphism ξ of $\mathcal{P}$ onto $\mathcal{P}^\sigma$.

Remark that if σ is the identity on K, there always exists an isomorphism of $\mathcal{P}$ onto $\mathcal{P}^\sigma$ (cf. Proposition 5 of [AF]). We shall now show the existence of normalized Kummer variety. For this purpose we need a result due to W. L. Chow [**1**], which we state as

LEMMA 2.1. *Let A and B be two abelian varieties and λ a homomorphism of A into B; let k be a field of definition for A and B. Then λ is defined over a separably algebraic extension of k.*

PROPOSITION 2.2. *Let $\mathcal{P}=(A, \mathcal{C}, \theta)$ and $\mathcal{P}_1=(A_1, \mathcal{C}_1, \theta_1)$ be two polarized abelian varieties of type $\mathfrak{r}$, and η an isomorphism of $\mathcal{P}$ onto $\mathcal{P}_1$. Let K be the field of moduli of $\mathcal{P}_1$, and (V, h) a quotient of A_1 by the group of automorphisms of $\mathcal{P}_1$ such that V is defined over K. Suppose that there exists a separably generated extension M of K satisfying the following conditions:*

i) *A_1 and h are defined over M;*

ii) *if σ is an isomorphism of M into the universal domain leaving invariant the elements of K, then we have $h^\sigma \circ \xi = h$ for every isomorphism ξ of $\mathcal{P}_1$ onto $\mathcal{P}_1^\sigma$. Then $(V, h \circ \eta)$ is a normalized Kummer variety of $\mathcal{P}$; in particular, (V, h) is a normalized Kummer variety of $\mathcal{P}_1$.*

PROOF. Since $\mathcal{P}$ is isomorphic to $\mathcal{P}_1$, K is also the field of moduli of $\mathcal{P}$.

It is easy to verify that $(V, h \circ \eta)$ is a quotient of A by the group of automorphisms of $\mathcal{P}$. Let k be a field of definition for $\mathcal{P}$ containing K, and τ an isomorphism of k into the universal domain leaving invariant the elements of K. By Lemma 2.1, there exists a separably algebraic extension k_1 of kM over which η is defined. We take an extension k_2 of k_1 over which $\mathcal{P}_1$ is defined, and extend τ to an isomorphism of k_2 which we denote by σ. Then, for every isomorphism ξ of $\mathcal{P}$ onto $\mathcal{P}^\sigma, \eta^\sigma \circ \xi \circ \eta^{-1}$ is an isomorphism of $\mathcal{P}_1$ onto $\mathcal{P}_1^\sigma$. By our assumption ii), we have $h^\sigma \circ \eta^\sigma \circ \xi \circ \eta^{-1} = h$, so that $(h \circ \eta)^\sigma \circ \xi = h \circ \eta$. If we assume that σ is the identity on k, we have $\mathcal{P} = \mathcal{P}^\sigma$, so that we can take ξ to be the identity mapping of $\mathcal{P}$ onto itself. We have then $(h \circ \eta)^\sigma = h \circ \eta$. This shows that $h \circ \eta$ is defined over k, since $h \circ \eta$ is defined over a separably generated extension k_1 of k. Therefore $(V, h \circ \eta)$ satisfies the conditions (K1, 2, 3).

Let $\mathcal{P} = (A, \mathcal{C}, \theta)$ be a polarized abelian variety of type $\mathfrak{r}$ and K the field of moduli of $\mathcal{P}$. By the definition of field of moduli, there exists an ample divisor X in $\mathcal{C}$ such that the field of moduli K is the smallest field of definition for the variety $\mathcal{F}(A, X, \theta)$ (cf. no. 5 of [AF]). By Proposition 4 of [AF], there exist a regular extension M of K, an abelian variety A_1 in a projective space P^n, a hyperplane section X_1 of A_1 and an isomorphism η of A onto A_1 satisfying the following conditions:

(A′1) $\eta(X)$ is algebraically equivalent to X_1;

(A′2) A_1 and $\eta\theta(r)\eta^{-1}$ for $r \in \mathfrak{r}$ are all defined over M, and X_1 is rational over M.

Put $\theta_1(r) = \eta\theta(r)\eta^{-1}$ for $r \in \mathfrak{r}, \mathcal{C}_1 = \mathcal{C}(X_1)$, and $\mathcal{P}_1 = (A_1, \mathcal{C}_1, \theta_1)$. Then η is an isomorphism of $\mathcal{P}$ onto $\mathcal{P}_1$. Denote by Ω_1 the group of automorphisms of $\mathcal{P}_1$. By virtue of Proposition 2.2, if we construct a quotient (V, h) of A_1 by Ω_1, satisfying the conditions i) and ii) of the proposition for the present $\mathcal{P}_1$ and M, then $(V, h \circ \eta)$ gives a normalized Kummer variety of $\mathcal{P}$. Therefore we shall now proceed in the construction of such a quotient. By Lemma 2.1, we can find a finite Galois extension M_1 of M such that every element of Ω_1 is defined over M_1; let $\mathcal{G}$ denote the Galois group of M_1 over M. Take any quotient (V, h) of A_1 by Ω_1 defined over M_1. We see easily that for every $\gamma \in \Omega_1$ and for every $\sigma \in \mathcal{G}, \gamma^\sigma$ is an automorphism of $\mathcal{P}_1$, so that $\gamma^\sigma \in \Omega_1$. Hence, for every $\sigma \in \mathcal{G}, (V^\sigma, h^\sigma)$ is a quotient of A_1 by Ω_1, defined over M_1. On account of (Q3), there exist rational mappings g_σ and g'_σ, of V into V^σ and of V^σ into V, such that $g_\sigma \circ h = h^\sigma, g'_\sigma \circ h^\sigma = h$, and, g_σ is everywhere defined on V and g'_σ is everywhere defined on V^σ. We see then that g_σ is a birational mapping of V onto V^σ which is everywhere biregular on V and $g'_\sigma = (g_\sigma)^{-1}$. By the remark of § 2.1, g_σ is defined over M_1. Put $f_{\tau,\sigma} = g_\tau \circ (g_\sigma)^{-1}$ for $\sigma, \tau \in \mathcal{G}$. Then we have

$$f_{\tau,\sigma} \circ f_{\sigma,\rho} = f_{\tau,\rho} .$$

Morever, if $\omega \in \mathcal{G}$, we have

$$g_{\sigma}^{\omega} \circ g_{\omega} \circ h = g_{\sigma}^{\omega} \circ h^{\omega} = (g_{\sigma} \circ h)^{\omega} = h^{\sigma\omega} = g_{\sigma\omega} \circ h ,$$

so that $g_{\sigma}^{\omega} \circ g_{\omega} = g_{\sigma\omega}$; hence we have

$$f_{\tau\omega,\sigma\omega} = g_{\tau\omega} \circ (g_{\sigma\omega})^{-1} = g_{\tau}^{\omega} \circ g_{\omega} \circ (g_{\sigma}^{\omega} \circ g_{\omega})^{-1} = g_{\tau}^{\omega} \circ (g_{\sigma}^{\omega})^{-1} = (f_{\tau,\sigma})^{\omega} .$$

Thus the mappings $f_{\tau,\sigma}$ satisfy the conditions of Theorem 1 of Weil [**32**]. Therefore, by the result of [**32**], there exist a projective variety V_1, defined over M, and a birational mapping f of V onto V_1, defined over M_1, such that f is everywhere biregular and $f_{\tau,\sigma} = (f^{\tau})^{-1} \circ f^{\sigma}$ for $\tau, \sigma \in \mathcal{G}$. Put $h_1 = f \circ h$; then we see that h_1 is defined over M_1. Moreover, for every $\rho \in \mathcal{G}$, we have

$$h_1^{\rho} = f^{\rho} \circ h^{\rho} = f \circ f_{1,\rho} \circ h^{\rho} = f \circ (g_{\rho})^{-1} \circ h^{\rho} = f \circ h = h_1 ;$$

this shows that h_1 is defined over M. We can easily verify that (V_1, h_1) satisfies (Q1, 2, 3) for A_1 and Ω_1, so that (V_1, h_1) is a quotient of A_1 by Ω_1, defined over M.

Now let t be a point in an affine space such that $M = K(t)$. As M is a regular extension of K, t has a locus over K, which we denote by T. For every generic point u of T over K, we consider the isomorphism of $K(t)$ onto $K(u)$ over K which maps t onto u, and denote by $\mathcal{P}_u, A_u, \Omega_u, V_u, h_u$ the transform of $\mathcal{P}_1, A_1, \Omega_1, V_1, h_1$ by the isomorphism. It is clear that Ω_u is the group of automorphisms of $\mathcal{P}_u$ and (V_u, h_u) is a quotient of A_u by Ω_u, defined over $K(u)$. Let u and v be two generic points of T over K. As K is the field of moduli of $\mathcal{P}_1$, we see that, by Proposition 5 of [AF], both $\mathcal{P}_u$ and $\mathcal{P}_v$ are isomorphic to $\mathcal{P}_1$. Hence there exists an isomorphism λ of $\mathcal{P}_u$ onto $\mathcal{P}_v$; and so we can find a birational mapping φ of V_u onto V_v, everywhere biregular on V_u, such that

$$\varphi \circ h_u = h_v \circ \lambda .$$

If λ' is another isomorphism of $\mathcal{P}_u$ onto $\mathcal{P}_v$, $\lambda' \circ \lambda^{-1}$ is contained in Ω_v; we have therefore $h_v = h_v \circ (\lambda' \circ \lambda^{-1})$ and hence

$$\varphi \circ h_u = h_v \circ \lambda = h_v \circ (\lambda' \circ \lambda^{-1}) \circ \lambda = h_v \circ \lambda' .$$

This shows that the mapping φ does not depend on the choice of λ; so we write $\varphi = \varphi_{v,u}$. We shall now prove that $\varphi_{v,u}$ is defined over $K(u, v)$. As A_u and A_v are defined over $K(u, v)$, we can find, on account of Lemma 2.1, a finite separably algebraic extension L of $K(u, v)$ over which λ is defined. Then, by the remark in § 2.1, $\varphi_{v,u}$ is defined over L. Let σ be an isomorphism of L over $K(u, v)$ into the algebraic closure of $K(u, v)$. Then λ^{σ} is an isomorphism of $\mathcal{P}_u$ onto $\mathcal{P}_v$, so that we have

$$(\varphi_{v,u})^{\sigma} \circ h_u = (\varphi_{v,u} \circ h_u)^{\sigma} = (h_v \circ \lambda)^{\sigma} = h_v \circ \lambda^{\sigma} = \varphi_{v,u} \circ h_u .$$

Hence we have $\varphi_{v,u}{}^{\sigma}=\varphi_{v,u}$; this shows that $\varphi_{v,u}$ is defined over $K(u,v)$. Now, u,v,w being three generic points of T over K, we have

$$(1) \qquad \varphi_{w,v}\circ\varphi_{v,u}=\varphi_{w,u}\,.$$

In fact, if λ is an isomorphism of $\mathcal{P}_u$ onto $\mathcal{P}_v$ and μ is an isomorphism of $\mathcal{P}_v$ onto $\mathcal{P}_w$, $\mu\circ\lambda$ is an isomorphism of $\mathcal{P}_u$ onto $\mathcal{P}_w$, so that $\varphi_{w,u}\circ h_u=h_w\circ\mu\circ\lambda=\varphi_{w,v}\circ h_v\circ\lambda=\varphi_{w,v}\circ\varphi_{v,u}\circ h_u$; this proves the relation (1). Applying the result of [**32**] to V_u and $\varphi_{v,u}$, we obtain a projective variety V_0, defined over K and a birational mapping φ_t of V_0 onto V_t, which is biregular on V_0 and defined over $K(t)$, such that

$$(2) \qquad \varphi_{v,u}=\varphi_v\circ(\varphi_u)^{-1}\,,$$

where φ_w denotes, for any generic point w of T over K, the transform of φ_t by the isomorphism of $K(t)$ onto $K(w)$ over K which maps t onto w. In [**32**], only independent generic points are considered; but once we obtain the relation (2) for independent generic points, we have the same formula for any two generic points by virtue of the relation (1), since (1) holds for any three generic points. Put now

$$h_0=(\varphi_t)^{-1}\circ h_t\,.$$

We note that $\mathcal{P}_1=\mathcal{P}_t$, $V_1=V_t$, $h_1=h_t$. It is easy to see that (V_0,h_0) is a quotient of A_1 by Ω_1, and h_0 is defined over M. Let σ be an isomorphism of M into the universal domain leaving invariant the elements of K, and ξ an isomorphism of $\mathcal{P}_1$ onto $\mathcal{P}_1^{\sigma}$. Putting $t^{\sigma}=u$, we have $\mathcal{P}_1^{\sigma}=\mathcal{P}_u$, $h_t^{\sigma}=h_u$, $\varphi_t^{\sigma}=\varphi_u$; and by the property of $\varphi_{u,v}$, we have $\varphi_{u,t}\circ h_t=h_u\circ\xi$. Hence,

$$h_0^{\sigma}\circ\xi=(\varphi_t^{-1}\circ h_t)^{\sigma}\circ\xi=\varphi_u^{-1}\circ h_u\circ\xi=\varphi_u^{-1}\circ\varphi_{u,t}\circ h_t=\varphi_t^{-1}\circ h_t=h_0\,.$$

Thus we have proved that $\{\mathcal{P}_1, M, (V_0,h_0)\}$ satisfies the conditions i), ii) of Proposition 2.2. Therefore, by that proposition, $(V_0,h_0\circ\eta)$ is a normalized Kummer variety of $\mathcal{P}$.

Now we consider about the uniqueness of normalized Kummer variety.

PROPOSITION 2.3. *Let $\mathcal{P}=(A,C,\theta)$ be a polarized abelian variety of type $\mathfrak{r}$, (V,h) and (V_1,h_1) two normalized Kummer variety of $\mathcal{P}$, and K the field of moduli of $\mathcal{P}$. Then, there exists a biregular birational mapping α of V onto V_1 such that $h_1=\alpha\circ h$; the mapping α is defined over a purely inseparable extension of K. Moreover, if A is defined over a separably generated extension of K, α is defined over K.*

PROOF. The existence of a biregular birational mapping α such that $h_1=\alpha\circ h$ follows directly from the property (Q3) of quotient. Let k be a field of definition for $\mathcal{P}$ containing K. Then, h and h_1 are defined over k, so that α is defined over k. Let σ be an isomorphism of k into the universal domain leaving invariant the elements of K. Then, for any isomorphism ξ of $\mathcal{P}$ onto

$\mathcal{P}^\sigma$, we have $h=h^\sigma\circ\xi, h_1=h_1^\sigma\circ\xi$, and hence $\alpha\circ h=h_1=h_1^\sigma\circ\xi=\alpha^\sigma\circ h^\sigma\circ\xi=\alpha^\sigma\circ h$; so we have $\alpha^\sigma=\alpha$. This proves the first assertion of our proposition. If k is separably generated over K, the relation $\alpha^\sigma=\alpha$ shows that α is defined over K; this proves the last assertion.

2.3. Homomorphisms of polarized abelian varieties. Let $\mathcal{P}=(A,C,\theta)$ and $\mathcal{P}'=(A',C',\theta')$ be two polarized abelian varieties of type $\mathfrak{r}$, of the same dimension, and λ a homomorphism of A onto A'. We call λ a *homomorphism* of $\mathcal{P}$ onto $\mathcal{P}'$ if we have $\lambda^{-1}(X')\in C$ for every $X'\in C'$ and $\lambda\theta(r)=\theta'(r)\lambda$ for every $r\in\mathfrak{r}$. The following proposition is an easy consequence of this definition.

PROPOSITION 2.4. *Let $\mathcal{P}=(A,C,\theta)$, $\mathcal{P}_1=(A_1,C_1,\theta_1)$, $\mathcal{P}_2=(A_2,C_2,\theta_2)$ be three polarized abelian varieties of type $\mathfrak{r}$, of the same dimension; let λ_1,λ_2,μ be respectively homomorphisms of A onto A_1, of A onto A_2, of A_1 onto A_2 such that $\mu\circ\lambda_1=\lambda_2$. If any two of λ_1,λ_2,μ are homomorphisms of polarized abelian varieties of type $\mathfrak{r}$, then so is the remaining one.*

PROPOSITION 2.5. *Let $\mathcal{P}=(A,C,\theta)$, $\mathcal{P}_1=(A_1,C_1,\theta_1)$, $\mathcal{P}_2=(A_2,C_2,\theta_2)$ be three polarized abelian varieties of type $\mathfrak{r}$, of the same dimension; let λ_i, for $i=1,2$, be a separable homomorphism of $\mathcal{P}$ onto $\mathcal{P}_i$ and $\mathfrak{g}_i$ the kernel of λ_i. Then the following two assertions hold.*

i) *If $\mathfrak{g}_1=\mathfrak{g}_2$, then there exists an isomorphism η of $\mathcal{P}_1$ onto $\mathcal{P}_2$ such that $\eta\circ\lambda_1=\lambda_2$.*

ii) *Suppose that $\nu(\lambda_1)=\nu(\lambda_2)$ and there exists an element a in $\mathfrak{r}$ for which we have, for each i,*

$$\beta\in\mathcal{A}(A),\quad \beta(\mathfrak{g}_i)=\{0\}\Leftrightarrow\beta\in\theta(a\mathfrak{r}).$$

Under these assumptions, if $\mathcal{P}_1$ is isomorphic to $\mathcal{P}_2$, then we have $\mathfrak{g}_1=\mathfrak{g}_2$.

PROOF. The assertion i) is an immediate consequence of Proposition 2.4; so we shall prove ii). Assumptions being as in ii), let ε be an isomorphism of $\mathcal{P}_2$ onto $\mathcal{P}_1$. Since $\theta(a)(\mathfrak{g}_1)=\{0\}$, there exists a homomorphism μ of A_1 into A such that $\mu\circ\lambda_1=\theta(a)$. As $\nu(\lambda_1)1_A$ is contained in $\theta(a\mathfrak{r})$, we have $\nu(\theta(a))\neq 0$, so that μ is an isogeny. We see that $\mu\circ\varepsilon\circ\lambda_2\in\mathcal{A}(A)$ and $\mu\circ\varepsilon\circ\lambda_2(\mathfrak{g}_2)=\{0\}$. Hence there exists an element $r\in\mathfrak{r}$ such that $\mu\circ\varepsilon\circ\lambda_2=\theta(ar)$; we obtain then $\mu\circ\varepsilon\circ\lambda_2=\mu\circ\lambda_1\circ\theta(r)$, so that $\varepsilon\circ\lambda_2=\lambda_1\circ\theta(r)$. From this and the assumption $\nu(\lambda_1)=\nu(\lambda_2)$, it follows that $\nu(\theta(r))=1$; this shows that $\theta(r)$ is an automorphism of A. As λ_1 commutes with the operation of $\mathfrak{r}$, we have $\varepsilon\circ\lambda_2=\theta_1(r)\circ\lambda_1$; this implies $\mathfrak{g}_1=\mathfrak{g}_2$, since ε and $\theta_1(r)$ are isomorphisms.

2.4. Fields obtained from the points of finite order.

PROPOSITION 2.6. *Let $\mathcal{P}=(A,C,\theta)$ be an abelian variety of type $\mathfrak{r}$ and (V,h) a normalized Kummer variety of $\mathcal{P}$. Let $\mathfrak{a}$ be a subset of $\mathfrak{r}$ such that $\theta(\mathfrak{a})$ contains a regular element of $\mathcal{A}_0(A)$; denote by $\mathfrak{g}(\mathfrak{a},A)$ the set of points t on A such* *that* $\theta(a)t=0$ *for every* $a\in\mathfrak{a}$. *Let* K *be the field of moduli of* $\mathcal{P}$ *and* $K_{\mathfrak{a}}$ *the field generated over* K *by the points* $h(t)$ *for* $t\in\mathfrak{g}(\mathfrak{a},A)$. *Then,* $K_{\mathfrak{a}}$ *is a normal algebraic extension of* K.

PROOF. As $\theta(\mathfrak{a})$ contains a regular element of $\mathcal{A}_0(A)$, the field $K_{\mathfrak{a}}$ is algebraic over K. Let σ be an isomorphism of the universal domain into itself, which leaves invariant the elements of K. Then, there exists an isomorphism ε of $\mathcal{P}$ onto $\mathcal{P}^{\sigma}$, for which we have $h^{\sigma}\circ\varepsilon=h$. Denote by $\mathfrak{g}(\mathfrak{a},A^{\sigma})$ the set of points u on A^{σ} such that $\theta^{\sigma}(a)u=0$ for every $a\in\mathfrak{a}$. It is easy to see that $t\rightarrow t^{\sigma}$ gives an isomorphism of $\mathfrak{g}(\mathfrak{a},A)$ onto $\mathfrak{g}(\mathfrak{a},A^{\sigma})$ and $u\rightarrow\varepsilon^{-1}u$ gives an isomorphism of $\mathfrak{g}(\mathfrak{a},A^{\sigma})$ onto $\mathfrak{g}(\mathfrak{a},A)$; hence $t\rightarrow\varepsilon^{-1}t^{\sigma}$ gives an automorphism of $\mathfrak{g}(\mathfrak{a},A)$. By the relation $h^{\sigma}\circ\varepsilon=h$, we have $h(t)^{\sigma}=h(\varepsilon^{-1}t^{\sigma})$. Therefore, $h(t)\rightarrow h(t)^{\sigma}$ is a permutation of the points $\{h(t)\,|\,t\in\mathfrak{g}(\mathfrak{a},A)\}$. This proves our proposition.

PROPOSITION 2.7. *Let* $\mathcal{P}=(A,C,\theta)$ *and* $\mathcal{P}'=(A',C',\theta')$ *be two polarized abelian varieties of type* $\mathfrak{r}$, *of the same dimension, defined over a field of characteristic* 0; *let* (V,h) *be a normalized Kummer variety of* $\mathcal{P}$. *Let* λ *be a homomorphism of* $\mathcal{P}$ *onto* $\mathcal{P}'$ *and* $\mathfrak{g}$ *the kernel of* λ. *Suppose that every automorphism of* $\mathcal{P}$ *leaves invariant* $\mathfrak{g}$ *as a whole. Let* K *and* K' *be respectively the fields of moduli of* $\mathcal{P}$ *and* $\mathcal{P}'$. *Then* K' *is contained in the field* $K(h(t)\,|\,t\in\mathfrak{g})$.

PROOF. Let σ be an isomorphism of the universal domain into itself, which is the identity on $K(h(t)\,|\,t\in\mathfrak{g})$. There exists an isomorphism ε of $\mathcal{P}$ onto $\mathcal{P}^{\sigma}$, for which we have $h^{\sigma}\circ\varepsilon=h$. For every $t\in\mathfrak{g}$, we have $h(t)=h(t)^{\sigma}=h(\varepsilon^{-1}t^{\sigma})$, so that by the property (Q2) of quotient, there exists an automorphism η of $\mathcal{P}$ such that $\varepsilon^{-1}t^{\sigma}=\eta t$. By our assumption, this shows that $\varepsilon^{-1}t^{\sigma}$ is contained in $\mathfrak{g}$. Hence $\mathfrak{g}$ is the kernel of $\lambda^{\sigma}\circ\varepsilon$. By i) of Proposition 2.5, $\mathcal{P}'^{\sigma}$ is isomorphic to $\mathcal{P}'$; so σ must be the identity on K'. This proves that K' is contained in $K(h(t)\,|\,t\in\mathfrak{g})$.

PROPOSITION 2.8. *Notations and assumptions being as in Proposition* 2.7, *let* (V',h') *be a normalized Kummer variety of* $\mathcal{P}'$; *and put* $K_1=K(h(t)\,|\,t\in\mathfrak{g})$. *Then, for every point* u *on* $A, K_1(h(u))$ *contains* $K'(h'(\lambda(u)))$.

PROOF. Let σ be an isomorphism of the universal domain into itself leaving invariant the elements of $K_1(h(u))$. ε being as in the proof of Proposition 2.7, we have $h(u)=h(u)^{\sigma}=h(\varepsilon^{-1}u^{\sigma})$, so that there exists an automorphism ξ of $\mathcal{P}$ such that $\varepsilon^{-1}u^{\sigma}=\xi u$. Put $\varepsilon_0=\varepsilon\xi$. Then ε_0 is also an isomorphism of $\mathcal{P}$ onto $\mathcal{P}'$. Applying the argument of the proof of Proposition 2.7 to ε_0, we observe that $\lambda^{\sigma}\circ\varepsilon_0$ has the same kernel as λ. Hence, by i) of Proposition 2.5, there exists an isomorphism α of $\mathcal{P}'$ onto $\mathcal{P}'^{\sigma}$ such that $\lambda^{\sigma}\circ\varepsilon_0=\alpha\circ\lambda$. We have then

$$h'(\lambda(u))^{\sigma}=h'^{\sigma}(\lambda^{\sigma}(u^{\sigma}))=h'^{\sigma}(\lambda^{\sigma}(\varepsilon_0(u)))=h'(\lambda(u)).$$

On account of Proposition 2.7, it follows that σ is the identity on $K'(h'(\lambda(u)))$;

this proves our proposition.

§ 3. Automorphic functions attached to an indefinite quaternion algebra.

We shall now consider the functions obtained from the points of finite order on the abelian varieties belonging to an analytic system. We shall only deal with the system attached to an indefinite quaternion algebra ([AF, § 5]), though our method is applicable to a more general case.

3.1. The analytic system $\mathcal{S}=\{\mathcal{P}(z)\mid z\in\mathfrak{H}\}$. First we recall the results of [AF, § 5] with a few changes of notations. Let Φ be an indefinite quaternion algebra over $\boldsymbol{Q}$. We fix once for all a faithful representation χ of Φ by real matrices of degree 2. Let $\mathfrak{H}$ denote the upper half complex plane defined by $\mathrm{Im}(z)>0$. For every $z\in\mathfrak{H}$, we denote by $e(z)$ the column-vector $\begin{pmatrix} z \\ 1 \end{pmatrix}$. Let $\mathfrak{o}$ be an order in Φ; for every $z\in\mathfrak{H}$, put

$$D(z)=\chi(\mathfrak{o})e(z)=\{\chi(\alpha)e(z)\mid\alpha\in\mathfrak{o}\}\,.$$

Then, $D(z)$ is a lattice in $\boldsymbol{C}^2$ and $\boldsymbol{C}^2/D(z)$ has a structure of abelian variety. This was shown by constructing a Riemann form on $\boldsymbol{C}^2/D(z)$ as follows (cf. [AF, no. 18]): Let ρ be an element of Φ such that ρ^2 is a negative rational number. Put, for every $\alpha\in\Phi$,

$$\alpha^*=\rho^{-1}\alpha'\rho\,.$$

Then $\alpha\rightarrow\alpha^*$ gives an involution of Φ; and we have $\mathrm{tr}(\alpha\alpha^*)>0$ for every $\alpha\neq0$ of Φ. Define an $\boldsymbol{R}$-bilinear form $E(x,y)$ on $\boldsymbol{C}^2$ in such a way that

$$E(\chi(\alpha)e(z),\quad\chi(\beta)e(z))=\mathrm{tr}\,(\rho\alpha\beta')$$

holds for every $\alpha\in\Phi$ and $\beta\in\Phi$. Then, for a suitable integer $c\neq0$, cE defines a non-degenerate Riemann form on the complex torus $\boldsymbol{C}^2/D(z)$.

Now we can construct (cf. [AF, no. 19]) a system of polarized abelian varieties $\{\mathcal{P}(z)\mid z\in\mathfrak{H}\}$ of type $\mathfrak{o}$ parametrized by an analytic mapping $\Lambda(x,z)$ of $\boldsymbol{C}^2\times\mathfrak{H}$ into a projective space P^N. The polarized abelian variety $\mathcal{P}(z)=(A(z),\mathcal{C}_z,\theta_z)$ of type $\mathfrak{o}$ is defined as follows.

i) For every $z\in\mathfrak{H}, x\rightarrow\Lambda(x,z)$ is an analytic isomorphism of $\boldsymbol{C}^2/D(z)$ onto the abelian variety $A(z)$.

ii) $\mathcal{C}_z$ is the polarization of $A(z)$ determined by the hyperplane sections; and it corresponds to the Riemann form $cE(x,y)$.

iii) For every $\alpha\in\mathfrak{o}, \theta_z(\alpha)$ is the endomorphism of $A(z)$ corresponding to $\chi(\alpha)$; namely, we have

$$\theta_z(\alpha)\Lambda(x,z)=\Lambda(\chi(\alpha)x,z)\,.$$

We shall denote the system $\{\mathcal{P}(z)\mid z\in\mathfrak{H}\}$ by $\mathcal{S}(\mathfrak{o},*)$ or simply by $\mathcal{S}$. For every $z \in \mathfrak{H}$, we put

$$\mathcal{T}(z) = \mathcal{T}(A(z), \theta_z).$$

The definition of $\mathcal{T}(A, \theta)$ is given in [AF, no. 4] or § 3.4 of the present paper. If we denote by $c(\mathcal{T}(z))$ the Chow-point of the variety $\mathcal{T}(z)$, the field $\boldsymbol{Q}(c(\mathcal{T}(z)))$ is the field of moduli of $\mathcal{P}(z)$. Now, there exist a discrete subset $\mathfrak{W}$ of $\mathfrak{H}$ and a set of meromorphic functions $\{f_1, \cdots, f_m\}$ on $\mathfrak{H}$ such that

$$c(\mathcal{T}(z)) = (1, f_1(z), \cdots, f_m(z)) \tag{3}$$

for every $z \in \mathfrak{H} - \mathfrak{W}$. Denote by $\Gamma = \Gamma(\mathfrak{o})$ the group composed of all units γ of $\mathfrak{o}$ such that $N(\gamma) = 1$. Then, Γ is a Fuchsian group on $\mathfrak{H}$. Let $\mathfrak{K}(\mathfrak{o})$ denote the field of automorphic functions on $\mathfrak{H}$ with respect to Γ. Then, Theorem 6 of [AF] asserts that the meromorphic functions f_i determined by (3) generate the function-field $\mathfrak{K}(\mathfrak{o})$; namely, we have

$$\mathfrak{K}(\mathfrak{o}) = \boldsymbol{C}(f_1, \cdots, f_m).$$

Furthermore, (3) implies that, for every $z \in \mathfrak{H} - \mathfrak{W}$, $\boldsymbol{Q}(f_1(z), \cdots, f_m(z))$ is the field of moduli of $\mathcal{P}(z)$.

PROPOSITION 3.1. *If $\boldsymbol{Q}(c(\mathcal{T}(z)))$ is not algebraic over $\boldsymbol{Q}$, we have $\mathcal{A}_0(A(z)) = \theta_z(\Phi)$, $\mathcal{A}(A(z)) = \theta_z(\mathfrak{o})$; and the automorphisms of $\mathcal{P}(z)$ are $\pm 1_z$, where 1_z denotes the identity element of $\mathcal{A}(A(z))$.*

PROOF. Suppose first that $A(z)$ is simple; then $\mathcal{A}_0(A(z))$ is a division algebra. Since $\mathcal{A}_0(A(z))$ has a rational representation of degree 4, we must have $[\mathcal{A}_0(A(z)) : \boldsymbol{Q}] \leqq 4$; this shows $\mathcal{A}_0(A(z)) = \theta_z(\Phi)$. Now consider the case where $A(z)$ is not simple; $A(z)$ is then isogenous to a product $E_1 \times E_2$ of two elliptic curves E_1 and E_2. If E_1 is not isogenous to E_2, $\mathcal{A}_0(A(z))$ is isomorphic to the direct sum of $\mathcal{A}_0(E_1)$ and $\mathcal{A}_0(E_2)$; this is impossible since $\mathcal{A}_0(A(z))$ contains a central simple algebra $\theta_z(\Phi)$ of degree 2 over $\boldsymbol{Q}$. Hence $A(z)$ must be isogenous to the product $E_1 \times E_1$; and so $\mathcal{A}_0(A(z))$ is isomorphic to the total matrix ring of degree 2 over $\mathcal{A}_0(E_1)$. By the same argument as in the proof of Theorem 6 of [AF], we can show that $\boldsymbol{Q}(c(\mathcal{T}(z)))$ is algebraic over $\boldsymbol{Q}(j(E_1))$, where $j(E)$ denotes the birational invariant o: an elliptic curve E. Since $\boldsymbol{Q}(c(\mathcal{T}(z)))$ is not algebraic over $\boldsymbol{Q}$, $j(E_1)$ can not be algebraic over $\boldsymbol{Q}$, so that $\mathcal{A}_0(E_1)$ is isomorphic to $\boldsymbol{Q}$. If follows from this that $\mathcal{A}_0(A(z)) = \theta_z(\Phi)$. Recall that $A(z)$ is isomorphic to $\boldsymbol{C}^2/D(z)$ and $D(z) = \chi(\mathfrak{o})e(z)$. Then the equality $\mathcal{A}_0(A(z)) = \theta_z(\Phi)$ implies $\mathcal{A}(A(z)) = \theta_z(\mathfrak{o})$. Now let α be an automorphism of $\mathcal{P}(z)$; since α commutes with every element of $\theta_z(\Phi)$, α is contained in the center $\boldsymbol{Q}$ of $\theta_z(\Phi)$. Hence α must be equal to 1_z or -1_z. Our proposition is thereby proved.

3.2. Functions obtained from the points of finite order. We shall now make use of the mapping $\Psi(z)$ attached to the analytic system $\mathcal{S}$, whose definition is given in [AF, no. 12]. This mapping has the following properties.

(Ψ1) $\Psi(z)$ is an analytic mapping of $\mathfrak{H}$ into a projective space.

(Ψ2) For every $z \in \mathfrak{H}$, $\mathcal{P}(z)$ is defined over $\boldsymbol{Q}(\Psi(z))$.

(Ψ3) If z_1 and z_2 are two points of $\mathfrak{H}$ and if $\mathfrak{p}$ is a place of $\boldsymbol{Q}(\Psi(z_1))$ taking values in $\boldsymbol{C}$ such that $\mathfrak{p}(\Psi(z_1)) = \Psi(z_2)$, then we have

$$\mathfrak{p}(A(z_1)) = A(z_2), \quad \mathfrak{p}(T(z_1)) = T(z_2), \quad \mathfrak{p}(U(\alpha, z_1)) = U(\alpha, z_2),$$

where $T(z)$ denotes the graph of the law of composition on $A(z)$, and $U(\alpha, z)$ denotes the graph of $\theta_z(\alpha)$. (For the definition of places and the notation $\mathfrak{p}(V)$, see Appendix of [AF] and [**25** Chap. III].)

Let $\mathfrak{H}_1$ be the set of all generic points of $\mathfrak{H}-\mathfrak{W}$ for Ψ over $\boldsymbol{Q}$. Take and fix a point z_0 of $\mathfrak{H}_1$. Let (V_0, h_0) be a normalized Kummer variety of $\mathcal{P}(z_0)$. If z is a point of $\mathfrak{H}_1$, there exists an isomorphism σ of $\boldsymbol{Q}(\Psi(z_0))$ onto $\boldsymbol{Q}(\Psi(z))$ such that $\Psi(z_0)^\sigma = \Psi(z)$; we have then $\mathcal{P}(z_0)^\sigma = \mathcal{P}(z)$. Put

$$V(z) = V_0^\sigma, \quad h_z = h_0^\sigma.$$

(V_z, h_z) is obviously a normalized Kummer variety of $\mathcal{P}(z)$. Now let $z \to u(z)$ be an analytic mapping of $\mathfrak{H}$ into $\boldsymbol{C}^2$. Put

$$\Theta_u(z) = A(u(z), z),$$

and consider, for every $z \in \mathfrak{H}_1$, the point $h_z(\Theta_u(z))$ lying on the variety $V(z)$. As h_z is defined over $\boldsymbol{Q}(\Psi(z))$, the quotients of the coordinates of this point are contained in $\boldsymbol{Q}(\Psi(z), \Theta_u(z))$. Let $\mathfrak{H}_1(u)$ be the set of all generic points of $\mathfrak{H}-\mathfrak{W}$ for Ψ and Θ_u over $\boldsymbol{Q}$. Take and fix a point z_1 of $\mathfrak{H}_1(u)$. Then there exist elements $y_1, \cdots, y_M$ of $\boldsymbol{Q}(\Psi(z_1), \Theta_u(z_1))$ such that

$$h_{z_1}(\Theta_u(z_1)) = (1, y_1, \cdots, y_M).$$

Let $g_1, \cdots, g_M$ be the elements of $\boldsymbol{Q}(\Psi, \Theta_u)$ corresponding to $y_1, \cdots, y_M$ by the canonical isomorphism of $\boldsymbol{Q}(\Psi, \Theta_u)$ onto $\boldsymbol{Q}(\Psi(z_1), \Theta_u(z_1))$. Then $g_1, \cdots, g_M$ are meromorphic functions on $\mathfrak{H}$; and for every $z \in \mathfrak{H}_1(u)$, we have

$$h_z(A(u(z), z)) = (1, g_1(z), \cdots, g_M(z)).$$

Now consider the case where $u(z)$ is defined by

$$u(z) = \chi(\xi)e(z),$$

where ξ is an element of Φ. In this case we denote by $g_\nu(\xi, z)$ the meromorphic function $g_\nu(z)$ and put $\mathfrak{H}_1(\xi) = \mathfrak{H}_1(u)$. Then, for every $z \in \mathfrak{H}_1(\xi)$, we have

$$h_z(A(\chi(\xi)e(z), z)) = (1, g_1(\xi, z), \cdots, g_M(\xi, z)). \tag{4}$$

PROPOSITION 3.2. *Notations being as above, for every $\xi \in \Phi$ and $\gamma \in \Gamma(\mathfrak{o})$, we have*

$$g_\nu(\xi\gamma, z) = g_\nu(\xi, \gamma[z]) \qquad (1 \leqq \nu \leqq M).$$

PROOF. Let z be a point of $\mathfrak{H}_1 \cap \gamma^{-1}(\mathfrak{H}_1)$. Putting

$$z'=\gamma[z],\quad \chi(\gamma)=\begin{pmatrix} a & b \\ c & d\end{pmatrix},\quad s=cz+d\,,$$

we get $s\cdot e(z')=\chi(\gamma)e(z)$. We can find an isomorphism η of $\mathcal{P}(z)$ onto $\mathcal{P}(z')$ such that $\eta A(sx,z)=A(x,z')$ (cf. the proof of Proposition 15 of [AF]). As z and z' are generic for Ψ over $\boldsymbol{Q}$, there exists an isomorphism σ of $\boldsymbol{Q}(\Psi(z))$ onto $\boldsymbol{Q}(\Psi(z'))$ such that $\Psi(z)^\sigma=\Psi(z')$; we have then $\mathcal{P}(z)^\sigma=\mathcal{P}(z')$. Since $\mathcal{P}(z)$ is isomorphic to $\mathcal{P}(z')$, σ must leave invariant the elements of the field of moduli of $\mathcal{P}(z)$. Therefore, by the property (K3) of normalized Kummer variety, the equality $h_z^\sigma\circ\eta=h_z$ holds. By our construction of h_z, we have $h_z^\sigma=h_{z'}$, so that

$$h_z(A(sx,z))=h_{z'}(\eta A(sx,z))=h_{z'}(A(x,z'))\,.$$

Substituting $\chi(\xi)e(z')$ for x, we obtain

$$h_z(A(\chi(\xi\gamma)e(z),z))=h_{z'}(A(\chi(\xi)e(z'),z'))\,.$$

If we take z sufficiently generic, this proves the relation of our proposition.

PROPOSITION 3.3. *Let ξ and ξ_1 be two elements of Φ. Then*

$$g_\nu(\xi,z)=g_\nu(\xi_1,z)$$

holds for every ν if and only if

$$\xi\equiv\pm\xi_1\qquad\mathrm{mod.}\,\mathfrak{o}\,.$$

PROOF. If $\xi\equiv\pm\xi_1\,\mathrm{mod.}\,\mathfrak{o}$, we have

$$\chi(\xi)e(z)\equiv\pm\chi(\xi_1)e(z)\qquad\mathrm{mod.}\,D(z)\,.$$

This implies $A(\chi(\xi)e(z),z)=\pm A(\chi(\xi_1)e(z),z)$. Since $h_z(\pm x)=h_z(x)$, we obtain

$$h_z(A(\chi(\xi)e(z),z))=h_z(A(\chi(\xi_1)e(z),z))\,.\tag{5}$$

This proves the "if" part of our proposition. Conversely, suppose that $g_\nu(\xi,z)=g_\nu(\xi_1,z)$ holds for every ν. Then, for every $z\in\mathfrak{H}_1(\xi)\cap\mathfrak{H}_1(\xi_1)$, the equality (5) holds. By Proposition 3.1, we have $A(\chi(\xi)e(z),z)=\pm A(\chi(\xi_1)e(z),z)$. Hence, we must have $\chi(\xi)e(z)\equiv\pm\chi(\xi_1)e(z)\,\mathrm{mod.}\,D(z)$, and so $\xi\equiv\pm\xi_1\,\mathrm{mod.}\,\mathfrak{o}$. This completes our proof.

3.3. Automorphic functions belonging to congruence-subgroups. Let $\mathfrak{a}$ be an integral right $\mathfrak{o}$-ideal. We denote by $\Gamma_{\mathfrak{a}}^*$ the subgroup of $\Gamma(\mathfrak{o})$ composed of the elements γ such that $\gamma\equiv\pm1\,\mathrm{mod.}\,\mathfrak{a}$. Then $\Gamma_{\mathfrak{a}}^*$ is of finite index in $\Gamma(\mathfrak{o})$. We denote by $\mathfrak{K}(\mathfrak{a})$ the field of automorphic functions on $\mathfrak{H}$ with respect to $\Gamma_{\mathfrak{a}}^*$.

PROPOSITION 3.4. *Let $\mathfrak{a}=\alpha\mathfrak{o}$ be an integral right $\mathfrak{o}$-ideal. Then we have*

$$\mathfrak{K}(\mathfrak{o}\,;\mathfrak{a})=\boldsymbol{C}(f_i(z),g_j(\alpha^{-1},z)\mid 1\leqq i\leqq m,1\leqq j\leqq M)\,,$$

where the f_i and the g_j are the meromorphic functions defined by (3) *and* (4) *of* §3.2.

PROOF. Let γ be an element of $\Gamma(\mathfrak{o})$. By Propositions 3.2 and 3.3,

$g_j(\alpha^{-1}, \gamma[z]) = g_j(\alpha^{-1}, z)$ holds for every j if and only if $\gamma \equiv \pm 1 \bmod. \mathfrak{a}$, On the other hand, we have obviously

$$\theta_z(\alpha) A(\chi(\alpha^{-1}) e(z), z) = 0\,;$$

hence, by Proposition 2.6, for every $z \in \mathfrak{H}_1(\alpha^{-1})$, the coordinates $g_j(\alpha^{-1}, z)$ of the point $h_z(A(\chi(\alpha^{-1})e(z), z))$ are algebraic over the field of moduli $\boldsymbol{Q}(f_i(z))$ of $\mathcal{P}(z)$. If follows that the functions $g_j(\alpha^{-1}, z)$ are algebraic over the function-field $\boldsymbol{Q}(f_i)$. This proves our proposition, since the equality $\mathfrak{K}(\mathfrak{o}) = \boldsymbol{C}(f_i)$ holds.

REMARK. Suppose that $\mathfrak{a} = \alpha\mathfrak{o}$ is an integral two-sided $\mathfrak{o}$-ideal. Then, we see that, for every $\beta \in \mathfrak{o}, g_j(\beta\alpha^{-1}, z)$ is invariant under $\Gamma(\mathfrak{o}\,; \mathfrak{a})$ and algebraic over $\boldsymbol{Q}(f_i)$. Hence we can write also

$$\mathfrak{K}(\mathfrak{o}\,; \mathfrak{a}) = \boldsymbol{C}(f_i(z), g_j(\beta\alpha^{-1}, z) \mid 1 \leqq i \leqq m, 1 \leqq j \leqq M, \beta \in \mathfrak{o}).$$

3.4. Generic members of the system $\mathcal{S}$. In order to make our later discussion easy, we recall here the definition of the variety $\mathcal{F}(A, \theta)$ introducing some new notations. Let $\mathcal{P} = (A, C, \theta)$ be a polarized abelian variety of type $\mathfrak{r}$. We assume that A is a variety in a projective space P^N of dimension N and C is the polarization determined by the hyperplane sections. Fix a basis $\{r_1, \cdots, r_d\}$ of $\mathfrak{r}$ over $\boldsymbol{Z}$. Let φ be a non-degenerate projective transformation in P^N and $v_1, \cdots, v_d$ be d points on A. Let W_ν be the graph of the rational mapping

$$x \to \varphi[\theta(r_\nu)\varphi^{-1}(x) + v_\nu]$$

of A into itself. Put

$$T(\varphi, v_1, \cdots, v_d) = c(\varphi(A)) \times c(W_1) \times \cdots \times c(W_d)$$

and $M = (N+1)^2 - 1$. We can regard φ as a point in the projective space P^M; then T defines a rational mapping of $P^M \times A \times \cdots \times A$ into a certain product of projective spaces. The image $T(P^M \times A \times \cdots \times A)$ is nothing but the variety $\mathcal{F}(A, \theta)$; we call it the projective family of (A, θ) with respect to $\{r_1, \cdots, r_d\}$. Let U be the set of the elements in P^M which are non-degenerate as projective transformations of P^N. Then U is an open subset of P^M in the sense of Zariski-topology. We observe that T is defined at every point on $U \times A \times \cdots \times A$. Denote by $\mathcal{F}^*(A, \theta)$ the set-theoretical image $T(U \times A \times \cdots \times A)$. By Lemma 8 of [AF], we have $\dim \mathcal{F}(A, \theta) = \dim (P_M \times A \times \cdots \times A)$, so that $\mathcal{F}^*(A, \theta)$ contains an open subset of $\mathcal{F}(A, \theta)$ in the sense of Zariski-topology.

PROPOSITION 3.5. *Let k be a subfield of $\boldsymbol{C}$ composed of countably infinite elements. $\mathcal{P}(z), \mathcal{F}(z), \Psi(z)$ being as in* § 3.1 *and* § 3.2, *let z_0 be a generic point for Ψ over k and y an arbitrary point on $\mathfrak{H}$. Then we have* $\dim_k c(\mathcal{F}(z_0) \geqq \dim_k c(\mathcal{F}(y))$. *Suppose that*

(6) $$\dim_k c(\mathcal{F}(z_0)) = \dim_k c(\mathcal{F}(y)).$$

Then, there exists an isomorphism σ of the universal domain over k such that

$\mathcal{P}(z_0)^\sigma$ is isomorphic to $\mathcal{P}(y)$.

PROOF. Take a place $\mathfrak{p}$ of the field $k(\Psi(z_0))$ such that, for every function f in $k(\Psi(z))$ holomorphic at y, $\mathfrak{p}(f(z_0))=f(y)$. The existence of such a place $\mathfrak{p}$ is shown in the proof of Theorem 1 of [AF]. We have then $\mathfrak{p}(\mathcal{T}(z_0))\supset\mathcal{T}(y)$. Put

$$K_0=k(c(\mathcal{T}(z_0))),\quad K=k(c(\mathcal{T}(y)))\,.$$

Then, the varieties $\mathcal{T}(z_0)$ and $\mathcal{T}(y)$ are respectively defined over K_0 and K. We can find a point a on $\mathcal{T}(z_0)$ and a point b on $\mathcal{T}(y)$ such that $a\rightarrow b$ ref. $\mathfrak{p}$, and, a is algebraic over K_0 and b is algebraic over K. Moreover, we can take a and b so that $a\in\mathcal{T}^*(A_{z_0},\theta_{z_0})$, $b\in\mathcal{T}^*(A_y,\theta_y)$. Then, by the definition of $\mathcal{T}^*$, there exist non-degenerate projective transformations φ,ψ and points $u_1,\cdots,u_d$ on $A(z_0)$, $v_1,\cdots,v_d$ on $A(y)$ such that

$$T(\varphi,u_1,\cdots,u_d)=a,\quad T(\psi,v_1,\cdots,v_d)=b\,.$$

Put $B_1=\varphi(A(z_0))$, $B_2=\psi(A(y))$. As B_1 is defined over $k(a)$, we can put into B_1 a structure of abelian variety defind over an algebraic extension L_1 of $k(a)$; we can then define easily a polarized abelian variety $\mathcal{P}_1=(B_1,C_1,\theta_1)$ of type $\mathfrak{o}$, defined over L_1, such that φ defines, up to a constant, an isomorphism of $\mathcal{P}(z_0)$ onto $\mathcal{P}_1$. We can find similarly an algebraic extension L_2 of $k(b)$ and a polarized abelian variety $\mathcal{P}_2=(B_2,C_2,\theta_2)$, defined over L_2, such that ψ defines, up to a constant, an isomorphism of $\mathcal{P}(y)$ onto $\mathcal{P}_2$. We have clearly

$$\mathcal{T}(A_{z_0},\theta_{z_0})=\mathcal{T}(B_1,\theta_1),\quad \mathcal{T}(A_y,\theta_y)=\mathcal{T}(B_2,\theta_2)\,.$$

It follows that $K_0\subset L_1, K\subset L_2$. We have therefore $\dim_k a=\dim_k K_0$, $\dim_k b=\dim_k K$; as b is a specialization of a over k, we have $\dim_k K_0\geqq\dim_k K$; this proves our first assertion. Now the assumption (6) implies

$$\dim_k a=\dim_k b\,.$$

Hence b must be a generic specialization of a over k; so there exists an isomorphism σ of $k(a)$ onto $k(b)$ such that $a^\sigma=b$. Extend this isomorphism to an isomorphism of the universal domain and denote it again by σ. On account of the definition of $T, a^\sigma=b$ implies $B_1^\sigma=B_2$. We may assume, without any loss of generality, that σ maps the origin of B_1 onto the origin of B_2. Then, again by the definition of T and by the equality $a^\sigma=b$, we see that $\mathcal{P}_1^\sigma=(B_1^\sigma,C_1^\sigma,\theta_1^\sigma)$ coincides with $\mathcal{P}_2=(B_2,C_2,\theta_2)$. This proves our proposition.

REMARK. Proposition 3.5 holds for a more general system of polarized abelian varieties constructed in [AF, no. 11]; in the above proof, we have only to substitute $\mathfrak{o}$ and $\mathfrak{H}$ for $\mathfrak{r}$ and $\mathfrak{Z}$. We also note that in the present case of quaternion algebra, we have

$$\dim_k c(\mathcal{T}(z_0))=1\,,$$

on account of Theorem 6 of [AF].

§ 4. Algebro-geometric theory of modular correspondences.

4.1. Determination of Galois groups. $\mathfrak{o}$ being as before an order in Φ, we assume henceforth that $\mathfrak{o}$ is *maximal*. Let $\mathfrak{a}$ be an integral two-sided $\mathfrak{o}$-ideal; in this § we denote by $G_{\mathfrak{a}}=G(\mathfrak{a})$ the multiplicative group of regular elements of the ring $\mathfrak{o}/\mathfrak{a}$ and by $S_{\mathfrak{a}}=S(\mathfrak{a})$ the subgroup of $G_{\mathfrak{a}}$ consisting of the residue-classes of the elements α such that $N(\alpha)\equiv 1 \bmod. \mathfrak{a}\frown \boldsymbol{Z}$. It is clear that $S_{\mathfrak{a}}$ is a normal subgroup of $G_{\mathfrak{a}}$. By Lemma 1.4, the mapping $\beta\rightarrow N(\beta)$ is an isomorphism of $G_{\mathfrak{a}}/S_{\mathfrak{a}}$ onto the multiplicative group of regular elements of $\boldsymbol{Z}/(\boldsymbol{Z}\frown\mathfrak{a})$. We note that if $\mathfrak{a}$ is of the form (3) of § 1.2, we have $\boldsymbol{Z}\frown\mathfrak{a}=(a_0N(\mathfrak{p}_1\cdots\mathfrak{p}_s))$. As before let Γ denote the group of units γ in $\mathfrak{o}$ such that $N(\gamma)=1$, and $\Gamma_{\mathfrak{a}}^{*}$ the subgroup of Γ consisting of the elements γ such that $\gamma\equiv\pm 1 \bmod. \mathfrak{a}$. Applying Lemma 1.3 to the case $b=1$, we observe that every element of $S_{\mathfrak{a}}$ has a representative in Γ. It follows that $\Gamma/\Gamma_{\mathfrak{a}}^{*}$ is canonically isomorphic to $S_{\mathfrak{a}}/\{\pm 1\}$.

Let $\mathcal{P}(z)$ be a member of our system $\mathcal{S}$ and $K_1=K_{1,z}$ the field of moduli of $\mathcal{P}(z)$. By Proposition 3.5, we have $\dim_{\boldsymbol{Q}} K_1=0$ or 1. Let (V, h) be a normalized Kummer variety of $\mathcal{P}(z)$. For every integral two-sided $\mathfrak{o}$-ideal $\mathfrak{a}$, we put

$$\mathfrak{g}(\mathfrak{a}, A_z)=\{t\in A_z \mid \theta_z(\alpha)t=0 \quad \text{for every } \alpha\in\mathfrak{a}\},$$

and denote by $K_{\mathfrak{a}}=K_{\mathfrak{a},z}$ the field generated over K_1 by the points $h(t)$ for $t\in\mathfrak{g}(\mathfrak{a}, A_z)$. By Proposition 2.3, $K_{\mathfrak{a}}$ does not depend on the choice of (V, h); and by Proposition 2.6, $K_{\mathfrak{a}}$ is a Galois extension of K_1. Our purpose in this § is to determine the Galois group of $K_{\mathfrak{a}}$ over K_1 in the case $\dim_{\boldsymbol{Q}} K_1=1$.

PROPOSITION 4.1. *Notations being as above, there exists an element t of $\mathfrak{g}(\mathfrak{a}, A_z)$ satisfying the following conditions:*

i) $\mathfrak{g}(\mathfrak{a}, A_z)=\theta_z(\mathfrak{o})t$;

ii) $\theta_z(\alpha)t=0\Rightarrow\alpha\in\mathfrak{a}$.

PROOF. As every $\mathfrak{o}$-ideal is a principal ideal, there exists an element α_0 such that $\mathfrak{a}=\mathfrak{o}\alpha_0$. We have then also $\mathfrak{a}=\alpha_0\mathfrak{o}$, since $\mathfrak{a}$ is a two-sided $\mathfrak{o}$-ideal and $\mathfrak{o}$ is maximal. Put $t=\Lambda(\chi(\alpha_0^{-1})e(z), z)$. It is easy to verify this point satisfies the conditions.

If t_0 is a point of $\mathfrak{g}(\mathfrak{a}, A_z)$ satisfying the conditions i) and ii), we observe that the mapping $\alpha\rightarrow\theta_z(\alpha)t_0$ gives an isomorphism of $\mathfrak{o}/\mathfrak{a}$ onto $\mathfrak{g}(\mathfrak{a}, A_z)$. It follows from this fact that the conditions i) and ii) of the above proposition are equivalent to each other. We call an element t of $\mathfrak{g}(\mathfrak{a}, A_z)$ satisfying these conditions a *primitive element* of $\mathfrak{g}(\mathfrak{a}, A_z)$.

Now let $\mathfrak{G}_{\mathfrak{a}}$ denote the Galois group of $K_{\mathfrak{a}}$ over K_1.

PROPOSITION 4.2. *Let t_0 be a primitive element of $\mathfrak{g}(\mathfrak{a}, A_z)$. Then, for every element σ of $\mathfrak{G}_{\mathfrak{a}}$, there exists an element $\alpha_\sigma\in\mathfrak{o}$ such that*

(1) $$h(\theta_z(\beta)t_0)^\sigma = h(\theta_z(\beta\alpha_\sigma)t_0)$$

for every $\beta \in \mathfrak{o}$. If K_1 is not algebraic over $\boldsymbol{Q}$, such an element α_σ is uniquely determined modulo $\mathfrak{a}$ up to the factors ± 1.

PROOF. Let σ be an element of $\mathfrak{G}_\mathfrak{a}$; extend σ to an isomorphism of the universal domain into itself and denote it again by σ. Since σ leaves invariant the elements of K_1, there exists an isomorphism η of $\mathcal{P}$ onto $\mathcal{P}^\sigma$; by the property (K3) of normalized Kummer variety, we have $h^\sigma \circ \eta = h$. We see easily that $\eta^{-1}t_0^\sigma$ is contained in $\mathfrak{g}(\mathfrak{a}, A_z)$. Hence, by the property i) of Proposition 4.1, there exists an element $\alpha_\sigma \in \mathfrak{o}$ such that $\eta^{-1}t_0^\sigma = \theta_z(\alpha_\sigma)t_0$. We have then, for every $\beta \in \mathfrak{o}$,

$$h(\theta_z(\beta)t_0)^\sigma = h^\sigma(\theta_z^\sigma(\beta)t_0^\sigma) = h(\eta^{-1}\theta_z^\sigma(\beta)t_0^\sigma) = h(\theta_z(\beta)\eta^{-1}t_0^\sigma) = h(\theta_z(\beta\alpha_\sigma)t_0).$$

This proves the first assertion. Suppose that K_1 is not algebraic over $\boldsymbol{Q}$ and we have $h(t_0)^\sigma = h(\theta_z(\gamma)t_0)$ for an element $\gamma \in \mathfrak{o}$; we have then, by Proposition 3.1, $\theta_z(\alpha_\sigma)t_0 = \pm\theta_z(\gamma)t_0$. As t_0 is a primitive element of $\mathfrak{g}(\mathfrak{a}, A_z)$, we have $\alpha_\sigma \equiv \pm\gamma \bmod. \mathfrak{a}$; this completes the proof.

If K_1 is not algebraic over $\boldsymbol{Q}$, we observe that the mapping $\sigma \rightarrow \alpha_\sigma$ gives an isomorphism of $\mathfrak{G}_\mathfrak{a}$ into $G_\mathfrak{a}/\{\pm 1\}$; this isomorphism depends on the choice of a primitive element t_0 of $\mathfrak{g}(\mathfrak{a}, A_z)$. If we choose another primitive element of $\mathfrak{g}(\mathfrak{a}, A_z)$, the isomorphism is transformed by an inner automorphism of $G_\mathfrak{a}/\{\pm 1\}$.

THEOREM 2. *Suppose that the field of moduli K_1 of $\mathcal{P}(z)$ is not algebraic over $\boldsymbol{Q}$. Then the following assertions hold.*

i) *The Galois group $\mathfrak{G}_\mathfrak{a}$ of $K_\mathfrak{a}$ over K_1 is isomorphic to $G_\mathfrak{a}/\{\pm 1\}$ by the correspondence $\sigma \rightarrow \alpha_\sigma$ defined by the relation (1) of Proposition 4.2.*

ii) *Let a be the smallest positive integer divisible by $\mathfrak{a}$ and ζ_a a primitive a-th root of unity. Then, $K_1(\zeta_a)$ is the subfield of $K_\mathfrak{a}$ corresponding to the subgroup $S_\mathfrak{a}/\{\pm 1\}$ of $G_\mathfrak{a}/\{\pm 1\}$.*

iii) *$\boldsymbol{Q}(\zeta_a)$ is algebraically closed in $K_\mathfrak{a}$.*

iv) *If α_σ is a representative of the element of $G_\mathfrak{a}/\{\pm 1\}$ corresponding to an element σ of $\mathfrak{G}_\mathfrak{a}$, we have $\zeta_a^\sigma = \zeta_a^{N(\alpha_\sigma)}$.*

PROOF. By virtue of Proposition 3.5, our theorem is established if we prove the assertions i-iv) for any one of the points z of $\mathfrak{H}$ such that $\dim_{\boldsymbol{Q}} c(\mathcal{T}(z)) = 1$. Therefore, in the course of our proof, we may assume, as occasion demands, the points z to be sufficiently generic. For convenience' sake, we use the letter y instead of z for a sufficiently generic point of $\mathfrak{H}$, reserving the letter z for the variable. Now the f_i being as in (3) of § 3.1, we have

$$K_1 = \boldsymbol{Q}(f_1(y), \cdots, f_m(y)).$$

Let α be an element of $\mathfrak{o}$ such that $\mathfrak{a} = \alpha\mathfrak{o}$; put $t_0 = \Lambda(\chi(\alpha^{-1})e(y), y)$. Then t_0 is a primitive element of $\mathfrak{g}(\mathfrak{a}, A_y)$; and we have $h_y(\theta_y(\beta)t_0) = h_y(\Lambda(\chi(\beta\alpha^{-1})e(y), y))$, so that

$$K_{\mathfrak{a}}=K_1(g_j(\beta\alpha^{-1},y)\mid 1\leqq j\leqq M, \beta\in\mathfrak{o}),$$

where the g_j are the functions determined by (4) of § 3.2. Let $\bar{\gamma}$ be an element of $S_{\mathfrak{a}}$. By Lemma 1.3, there exists an element γ of $\mathfrak{o}$ such that $N(\gamma)=1$ and $\bar{\gamma}$ is the class of γ modulo $\mathfrak{a}$. If y is sufficiently generic, $K_{\mathfrak{a}}$ is isomorphic to the function-field

$$(2)\qquad \boldsymbol{Q}(f_i(z), g_j(\beta\alpha^{-1},z)\mid 1\leqq i\leqq m, 1\leqq j\leqq M, \beta\in\mathfrak{o}),$$

and K_1 corresponds to $\boldsymbol{Q}(f_i(z))$. As $\mathfrak{a}$ is a two-sided $\mathfrak{o}$-ideal and $\mathfrak{o}$ is maximal, we have $\alpha\mathfrak{o}\alpha^{-1}=\mathfrak{o}$, so that $\alpha\gamma\alpha^{-1}$ is a unit of $\mathfrak{o}$. Put $\gamma_1=\alpha\gamma\alpha^{-1}$. By proposition 3.2, we have

$$g_j(\beta\alpha^{-1},\gamma_1[z])=g_j(\beta\gamma\alpha^{-1},z).$$

Therefore, the mapping $F(z)\rightarrow F(\gamma_1[z])$ gives an automorphism of the field (2) over $\boldsymbol{Q}(f_i(z))$. If we transform this onto $K_{\mathfrak{a}}/K_1$, we observe that $h_y(\theta_y(\beta)t_0)\rightarrow h_y(\theta_y(\beta\gamma)t_0)$ gives an element of $\mathcal{G}_{\mathfrak{a}}$. In other words, $S_{\mathfrak{a}}/\{\pm 1\}$ is contained in the image of the isomorphism $\sigma\rightarrow\alpha_\sigma$.

Let Y be a divisor contained in the polarization $\mathcal{C}_y$. Then Y corresponds to a Riemann form E_1 on $\boldsymbol{C}^2/D(y)$ defined by

$$E_1(\chi(\xi)e(y), \chi(\eta)e(y))=\mathrm{tr}\,(\rho_1\xi\eta'),$$

where ρ_1 is an element of $\varPhi$. As $E_1(u,v)$ is an integer for every u, v in $D(y)=\chi(\mathfrak{o})e(y)$, $\mathrm{tr}\,(\rho_1\mathfrak{o})$ is an ideal of $\boldsymbol{Z}$. Let q be a positive integer such that $\mathrm{tr}\,(\rho_1\mathfrak{o})=q\boldsymbol{Z}$. Then $q^{-1}E_1$ is also a Riemann form. Let X be a divisor on A_y corresponding to $q^{-1}E_1$. Then qX is algebraically equivalent to Y, so that $X\in\mathcal{C}_y$. Put $q^{-1}\rho_1=\rho, q^{-1}E_1=E$. Then there exists an element $\xi_0\in\mathfrak{o}$ such that $\mathrm{tr}\,(\rho\xi_0)=1$. Now, a being as in ii) of our theorem, consider the symbol $e_{X,a}$ defined in Weil [**29**, no. 75]. By the formula (7) of [**25**, p. 25], we have

$$e_{X,a}(t_2,t_1)=\exp\,(2\pi iaE(x_1,x_2)),$$

where t_1 and t_2 are points on A_y such that $at_1=at_2=0$ and x_1, x_2 are vectors in $\boldsymbol{C}^2$ corresponding to t_1 and t_2. Hence, for every β_1 and β_2 of $\mathfrak{o}$ we have

$$\begin{aligned}(3)\qquad e_{X,a}(\theta_y(\beta_2)t_0, \theta_y(\beta_1)t_0)&=\exp\,(2\pi iaE(\chi(\beta_1\alpha^{-1})e(y), \chi(\beta_2\alpha^{-1})e(y)))\\ &=\exp\,(2\pi iaN(\mathfrak{a})^{-1}\,\mathrm{tr}\,(\rho\beta_1\beta_2')).\end{aligned}$$

Let σ be an element of $\mathcal{G}_a$; extend σ to an isomorphism of the universal domain into itself and denote it again by σ. η and α_σ being as in the proof of Proposition 4.2, $\eta^{-1}(X^\sigma)$ is algebraically equivalent to X, so that $e_{X^\sigma,a}(s_2,s_1)=e_{X,a}(\eta^{-1}s_2,\eta^{-1}s_1)$; we have therefore

$$(4)\quad e_{X,a}(\theta_y(\beta_2)t_0, \theta_y(\beta_1)t_0)^\sigma=e_{X^\sigma,a}(\theta_y^\sigma(\beta_2)t_0^\sigma, \theta_y^\sigma(\beta_1)t_0^\sigma)=e_{X,a}(\theta_y(\beta_2\alpha_\sigma)t_0, \theta_y(\beta_1\alpha_\sigma)t_0).$$

Now assume that $\mathfrak{a}=a\mathfrak{o}$ and put $\zeta_a=e_{X,a}(t_0, \theta_y(\xi_0)t_0)$. By (3), we have $\zeta_a=\exp\,(2\pi ia^{-1})$, so that ζ_a is a primitive a-th root of unity. Substituting ξ_0 and

1 for β_1 and β_2 in (4), we obtain, on account of (3), $\zeta_a^\sigma = \zeta_a^{N(\alpha_\sigma)}$; this proves that ζ_a is contained in K_a and the assertion iv) in the case $\mathfrak{a} = a\mathfrak{o}$.

Coming back to the general case, put $a = \alpha\alpha_1$ and

$$u_0 = \Lambda(\chi(a^{-1})e(y), y).$$

Then α_1 is an element of $\mathfrak{o}$ and we have $t_0 = \theta_y(\alpha_1)u_0$. Obviously K_a contains $K_\mathfrak{a}$. Taking $a\mathfrak{o}$ in place of $\mathfrak{a}$, we obtain an isomorphism $\sigma \rightarrow \beta_\sigma$ of the Galois group $\mathcal{G}_a$ of K_a over K_1 into $G_a/\{\pm 1\}$ by means of the relation $h_y(\theta_y(\beta)u_0)^\sigma = h_y(\theta_y(\beta\beta_\sigma)u_0)$. By what we have just proved, ζ_a is contained in K_a and $\zeta_a^\sigma = \zeta^{N(\beta_\sigma)}$. As $\alpha_1 = a\alpha^{-1}$, we have $\alpha_1\mathfrak{o}\alpha_1^{-1} = \mathfrak{o}$. Put $\alpha_1\beta_\sigma\alpha_1^{-1} = \gamma_\sigma$. We have then, $h_y(\theta_y(\beta)t_0)^\sigma = h_y(\theta_y(\beta\gamma_\sigma)t_0)$, so that $\gamma_\sigma \equiv \pm\alpha_\sigma \bmod. \mathfrak{a}$. Hence an element σ of $\mathcal{G}_a$ leaves invariant the elements of $K_\mathfrak{a}$ if and only if $\alpha_1\beta_\sigma\alpha_1^{-1} \equiv \pm 1 \bmod. \mathfrak{a}$, namely, $\beta_\sigma \equiv \pm 1 \bmod. \mathfrak{a}$. Now if $\beta_\sigma \equiv \pm 1 \bmod. \mathfrak{a}$, we have $N(\beta_\sigma) \equiv 1 \bmod. a\boldsymbol{Z}$, so that $\zeta_a^\sigma = \zeta_a$. This shows that if an element σ of $\mathcal{G}_a$ leaves invariant the elements of $K_\mathfrak{a}$, we have $\zeta_a^\sigma = \zeta_a$. It follows that ζ_a is contained in $K_\mathfrak{a}$; and we have, for every element σ of $\mathcal{G}_a$, $\zeta_a^\sigma = \zeta_a^{N(\beta_\sigma)} = \zeta_a^{N(\alpha_\sigma)}$. This proves the assertion iv) in the general case. In particular, σ is the identity on $K_1(\zeta_a)$ if and only if the class of $\alpha_\sigma \bmod. \mathfrak{a}$ is contained in $S_\mathfrak{a}$. Let $G'_\mathfrak{a}$ denote the image of the isomorphism $\sigma \rightarrow \alpha_\sigma$. We have proved above $G'_\mathfrak{a} \supset S_\mathfrak{a}/\{\pm 1\}$. As $K_1(\zeta_a)$ corresponds to $S_\mathfrak{a}/\{\pm 1\}$, we have

$$[G'_\mathfrak{a} : S_\mathfrak{a}/\{\pm 1\}] = [K_1(\zeta_a) : K_1].$$

If we denote by $\varphi(a)$ the order of the multiplicative group of $\boldsymbol{Z}/a\boldsymbol{Z}$, we get $[G_\mathfrak{a}/\{\pm 1\} : S_\mathfrak{a}/\{\pm 1\}] = [G_\mathfrak{a} : S_\mathfrak{a}] = \varphi(a)$. On the other hand, by Theorem 6 of [AF], $\boldsymbol{Q}$ is algebraically closed in K_1, so that

$$[K_1(\zeta_a) : K_1] = [\boldsymbol{Q}(\zeta_a) : \boldsymbol{Q}] = \varphi(a).$$

It follows that $G'_\mathfrak{a} = G_\mathfrak{a}/\{\pm 1\}$. Thus we have proved the assertions i) and ii). Now let k_1 be the set of elements of $K_\mathfrak{a}$ which is algebraic over $\boldsymbol{Q}$. Then k_1 contains $\boldsymbol{Q}(\zeta_a)$. We have seen above that every element σ of $\mathcal{G}_\mathfrak{a}$ corresponding to $S_\mathfrak{a}$ is obtained from an isomorphism $F(z) \rightarrow F(\gamma_1[z])$ of the function-field (2). Obviously, this isomorphism leaves invariant the elements of k_1. Therefore k_1 must be contained in the subfield of $K_\mathfrak{a}$ corresponding to $S_\mathfrak{a}$; so we have $k_1 \subset K_1(\zeta_a)$, and hence $k_1 = \boldsymbol{Q}(\zeta_a)$. Our theorem is thereby completely proved.

In the above proof, we have used an isomorphism between $K_\mathfrak{a}$ and the function-field (2). Therefore, we may consider Theorem 2 as a statement concerning the Galois-group of the function-field (2) over $\boldsymbol{Q}(f_i)$. If we extend the constant field to the complex number field, the function-fields (2) and $\boldsymbol{Q}(f_i)$ yield $\mathfrak{K}(\mathfrak{o}; \mathfrak{a})$ and $\mathfrak{K}(\mathfrak{o})$. The relation between the fields and the groups is illustrated by the following table.

$$\begin{tikzcd}
 & & & & & & 1 \arrow[d, dash] \\
 & & & & & C K \cong \mathfrak{K}(\mathfrak{o}\,;\,\mathfrak{a}) \arrow[r, dotted, dash] \arrow[dd, dash] & \Gamma_{\mathfrak{a}}{}^{*} \arrow[dd, dash] \\
 & 1 \arrow[rr, dotted, dash] \arrow[dd, dash] & & K_{\mathfrak{a}} \arrow[urr, dash] \arrow[dd, dash] & & & \\
 & & & & & C K_1 \cong \mathfrak{K}(\mathfrak{o}) \arrow[r, dotted, dash] \arrow[dd, dash] & \Gamma \\
 & S_{\mathfrak{a}}/\{\pm 1\} \arrow[rr, dotted, dash] \arrow[ddl, dash] & & K_1(\zeta_{\mathfrak{a}}) \arrow[urr, dash] \arrow[ddl, dash] \arrow[dd, dash] & & & \\
 & & & & & C & \\
G_{\mathfrak{a}}/\{\pm 1\} \arrow[rr, dotted, dash] & & K_1 \arrow[d, dash] & \boldsymbol{Q}(\zeta_{\mathfrak{a}}) \arrow[urr, dash] & & & \\
 & & \boldsymbol{Q} \arrow[ur, dash] & & & &
\end{tikzcd}$$

4.2. Transformations of $\mathcal{P}(z)$. Let $\mathfrak{q}=\mathfrak{o}\alpha$ be an integral left $\mathfrak{o}$-ideal; suppose that $N(\alpha)>0$; and let $\{\mathfrak{q}_1,\cdots,\mathfrak{q}_m\}$ be the set of integral left $\mathfrak{o}$-ideals having the same elementary divisors as $\mathfrak{q}$. $\{\mathfrak{q}_1,\cdots,\mathfrak{q}_m\}$ corresponds to a double coset $\Gamma\alpha\Gamma$; and if we take elements α_i so that $\mathfrak{q}_i=\mathfrak{o}\alpha_i$ and $N(\alpha_i)>0$ for every i, $\Gamma\alpha\Gamma=\bigcup_{i=1}^{m}\Gamma\alpha_i$ is a disjoint sum. Put $q=N(\mathfrak{q})$. We have then $\mathfrak{o}\supset\mathfrak{q}\supset q\mathfrak{o}$, and $\mathfrak{o}/\mathfrak{q}$ is $\mathfrak{o}$-isomorphic to $\mathfrak{o}\alpha'/q\mathfrak{o}$. As we have $\Gamma\alpha\Gamma=\Gamma\alpha'\Gamma$, $\mathfrak{o}\alpha'$ coincides with one of the $\mathfrak{q}_i$. Therefore, $\mathfrak{o}/q\mathfrak{o}$ contains exactly m $\mathfrak{o}$-submodules isomorphic to $\mathfrak{o}/\mathfrak{q}$.

Now let $\mathcal{P}(y)=(A_y, C_y, \theta_y)$ be a member of the system $\mathcal{S}$. By Proposition 4.1, $\mathfrak{g}(q, A_y)$ is isomorphic to $\mathfrak{o}/q\mathfrak{o}$ as $\mathfrak{o}$-module. Hence $\mathfrak{g}(q, A_y)$ has exactly m subgroups $\mathfrak{g}_i$ which are $\mathfrak{o}$-isomophic to $\mathfrak{o}/\mathfrak{q}$.

PROPOSITION 4.3. *Notations being as above, there exist m members $\mathcal{P}(y_i)$ $(1\leqq i\leqq m)$ of $\mathcal{S}$ and a homomorphism λ_i of $\mathcal{P}(y)$ onto $\mathcal{P}(y_i)$ for each i such that the kernel of λ_i is $\mathfrak{g}_i$.*

PROOF. The elements α_i being as above, put $\alpha_i[y]=y_i$; then there exists a complex number a_i such that $\chi(\alpha_i)e(y)=a_i e(y_i)$. We have obviously

$$D(y_i)=\chi(\mathfrak{o})e(y_i)=a_i^{-1}\chi(\mathfrak{q}_i)e(y)\,.$$

Hence the linear mapping $x\rightarrow q a_i^{-1}x$ gives a homomorphism of $\boldsymbol{C}^2/D(y)$ onto $\boldsymbol{C}^2/D(y_i)$; denote by λ_i the homomorphism of $A(y)$ onto $A(y_i)$ corresponding to this linear mapping. Since λ_i commutes with the operation of $\mathfrak{o}$, λ_i is a homomorphism of $\mathcal{P}(y)$ onto $\mathcal{P}(y_i)$ (cf. [AF, no. 20]). Put $t_0=\Lambda(q^{-1}e(y), y)$; then t_0 is a primitive element of $\mathfrak{g}(q, A_y)$; and $\theta_y(\mathfrak{q}_i)t_0$ for $1\leqq i\leqq m$ give the submodules of $\mathfrak{g}(q, A_y)$ which are $\mathfrak{o}$-isomorphic to $\mathfrak{o}/\mathfrak{q}$. We see easily that the kernel of λ_i is $\theta_y(\mathfrak{q}_i)t_0$. This proves our proposition.

Let $\mathfrak{a}$ be an integral two-sided $\mathfrak{o}$-ideal. We shall now consider the fields $K_{1,z}$ and $K_{\mathfrak{a},z}$ for the points y_i determined in Proposition 4.3. The α_i being as above, suppose that y is generic for $\Psi(z), \Psi(\alpha_i[z])$ over $\boldsymbol{Q}$; then there exists an isomorphism ρ_i of $\boldsymbol{Q}(\Psi(y))$ onto $\boldsymbol{Q}(\Psi(y_i))$ such that $\Psi(y)^{\rho_i}=\Psi(y_i)$. We have then

$$\mathcal{P}(y_i)^{\rho_i}=\mathcal{P}(y_i),\quad V(y)^{\rho_i}=V(y_i),\quad h_y^{\rho_i}=h_{y_i}\,. \tag{6}$$

It is easy to see that ρ_i induces an isomorphisms of $K_{\mathfrak{a},y}$ onto $K_{\mathfrak{a},y_i}$ and of $K_{1,y}$ onto K_{1,y_i}. Now suppose that q is prime to $\mathfrak{a}$. Then, the mapping $t\rightarrow$

$(\lambda_i t)^{\rho_i^{-1}}$ gives an $\mathfrak{o}$-automorphism of $\mathfrak{g}(\mathfrak{a}, A_y)$. Hence, if t_0 is a primitive element of $\mathfrak{g}(\mathfrak{a}, A_y)$, there exists an element γ_i of $\mathfrak{o}$, prime to $\mathfrak{a}$, such that

$$(\lambda_i \theta_y(\beta) t_0)^{\rho_i^{-1}} = \theta_y(\beta\gamma_i) t_0$$

for every $\beta \in \mathfrak{o}$. By Theorem 2, there exists an automorphism τ_i of $K_{\mathfrak{a},y}$ over $K_{1,y}$ such that

$$h_y(\theta_y(\beta) t_0)^{\tau_i} = h_y(\theta_y(\beta\gamma_i) t_0)$$

for every $\beta \in \mathfrak{o}$. Put $\sigma_i = \tau_i \rho_i$. We have then

$$h_y(\theta_y(\beta) t_0)^{\sigma_i} = h_{y_i}(\lambda_i \theta_y(\beta) t_0) .$$

We have thus proved the following proposition.

PROPOSITION 4.4. *Let $\mathfrak{a}$ be an integral two-sided $\mathfrak{o}$-ideal and y a point of $\mathfrak{H}$; define $\mathcal{P}(y_i)$ and λ_i as in Proposition 4.3. Suppose that q and $\mathfrak{a}$ are relatively prime. If y is sufficiently generic, there exists, for each i, an isomorphism σ_i of $K_{\mathfrak{a},y}$ onto $K_{\mathfrak{a},y_i}$ such that*

$$c(\mathcal{F}(y))^{\sigma_i} = c(\mathcal{F}(y_i)) , \tag{7}$$

$$h_y(t)^{\sigma_i} = h_{y_i}(\lambda_i t) \tag{8}$$

for every $t \in \mathfrak{g}(\mathfrak{a}, A_y)$.

Since $K_{\mathfrak{a},y}$ is generated over $\boldsymbol{Q}$ by the points $c(\mathcal{F}(y))$ and $h_y(t)$ for $t \in \mathfrak{g}(\mathfrak{a}, A_y)$, the isomorphism σ_i is uniquely determined by (7) and (8).

From now on, we assume y to be so generic that we may apply Proposition 4.4 to $\mathcal{P}(y)$ for any pair of q and $\mathfrak{a}$. By Propositions 2.7 and 2.8, $K_{\mathfrak{a},y_i}$ is contained in $K_{q\mathfrak{a},y}$; this implies in particular that $K_{\mathfrak{a},y_i}$ is algebraic over $K_{1,y}$.

PROPOSITION 4.5. *Notations being as in Proposition 4.4, every conjugate of $c(\mathcal{F}(y_1))$ over $K_{1,y}$ is of the form $c(\mathcal{F}(y_i))$ for $1 \leqq i \leqq m$.*

PROOF. Let τ be an isomorphism of the universal domain into itself leaving invariant the elements of $K_{1,y}$. Then, there exists an isomorphism η of $\mathcal{P}(y)$ onto $\mathcal{P}(y)^\tau$. We see that $\lambda_1^\tau \circ \eta$ is a homomorphism of $\mathcal{P}(y)$ onto $\mathcal{P}(y_1)^\tau$, and, the kernel of $\lambda_1^\tau \circ \eta$ is contained in $\mathfrak{g}(q, A_y)$ and is $\mathfrak{o}$-isomorphic to $\mathfrak{o}/\mathfrak{q}$. Therefore, the kernel of $\lambda_1^\tau \circ \eta$ coincides with one of the $\mathfrak{g}_i$. Then, by i) of Proposition 2.5, $\mathcal{P}(y_1)^\tau$ is isomorphic to one of the $\mathcal{P}(y_i)$. It follows that $\mathcal{F}(y_1)^\tau$ coincides with one of the $\mathcal{F}(y_i)$ on account of Proposition 1 of [AF]; this proves our proposition.

Now let $\mathfrak{b}$ be the set of elements β such that $\beta\mathfrak{o} \subset \mathfrak{q}$. Then $\mathfrak{b}$ is an integral two-sided $\mathfrak{o}$-ideal; and we have $\mathfrak{q} \supset \mathfrak{b} \supset q\mathfrak{o}$. As $\mathfrak{g}_i$ is $\mathfrak{o}$-isomorphic to $\mathfrak{o}/\mathfrak{q}$, we have

$$\theta_y(\beta)\mathfrak{z}_i = \{0\} \Leftrightarrow \beta \in \mathfrak{b} . \tag{9}$$

We shall use this relation in the proof of the following proposition.

PROPOSITION 4.6. *Let $u = (u_1, \cdots, u_l)$ be a set of quantities such that $K_{\mathfrak{a},y} \supset \boldsymbol{Q}(u) \supset K_{1,y}$. Let $\sigma_1, \cdots, \sigma_m$ be the isomorphisms of $K_{\mathfrak{a},y}$ onto the $K_{\mathfrak{a},y_i}$ deter-*

mined by (7) *and* (8) *of Proposition* 4.4. *Then:*

i) $\boldsymbol{Q}(u, c(\mathcal{F}(y_i)))$ *contains* $\boldsymbol{Q}(u^{\sigma_i})$ *for each* i;

ii) $(u^{\sigma_1}, \cdots, u^{\sigma_m})$ *is the complete set of conjugates of* u^{σ_1} *over* $\boldsymbol{Q}(u)$.

PROOF. Let τ be an isomorphism of the universal domain into itself leaving invariant the elements of $\boldsymbol{Q}(c(\mathcal{F}(y)), c(\mathcal{F}(y_1)))$. Then there exist an isomorphism ε of $\mathcal{P}(y)$ onto $\mathcal{P}(y)^\tau$ and an isomorphism ε_1 of $\mathcal{P}(y_1)$ onto $\mathcal{P}(y_1)^\tau$; by the property (K3) of normalized Kummer variety, we have

$$(10) \qquad h_y{}^\tau \circ \varepsilon = h_y, \quad h_{y_1}{}^\tau \circ \varepsilon_1 = h_{y_1}.$$

We observe that the kernel of $\lambda_1{}^\tau \circ \varepsilon$ is $\mathfrak{o}$-isomorphic to $\mathfrak{o}/\mathfrak{q}$. We can apply, on account of (9), Proposition 2.5 to the homomorphisms $\varepsilon_1 \circ \lambda_1$ and $\lambda_1{}^\tau \circ \varepsilon$ of $\mathcal{P}(y)$ onto $\mathcal{P}(y_1)^\tau$; then by ii) of that proposition, $\varepsilon_1 \circ \lambda_1$ and $\lambda_1{}^\tau \circ \varepsilon$ have the same kernel; hence by i) of the same proposition, there exists an automorphism η of $\mathcal{P}(y_1)^\tau$ such that $\eta \circ \varepsilon_1 \circ \lambda_1 = \lambda_1{}^\tau \circ \varepsilon$. By Proposition 3.1, η must be ± 1, so that

$$(11) \qquad \pm \varepsilon_1 \circ \lambda_1 = \lambda_1{}^\tau \circ \varepsilon.$$

Let t_0 be a primitive element of $\mathfrak{g}(\mathfrak{a}, A_y)$ and α_τ be an element of $\mathfrak{o}$ such that

$$(12) \qquad h_y(\theta_y(\beta)t_0)^\tau = h_y(\theta_y(\beta\alpha_\tau)t_0)$$

for every $\beta \in \mathfrak{o}$. Then, by the relation (10), we have

$$(13) \qquad \varepsilon^{-1}(\theta_y(\beta)t_0)^\tau = \pm\theta_y(\beta\alpha_\tau)t_0.$$

The relations (8), (10), (11), (12), (13) yield

$$(14) \quad h_y(\theta_y(\beta)t_0)^{\sigma_1\tau} = h_{y_1}(\lambda_1\theta_y(\beta)t_0)^\tau = h_{y_1}{}^\tau(\lambda_1{}^\tau \circ \varepsilon \circ \varepsilon^{-1}(\theta_y(\beta)t_0)^\tau) = h_{y_1}{}^\tau(\varepsilon_1\lambda_1\theta_y(\beta\alpha_\tau)t_0)$$
$$= h_{y_1}(\lambda_1\theta_y(\beta\alpha_\tau)t_0) = h_y(\theta_y(\beta\alpha_\tau)t_0)^{\sigma_1} = h_y(\theta_y(\beta)t_0)^{\tau\sigma_1}.$$

On the other hand, we have $c(\mathcal{F}(y))^{\sigma_1\tau} = c(\mathcal{F}(y_1)) = c(\mathcal{F}(y))^{\tau\sigma_1}$. This combined with (14) shows $\sigma_1\tau = \tau\sigma_1$, since $K_{\mathfrak{a},y}$ is generated by $c(\mathcal{F}(y))$ and $h_y(\theta_y(\beta)t_0)$. Therefore, if τ leaves invariant the elements of $\boldsymbol{Q}(u, c(\mathcal{F}(y_1)))$, we have $u^{\sigma_1\tau} = u^{\tau\sigma_1} = u^{\sigma_1}$; this proves the assertion i). From i) we obtain

$$[\boldsymbol{Q}(u, u^{\sigma_1}) : \boldsymbol{Q}(u)] = [\boldsymbol{Q}(u, c(\mathcal{F}(y_1)) : \boldsymbol{Q}(u)]$$
$$\leqq [\boldsymbol{Q}(c(\mathcal{F}(y)), c(\mathcal{F}(y_1))) : \boldsymbol{Q}(c(\mathcal{F}(y)))].$$

By Proposition 4.5, the right hand side of this inequality is not greater than m. If $i \neq j$, the kernel of λ_i and λ_j are different from each other; hence, by ii) of Proposition 2.5 and (9), $\mathcal{P}(y_i)$ and $\mathcal{P}(y_j)$ are not isomorphic. It follows that m points $c(\mathcal{F}(y_i))$ are different from each other. Therefore, our proposition is completely proved if we show that u^{σ_i} is a conjugate of u^{σ_1} over $K_{\mathfrak{a},y}$ for every i. Let s be a primitive element of $\mathfrak{g}(q\mathfrak{a}, A_y)$ and α an element of $\mathfrak{o}$ such that $\mathfrak{a} = \alpha\mathfrak{o}$. Put $r = \theta_y(\alpha)s$. Then r is a primitive element of $\mathfrak{g}(q, A_y)$. The ideals $\mathfrak{q}_i$ being as in the first part of this §, we may, after reordering if necessary, assume that $\theta_y(\mathfrak{q}_i)r$ is the kernel of λ_i for each i. Now by iv) of Proposition 1.6, there exists a unit γ_1 of $\mathfrak{o}$ such that

$$\mathfrak{q}_1\gamma_1=\mathfrak{q}_i\,. \tag{15}$$

As q is prime to $\mathfrak{a}$, and as we have $\alpha^{-1}\mathfrak{o}\alpha=\mathfrak{o}$, there exists an element γ of $\mathfrak{o}$ such that

$$\gamma\equiv\alpha^{-1}\gamma_1\alpha \text{ mod.}\, q\mathfrak{o},\quad \gamma\equiv 1 \text{ mod.}\,\mathfrak{a}\,. \tag{16}$$

By Theorem 2, there exists an automorphism ρ of $K_{q\mathfrak{a},y}$ over $K_{1,y}$ such that

$$h_y(\theta_y(\beta)s)^\rho=h_y(\theta_y(\beta\gamma)s) \tag{17}$$

for every $\beta\in\mathfrak{o}$. Obviously qs is a primitive element of $\mathfrak{g}(\mathfrak{a}, A_y)$; and by (16) we have $\beta\gamma\equiv\beta$ mod. $\mathfrak{a}$, so that $\theta_y(\beta\gamma)qs=\theta_y(\beta)qs$. Hence we obtain

$$h_y(\theta_y(\beta)qs)^\rho=h_y(\theta_y(\beta\gamma)qs)=h_y(\theta_y(\beta)qs)\,.$$

This shows that ρ leaves invariant the elements of $K_{\mathfrak{a},y}$. Extend ρ to an isomorphism of the universal domain into itself and denote it again by ρ. As ρ is the identity on $K_{1,y}$, there exists an isomorphism ξ of $\mathcal{P}(y)$ onto $\mathcal{P}(y)^\rho$: and we have $h_y{}^\rho\circ\xi=h_y$. By (16) and (17), we find

$$h_y(\xi^{-1}(\theta_y(\beta)r)^\rho)=h_y(\theta_y(\beta)r)^\rho=h_y(\theta_y(\beta\alpha\gamma\alpha^{-1})r)=h_y(\theta_y(\beta\gamma_1)r)\,,$$

and hence $\xi^{-1}(\theta_y(\beta)r)^\rho=\pm\theta_y(\beta\gamma_1)r$. We have therefore by (15)

$$\xi^{-1}(\theta_y(\mathfrak{q}_1)r)^\rho=\theta_y(\mathfrak{q}_1\gamma_1)r=\theta_y(\mathfrak{q}_i)r\,.$$

This show that the kernel of $\lambda_1{}^\rho\circ\xi$ coincides with the kernel of λ_i. By i) of Proposition 2.5, there exists an isomorphism ξ_1 of $\mathcal{P}(y_i)$ onto $\mathcal{P}(y_1)^\rho$ such that

$$\xi_1\circ\lambda_i=\lambda_1{}^\rho\circ\xi\,. \tag{18}$$

It follows that $c(\mathcal{F}(y_1))^\rho=c(\mathcal{F}(y_i))$ by virtue of Proposition 1 of [AF], and hence

$$c(\mathcal{F}(y))^{\sigma_1\rho}=c(\mathcal{F}(y_i))=c(\mathcal{F}(y))^{\sigma_i}\,. \tag{19}$$

Consider the isomorphisms ρ_i satisfying the relation (6). We have obviously $\mathcal{P}(y_1)^\rho=\mathcal{P}(y_i)^{\rho_i^{-1}\rho_1\rho}$. Applying the property (K3) of normalized Kummer variety to $\mathcal{P}(y_i)$, we have $(h_{y_i})^{\rho_i^{-1}\rho_1\rho}\circ\xi_1=h_{y_i}$, namely,

$$h_{y_1}{}^\rho\circ\xi_1=h_{y_i}\,. \tag{20}$$

As ρ leaves invariant the elements of $K_{\mathfrak{a},y}$, we have, for every $t\in\mathfrak{g}(\mathfrak{a}, A_y)$, $h_y(t)=h_y{}^\rho(t^\rho)=h_y(\xi^{-1}t^\rho)$, so that

$$\xi^{-1}t^\rho=\pm t\,. \tag{21}$$

By (8), (18), (20), (21), we obtain, for every $t\in\mathfrak{g}(\mathfrak{a}, A_y)$,

$$h_y(t)^{\sigma_1\rho}=h_{y_1}(\lambda_1 t)^\rho=h_{y_1}{}^\rho(\lambda_1{}^\rho\xi\xi^{-1}t^\rho)=h_{y_1}{}^\rho(\xi_1\lambda_i t)=h_{y_i}(\lambda_i t)=h_y(t)^{\sigma_i}\,.$$

This together with (19) shows $\sigma_1\rho=\sigma_i$. Hence we have $u^{\sigma_i}=(u^{\sigma_1})^\rho$. It follows that u^{σ_i} is a conjugate of u^{σ_1} over $K_{\mathfrak{a},y}$. This completes the proof.

PROPOSITION 4.7. *Notations being as in Proposition 4.4, let τ_q be the automorphism of $K_{\mathfrak{a},y}$ corresponding to the element q of $G_{\mathfrak{a}}$. Then there exists a isomorphism τ of the universal domain into itself such that $\tau=\sigma_1$ on $K_{\mathfrak{a},y}$ an $\tau=\sigma_1^{-1}\tau_q$ on $K_{\mathfrak{a},y_1}$.*

PROOF. As the kernel of λ_1 is contained in $\mathfrak{g}(q, A_y)$, there exists a homomorphism μ of $A(y_1)$ onto A_y such that $\mu\circ\lambda=q1_y$, where 1_y denotes th identity of $\mathcal{A}(A_y)$. By Proposition 2.4, μ is a homomorphism of $\mathcal{P}(y_1)$ ont $\mathcal{P}(y)$. We observe that the kernel of μ is $\mathfrak{o}$-isomorphic to $\mathfrak{o}/\mathfrak{q}$. Therefore, i y is sufficiently generic, we can apply Proposition 4.4 to $\mathcal{P}(y_1)$; we obtain the an isomorphism σ of $K_{\mathfrak{a},y_1}$ onto $K_{\mathfrak{a},y}$ such that

$$c(\mathcal{T}(y_1))^{\sigma}=c(\mathcal{T}(y)), \tag{22}$$

$$h_{y_1}(t)^{\sigma}=h_y(\mu t), \tag{23}$$

for every $t\in\mathfrak{g}(\mathfrak{a}, A(y))$. Extend σ to an isomorphism of the universal domai and denote it again by σ. By (22), there exists an isomorphism ε of $\mathcal{P}(y)$ ont $\mathcal{P}(y_1)^{\sigma}$. The isomorphisms ρ_i being as in (6), we have $\mathcal{P}(y_1)^{\sigma}=\mathcal{P}(y)^{\rho_1\sigma}$, so tha by the property (K3) of normalized Kummer variety, we obtain $h_{y_1}{}^{\sigma}\circ\varepsilon=h_y{}^{\rho_1\sigma}\circ\varepsilon=h_y$. Hence, for every $t\in\mathfrak{g}(\mathfrak{a}, A_y)$, we get, by (23),

$$h_y(t)=h_{y_1}{}^{\sigma}(\varepsilon t)=h_{y_1}((\varepsilon t)^{\sigma^{-1}})^{\sigma}=h_y(\mu(\varepsilon t)^{\sigma^{-1}}).$$

It follows that $t=\pm\mu(\varepsilon t)^{\sigma^{-1}}$, namely

$$t^{\sigma}=\pm\mu^{\sigma}\varepsilon t. \tag{24}$$

Now we observe that $\mu^{\sigma}\circ\varepsilon$ is a homomorphism of $\mathcal{P}(y)$ onto $\mathcal{P}(y)^{\sigma}$ whos kernel is $\mathfrak{o}$-isomorphic to $\mathfrak{o}/\mathfrak{q}$. By i) of Proposition 2.5, there exists, for som i, an isomorphism η of $\mathcal{P}(y_i)$ onto $\mathcal{P}(y)^{\sigma}$ such that

$$\eta\circ\lambda_i=\mu^{\sigma}\circ\varepsilon. \tag{25}$$

We have then

$$c(\mathcal{T}(y))^{\sigma}=c(\mathcal{T}(y_i)). \tag{26}$$

As we have $\mathcal{P}(y)^{\sigma}=\mathcal{P}(y_i)^{\rho_i{}^{-1}\sigma}$, we obtain, by the property (K3),

$$h_y{}^{\sigma}\circ\eta=h_{y_i}{}^{\rho_i{}^{-1}\sigma}\circ\eta=h_{y_i}. \tag{27}$$

In the proof of Proposition 4.6, we have constructed an isomorphism ρ of th universal domain such that ρ leaves invariant the elements of $K_{\mathfrak{a},y}$ and $\sigma_1\rho=\sigma_i$ Put now $\tau=\sigma\rho^{-1}$. Then, by (26), we have

$$c(\mathcal{T}(y))^{\sigma\rho^{-1}}=c(\mathcal{T}(y_i))^{\rho^{-1}}=c(\mathcal{T}(y))^{\sigma_i\rho^{-1}}=c(\mathcal{T}(y))^{\sigma_1},$$

and by (24), (25), (27), (8), for every $t\in\mathfrak{g}(\mathfrak{a}, A_y)$,

$$h_y(t)^{\sigma\rho^{-1}}=h_y{}^{\sigma}(t^{\sigma})^{\rho^{-1}}=h_y{}^{\sigma}(\mu^{\sigma}\varepsilon t)^{\rho^{-1}}=h_y{}^{\sigma}(\eta\lambda_i t)^{\rho^{-1}}=h_{y_i}(\lambda_i t)^{\rho^{-1}}=h_y(t)^{\sigma_i\rho^{-1}}=h_y(t)^{\sigma_1}.$$

Hence we have $\tau=\sigma_1$ on $K_{\mathfrak{a},y}$. Now, by (22),

$$c(\mathscr{F}(y_1))^{\sigma\rho^{-1}}=c(\mathscr{F}(y))^{\rho^{-1}}=c(\mathscr{F}(y))=c(\mathscr{F}(y))^{\tau_q}=c(\mathscr{F}(y_1))^{\sigma_1^{-1}\tau_q},$$

and by (23), (8), for every $t\in\mathfrak{g}(\mathfrak{a},A(y_1))$,

$$h_{y_1}(qt)^{\sigma\rho^{-1}}=h_y(q\mu t)^{\rho^{-1}}=h_y(q\mu t)=h_y(\mu t)^{r_q}=h_{y_1}(\lambda_1\mu t)^{\sigma_1^{-1}\tau_q}=h_{y_1}(qt)^{\sigma_1^{-1}\tau_q}.$$

This shows that $\tau=\sigma_1^{-1}\tau_q$ on $K_{\mathfrak{a},y_1}$; our proposition is thereby proved.

u being as in Proposition 4.6, we have, by Proposition 4.7, $u^{\tau}=u^{\sigma_1}$, $u^{\sigma_1\tau}=u^{\tau_q}$. As τ_q is contained in the center of the group $\mathcal{G}_{\mathfrak{a}}$, we have $\boldsymbol{Q}(u)=\boldsymbol{Q}(u^{\tau_q})$; hence τ gives an automorphism of $\boldsymbol{Q}(u,u^{\sigma_1})$ and maps $\boldsymbol{Q}(u)$ onto $\boldsymbol{Q}(u^{\sigma_1})$. We have therefore, by Proposition 4.6,

$$[\boldsymbol{Q}(u^{\sigma_1},u):\boldsymbol{Q}(u)]=[\boldsymbol{Q}(u,u^{\sigma_1}):\boldsymbol{Q}(u^{\sigma_1})]=m. \tag{28}$$

4.3. Modular correspondences. Let L be a subfield of $K_{\mathfrak{a},y}$ such that

$$L\supset K_{1,y},\quad L\cap\boldsymbol{Q}(\zeta_a)=\boldsymbol{Q}, \tag{29}$$

where a is the smallest positive integer divisible by $\mathfrak{a}$ and ζ_a is a primitive a-th root of unity. By Theorem 2, $\boldsymbol{Q}$ is algebraically closed in L. Hence we can find a complete non-singular curve $\mathfrak{C}=\mathfrak{C}_L$ defined over $\boldsymbol{Q}$ such that we have $L=\boldsymbol{Q}(u)$ for a generic point u of $\mathfrak{C}$ over $\boldsymbol{Q}$. We call $\{\mathfrak{C},u\}$ a model of L. We shall now define certain algebraic correspondences on the curve $\mathfrak{C}$.

Fix an integral left $\mathfrak{o}$-deal $\mathfrak{q}$ and put $N(\mathfrak{q})=q$; suppose that q is prime to $\mathfrak{a}$. Define the isomorphisms $\{\sigma_1,\cdots,\sigma_m\}$ as in Proposition 4.4. Let $X_{\mathfrak{q}}$ be the locus of $u\times u^{\sigma_1}$ on $\mathfrak{C}\times\mathfrak{C}$ over $\boldsymbol{Q}$. We have then, using the notation of Weil [28],

$$X_{\mathfrak{q}}(u)=u^{\sigma_1}+\cdots+u^{\sigma_m}. \tag{30}$$

We call $X_{\mathfrak{q}}$ the *modular correspondence on* $\mathfrak{C}$ *associated with* $\mathfrak{q}$.

Let n be an integer prime to $\mathfrak{a}$ and τ_n be the automorphism of $K_{\mathfrak{a},y}$ corresponding to the element n of $G_{\mathfrak{a}}$. As τ_n is contained in the center of $G_{\mathfrak{a}}$, τ_n induces an automorphism on $L=\boldsymbol{Q}(u)$. Let Y_n be the locus of $u\times u^{\tau_n}$ on $\mathfrak{C}\times\mathfrak{C}$ over $\boldsymbol{Q}$. Obviously, Y_n gives a birational correspondence on $\mathfrak{C}$. By Proposition 4.7, we obtain

$$X_{\mathfrak{q}}'\circ Y_q=X_{\mathfrak{q}},$$

$$d(X_{\mathfrak{q}})=d'(X_{\mathfrak{q}})=m,$$

the notations being as in [28].

Now assume that $\mathfrak{a}$ is prime to $d(\Phi)$. Then we have $\mathfrak{a}=\mathfrak{o}N$ for a positive integer N: and $\mathfrak{o}/\mathfrak{a}$ is isomorphic to the total matric ring $\boldsymbol{M}_2(\boldsymbol{Z}/N\boldsymbol{Z})$. Fix an isomorphism of $\mathfrak{o}/\mathfrak{a}$ onto $\boldsymbol{M}_2(\boldsymbol{Z}/N\boldsymbol{Z})$; then $G_{\mathfrak{a}}$ is identified with the group of regular elements of $\boldsymbol{M}_2(\boldsymbol{Z}/N\boldsymbol{Z})$. Let H be the subgroup of $G_{\mathfrak{a}}$ consisting of the matrices $\begin{pmatrix}a & 0\\ 0 & \pm 1\end{pmatrix}$ for $(a,N)=1$. Let L_N be the subfield of $K_{\mathfrak{a},y}$ corresponding to H. Then we see easily

$$L_N(\zeta_N)=K_{\mathfrak{a},y},\quad L_N\cap \boldsymbol{Q}(\zeta_N)=\boldsymbol{Q}\,.$$

Let $\{\mathfrak{C}_N, u\}$ be a model of L_N. Put $\psi=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$. It is clear that

$$K_{\mathfrak{a},y}=\boldsymbol{Q}(u,\zeta_N)=\boldsymbol{Q}(u^{\psi},\zeta_N)\,.$$

Let Z be the locus of $u\times u^{\psi}$ over $\boldsymbol{Q}(\zeta_N)$; then Z is a birational correspondence on $\mathfrak{C}_N$.

PROPOSITION 4.8 *Let φ_n be an automorphism of $\boldsymbol{Q}(\zeta_N)$ such that $\zeta_N{}^{\varphi_n}=\zeta_N{}^n$. Then we have*

$$Z^{\varphi_n}\circ Y_n=Z\,.$$

As the proof is quite similar to that of Proposition 12 of [22], we omit it.

§ 5. Congruence-relations for modular correspondences.

5.1. In the following treament, we shall make use of the theory of reduction modulo p of algebraic varieties (cf. [**21**, **25**]). We shall use mainly the terminology of [**25**]; and a place (or valuation) will mean a *discrete* one. We recall here only one definition: let U be a variety defined over a field with a place $\boldsymbol{p}$; U is then called *$\boldsymbol{p}$-simple* if the reduction of U modulo $\boldsymbol{p}$ has only one component and its multiplicity is 1.

Let k be a field with a place $\boldsymbol{p}$; we denote by $\boldsymbol{p}(U)$ or $\tilde{U}$ the reduction of any object U modulo $\boldsymbol{p}$. By [**21**, Proposition 5, Theorem 15] (see also [**14**, Appendix]), we obtain

LEMMA R. *Let U be a variety defined over k, which is $\boldsymbol{p}$-simple. Let x be a generic point of U over k and ξ a generic point of $\tilde{U}$ over $\tilde{k}$. Then, the specialization-ring $[x\rightarrow\xi\,;\,\boldsymbol{p}]$ is a discrete valuation ring.*

Hence there exists one and only one extension $\boldsymbol{p}_1$ of $\boldsymbol{p}$ in $k(x)$ such that $\boldsymbol{p}_1(x)=\xi$; we call $\boldsymbol{p}_1$ the place determined by the specialization $x\rightarrow\xi$ ref. $\boldsymbol{p}$.

PROPOSITION 5.1. *Let A be a projective abelian variety, defined over k, satisfying the following conditions:*

i) *there is no hyperplane containing A;*

ii) *the linear system on A defined by hyperplane sections is complete.*

Suppose that A is without defect for $\boldsymbol{p}$ in the sense of [**25**, § 11]. *Then, $\tilde{A}$ satisfies the conditions* i, ii).

PROOF. We can find a prolongation $\{k_1,\boldsymbol{p}_1\}$ of $\{k,\boldsymbol{p}\}$ and a hyperplane section X of A, rational over k_1, so that $\tilde{X}=\boldsymbol{p}(X)$ is a hyperplane section of $\tilde{A}$. Let $L(X;\,k_1)$ and $L(\tilde{X};\,\tilde{k}_1)$ be respectively the set of functions f on A defined over k_1 such that $(f)>-X$ and the set of functions g on $\tilde{A}$ defined over $\tilde{k}_1$ such that $(g)>-\tilde{X}$; denote by $l(X)$ and $l(\tilde{X})$ the dimensions of $L(X;\,k_1)$ over k_1 and of $L(\tilde{X};\,\tilde{k}_1)$ over $\tilde{k}_1$. By our assumption, if we denote by n the dimension of the ambient space for A, we have $l(X)=n+1$. By the result of [**25**, pp. 86-87], $L(X;\ k_1)$ has a base $\{f_0, \cdots, f_n\}$ over k_1 such that $\boldsymbol{p}(f_0), \cdots, \boldsymbol{p}(f_n)$ are linearly independent over $\tilde{k}_1$. Hence, no hyperplane contains $\tilde{A}$. Now by Nishi [**16**], we have $l(X)=l(\tilde{X})$. It follows that $\tilde{A}$ satisfies ii).

Let $\mathcal{P}=(A, C, \theta)$ be a polarized abelian variety of type $\mathfrak{r}$, defined over k. Suppose that A is without defect for $\boldsymbol{p}$. Take a divisor X in C which is rational over k. Then, by [**25**, §11, Proposition 14], $\tilde{X}$ is non-degenerate divisor on $\tilde{A}$; so $\tilde{X}$ determines a polarization on $\tilde{A}$, which we denote by $\tilde{C}$. Let $\tilde{\theta}(\alpha)$ be the reduction of $\theta(\alpha)$ modulo $\boldsymbol{p}$ for every $\alpha \in \mathfrak{r}$. In this way, we obtain a polarized abelian variety $\tilde{\mathcal{P}}=(\tilde{A}, \tilde{C}, \tilde{\theta})$ of type $\mathfrak{r}$, defined over k.

PROPOSITION 5.2. *Let $\mathcal{P}=(A, C, \theta)$ be a polarized abelian variety of type $\mathfrak{r}$, defined over k. Suppose that A is a projective variety satisfying* i, ii) *of Proposition* 5.1 *and that A is without defect for $\boldsymbol{p}$. Then we have*

$$\boldsymbol{p}[\mathcal{T}(A, \theta)] \supset \mathcal{T}(\tilde{A}, \tilde{\theta}).$$

Moreover, if $\mathcal{T}(A, \theta)$ is $\boldsymbol{p}$-simple, we have

$$\boldsymbol{p}[\mathcal{T}(A, \theta)] = \mathcal{T}(\tilde{A}, \tilde{\theta}).$$

PROOF. The first assertion is proved in a straightforward way; the argument is the same as in the proof of [AF, Theorem 1]. Now we note that [AF, Lemma 8] is valid for any polarized abelian variety of type $\mathfrak{r}$ whenever the variety satisfies the conditions i, ii) of Proposition 5.1. Therefore, by the proposition, $\mathcal{T}(A, \theta)$ and $\mathcal{T}(\tilde{A}, \tilde{\theta})$ are of the same dimension; so $\mathcal{T}(\tilde{A}, \tilde{\theta})$ is a component of the cycle $\boldsymbol{p}[\mathcal{T}(A, \theta)]$. Hence, if $\mathcal{T}(A, \theta)$ is $\boldsymbol{p}$-simple, we must have the equality of our proposition.

5.2. Fix a sufficiently generic point y on $\mathfrak{H}$ and denote $\mathcal{P}_y=(A_y, C_y, \theta_y)$, (V_y, h_y) simply by $\mathcal{P}=(A, C, \theta)$, (V, h), respectively. Let U be the locus of $c(\mathcal{T}(y))$ over $\boldsymbol{Q}$. Let k_0 be a field of definition for $\mathcal{P}$, which is finitely generated over $\boldsymbol{Q}$. Fix a set of independent variables $(t_1, \cdots, t_s)$ in k_0 such that k_0 is algebraic over $\boldsymbol{Q}(t_1, \cdots, t_s)$. For each prime number p, we obtain a place of $\boldsymbol{Q}$: $a \rightarrow a \bmod p$. We extend this to a place $\boldsymbol{p}_0$ of k_0 as follows: first define a place p_1 of $\boldsymbol{Q}(t_1, \cdots, t_s)$ so that $p_1=p$ on $\boldsymbol{Q}$ and $p_1(t_1), \cdots, p_1(t_s)$ are independent variables over $\boldsymbol{Z}/p\boldsymbol{Z}$; then extend p_1 to a place $\boldsymbol{p}_0$ of k_0. Such a place $\boldsymbol{p}_0$ is not necessarily unique. We choose and fix once for all a place $\boldsymbol{p}_0$ for each p. By the result of [**25**, §12], the following assertions hold for almost all p.

P1) A is without defect for $\boldsymbol{p}_0$.

P2) $\mathcal{T}=\mathcal{T}(A, \theta)$ is $\boldsymbol{p}_0$-simple.

P3) U is $\boldsymbol{p}_0$-simple.

P4) $\boldsymbol{p}_0(c(\mathcal{T}))$ is not algebraic over $\boldsymbol{Z}/p\boldsymbol{Z}$.

P5) V is $\boldsymbol{p}_0$-simple.

P6) h is everywhere defined on $\boldsymbol{p}_0(A)$.

Here and henceforth, by the terms "for almost all", we understand "for all except a finite number of ".

PROPOSITION 5.3. *If the conditions* P1, 2, 4) *are satisfied and if p is prime to $d(\Phi)$, we have $\nu_i(p\delta)=\nu_s(p\delta)=p^2$, where δ is the identity element of $\mathcal{A}(\tilde{A})$.*

PROOF. As p is prime to $d(\Phi)$, we can find two integral left $\mathfrak{o}$-ideals $\mathfrak{b}_1$ and $\mathfrak{b}_2$ such that $\mathfrak{o}=\mathfrak{b}_1+\mathfrak{b}_2$, $p\mathfrak{o}=\mathfrak{b}_1\cap\mathfrak{b}_2$, $N(\mathfrak{b}_1)=N(\mathfrak{b}_2)=p$. Take a generic point x of $\tilde{A}$ over $\tilde{k}_0$. Let K_i, for $i=1,2$, be the composite of the fields $\tilde{k}_0(\tilde{\theta}(\beta)x)$ for $\beta\in\mathfrak{b}_i$. We have obviously

$$(1)\qquad \tilde{k}_0(x)=K_1K_2\,,\quad \tilde{k}_0(x)\supset K_i\supset\tilde{k}_0(px)\,.$$

By [25, § 7.2, Proposition 10], we have $[\tilde{k}_0(x): K_i]=p^2$; and by a well-known theorem, we have $p^4\geqq\nu_i(p\delta)\geqq p^2$, so that $1\leqq\nu_s(p\delta)\leqq p^2$. On the other hand, we observe that the points of order p on $\tilde{A}$ form an $\mathfrak{o}$-module. Since there is no $\mathfrak{o}$-module of order p, we must have $\nu_s(p\delta)=1$ or p^2, so that $\nu_i(p\delta)=p^4$ or p^2. Suppose that $\nu_i(p\delta)=p^4$. Then, $\tilde{k}_0(x)$ is purely inseparable over K_i and hence $K_i\supset\tilde{k}_0(x^{p^2})$. Putting $M=K_1\cap K_2$, we see that $M\supset\tilde{k}_0(x^{p^2})$. If $M\neq\tilde{k}_0(x^{p^2})$, we must have $[K_1: M]=[K_2: M]\leqq p$, so that $[K_1K_2: K_1]\leqq p$; but this is a contradiction in view of (1); so we must have $M=\tilde{k}_0(x^{p^2})$. As $K_i\supset\tilde{k}_0(px)$, we have $M\supset\tilde{k}_0(px)$; and considering the degrees, we find $\tilde{k}_0(x^{p^2})=\tilde{k}_0(px)$. Hence there exists an isomorphism ε of $\tilde{A}^{p^2}$ onto $\tilde{A}$ such that $\varepsilon\pi=p$, where π denotes the p^2-th power homomorphism of $\tilde{A}$ onto $\tilde{A}^{p^2}$. Put $\tilde{\theta}^{p^2}(\alpha)=\tilde{\theta}(\alpha)^{p^2}$ for every $\alpha\in\mathfrak{o}$. We have then $\mathcal{T}(\tilde{A},\tilde{\theta})^{p^2}=\mathcal{T}(\tilde{A}^{p^2},\tilde{\theta}^{p^2})$. We see easily that π is a homomorphism of $\tilde{\mathcal{P}}$ onto $\tilde{\mathcal{P}}^{p^2}$. Then, by Proposition 2.4, ε is an isomorphism of $\tilde{\mathcal{P}}^{p^2}$ onto $\tilde{\mathcal{P}}$; so we have, by [AF, Proposition 1], $\mathcal{T}(\tilde{A},\tilde{\theta})=\mathcal{T}(\tilde{A},\tilde{\theta})^{p^2}$. On account of Proposition 5.2, this shows that $\boldsymbol{p}_0(c(\mathcal{T}))$ is algebraic over $\boldsymbol{Z}/p\boldsymbol{Z}$; this contradicts the condition P4). Therefore we must have $\nu_i(p\delta)=p^2$.

5.3. Let p be a prime number which does not divide $d(\Phi)$. There are exactly $p+1$ integral left $\mathfrak{o}$-ideals $\mathfrak{q}$ such that $N(\mathfrak{q})=p^2$; we denote them by $\mathfrak{q}_0,\cdots,\mathfrak{q}_p$. For these $\mathfrak{q}_i$, we define $\mathcal{P}(y_i)$, $V(y_i)$, h_{y_i} and λ_i for $0\leqq i\leqq p$ as in § 4.2; we denote $\mathcal{P}(y_i)$, $V(y_i)$, h_{y_i} simply by $\mathcal{P}_i=(A_i, C_i, \theta_i)$, V_i, h_i. Let $\mathfrak{g}_i$ denote the kernel of λ_i. As $\mathfrak{g}_i$ is contained in $\mathfrak{g}(p, A)$, there exists a homomorphism μ_i of A_i onto A such that $\mu_i\circ\lambda_i=p$; then μ_i is a homomorphism of $\mathcal{P}_i$ onto $\mathcal{P}$.

THEOREM 3. *Let p be a prime number which satisfies the conditions* P1~6) *and is prime to $d(\Phi)$. Let k be an extension of k_0 such that the $\mathcal{P}_i$ and the λ_i are defined over k; and let $\boldsymbol{p}$ be an extension of $\boldsymbol{p}_0$ in k. Then, reordering the $\mathcal{P}_i$ suitably, the following relations hold.*

$$\boldsymbol{p}(c(\mathcal{T}(y_0)))=\boldsymbol{p}(c(\mathcal{T}(y)))^p\,,$$

$$\boldsymbol{p}(c(\mathcal{T}(y_i)))=\boldsymbol{p}(c(\mathcal{T}(y)))^{1/p}\qquad (i>0)\,,$$

$$\boldsymbol{p}(h_0(\lambda_0 t))=\boldsymbol{p}(h(t))^p\,,$$

$$\boldsymbol{p}(h_i(\lambda_i t))=\boldsymbol{p}(h(pt))^{1/p}\qquad (i>0)\,,$$

for every point t of A rational over k.

We prove this theorem in this and the following sections.

PROPOSITION 5.4. *There exist an extension $\{k_1, \boldsymbol{p}_1\}$ of $\{k, \boldsymbol{p}\}$ and polarized abelian varieties $\mathcal{P}_i^* = (A_i^*, C_i^*, \theta_i^*)$ of type $\mathfrak{o}$, defined over k_1, having the following properties.*

i) *For each i, there exists an isomorphism η_i of $\mathcal{P}_i$ onto $\mathcal{P}_i^*$.*

ii) *$\eta_i =$ (a projective transformation)$+$const.*

iii) *A_i^* is without defect for $\boldsymbol{p}_1$.*

iv) *Reordering suitably,*

$$\tilde{A}_0^* = \tilde{A}^p\,, \quad \tilde{\theta}_0^* = \tilde{\theta}^p\,, \quad \tilde{A}_i^{*p} = \tilde{A}\,, \quad \tilde{\theta}_i^{*p} = \tilde{\theta} \qquad (i > 0)\,.$$

v) *Let π be the p-th power homomorphism of $\tilde{A}$ onto $\tilde{A}^p$ and π' the p-th power homomorphism of $\tilde{A}^{1/p}$ onto $\tilde{A}$; then*

$$\boldsymbol{p}_1(\eta_0 \circ \lambda_0) = \pi\,, \quad \boldsymbol{p}_1(\mu_i \circ \eta_i^{-1}) = \pi' \qquad (i > 0)\,.$$

PROOF. Without loss of generality, we may assume that the points in $\mathfrak{g}(p, A)$ are rational over k. As A_i is isogenous to A, we can find, by [**14**, Theorem 4], an abelian variety B_i and an isomorphism ξ_i of A_i onto B_i, both defined over k, such that B_i is without defect for $\boldsymbol{p}$. Put $\alpha_i = \xi_i \circ \lambda_i$, $\beta_i = \mu_i \circ \xi_i^{-1}$; we have then $\beta_i \circ \alpha_i = p$. Now the reduction modulo $\boldsymbol{p}$ defines a homomorphism of $\mathfrak{g}(p, A)$ onto $\mathfrak{g}(p, \tilde{A})$, By Proposition 5.3, the kernel $\mathfrak{g}^*$ of this homomorphism is of order p^2; and we observe that $\mathfrak{g}^*$ is an $\mathfrak{o}$-module. Hence $\mathfrak{g}^*$ must coincide with one of the $\mathfrak{g}_i$, say $\mathfrak{g}_0$. Then we have $\mathfrak{g}_0 = \{0\}$. As $\mathfrak{g}(p, A) = \mathfrak{g}_0 + \mathfrak{g}_i$ for $i > 0$, $\mathfrak{g}_i$ is of order p^2 for $i > 0$. By [**25**, § 11, Proposition 3], $\tilde{\mathfrak{g}}_i$ is the kernel of $\tilde{\alpha}_i$ for every i. It follows that $\tilde{\alpha}_0$ is purely inseparable and $\tilde{\alpha}_i$ is separable for $i > 0$. As we have $\tilde{\beta}_i \circ \tilde{\alpha}_i = p$, we see, on account of Proposition 5.3, that β_0 is separable and $\tilde{\beta}_i$ is purely inseparable for $i > 0$. Let x be a generic point of $\tilde{A}$ over $\tilde{k}$. We have then $\tilde{k}(x) \supset \tilde{k}(x^p) \supset \tilde{k}(px)$. By Proposition 5.3, $\tilde{k}(x^p)$ is the maximal separable extension of $\tilde{k}(px)$ in $\tilde{k}(x)$. We have therefore

$$\tilde{k}(x^p) = \tilde{k}(\tilde{\alpha}_0 x)\,; \tag{2}$$

a similar consideration shows, for $i > 0$,

$$\tilde{k}(x_i^p) = \tilde{k}(\tilde{\beta}_i x_i) \tag{3}$$

for a generic point x_i of $\tilde{B}_i$ over $\tilde{k}$. Putting $x_i = \tilde{\alpha}_i x$, we obtain

$$\tilde{k}((\tilde{\alpha}_i x)^p) = \tilde{k}(px)\,. \tag{4}$$

Now take a hyperplane section X of A and a hyperplane section X_i of A_i for each i, all defined over k. By our construction of $A(z)$, we see that $\lambda_i^{-1}(X_i) \equiv pX$, $\mu_i^{-1}(X) \equiv pX_i$, where $\equiv$ denotes algebraic equivalence. Put $Y_i = \xi_i(X_i)$; then we have $\alpha_i^{-1}(Y_i) \equiv pX$, $\beta_i^{-1}(X) \equiv pY_i$. By virtue of [**25**, § 11, Proposition 14], we see that

$$\tilde{\alpha}_i^{-1}(\tilde{Y}_i)\equiv p\tilde{X},\quad \tilde{\beta}_i^{-1}(\tilde{X})\equiv p\tilde{Y}_i. \tag{5}$$

Let π be the p-th power homomorphism of $\tilde{A}$ onto $\tilde{A}^p$; by (2), there exists an isomorphism ε of $\tilde{A}^p$ onto $\tilde{B}_0$ such that $\tilde{\alpha}_0=\varepsilon\pi$. We have then, $\tilde{\alpha}_0^{-1}(\varepsilon(\tilde{X}^p))=\pi^{-1}(\tilde{X}^p)=p\tilde{X}$; hence on account of (5), $\varepsilon(\tilde{X}^p)\equiv\tilde{Y}_0$. By Proposition 5.1, $\tilde{X}$ is ample; therefore, $\tilde{X}^p$ is ample, and hence $\tilde{Y}_0$ is ample. By the result of [**14**, §4], we can find a projective embedding C_0 of B_0 by Y_0, whose reduction modulo $\boldsymbol{p}$ is a projective embedding of $\tilde{B}_0$ by $\tilde{Y}_0$; as $Y_0=\xi_0(X_0)$, C_0 is a projective transform of A_0. We can take C_0 as B_0; namely, we may assume that B_0 is a projective transform of A_0, and ξ_0 differs from a projective transformation only by a translation. Define a polarized abelian variety $\mathcal{P}_0'=(B_0,\mathcal{C}_0',\theta_0')$ of type $\mathfrak{o}$ so that ξ_0 is an isomorphism of $\mathcal{P}_0$ onto $\mathcal{P}_0'$; then $\mathcal{C}_0'$ is determined by the hyperplane sections. As $\alpha_0=\xi_0\circ\lambda_0$, α_0 is a homomorphism of $\mathcal{P}$ onto $\mathcal{P}_0'$, so that $\tilde{\alpha}_0$ is a homomorphism of $\tilde{\mathcal{P}}$ onto $\tilde{\mathcal{P}}_0'$. Since π is a homomorphism of $\tilde{\mathcal{P}}$ onto $\tilde{\mathcal{P}}^p$ and $\tilde{\alpha}_0=\varepsilon\circ\pi$, we see that, by Proposition 2.4, ε is an isomorphism of $\tilde{\mathcal{P}}^p$ onto $\tilde{\mathcal{P}}_0'$. Now by Proposition 5.1 and by the proof of [AF, Proposition 1], there exists a projective transformation $\bar{\psi}$ and a point $\bar{a}$ on $\tilde{B}_0$ such that $\bar{\psi}(u)=\varepsilon(u)+\bar{a}$ for $u\in\tilde{A}^p$. We can find a projective transformation ψ, rational over k, and a point a of B_0 so that $(\psi,a)\rightarrow(\bar{\psi},\bar{a})$ ref. $\boldsymbol{p}$. Put $k_1=k(a)$ and extend this specialization to a place $\boldsymbol{p}_1$ of k_1. Put $A_0^*=\psi^{-1}(B_0)$, $\zeta_0=\psi-a$; and define a polarized abelian variety $\mathcal{P}_0^*=(A_0^*,\mathcal{C}_0^*,\theta_0^*)$ of type $\mathfrak{o}$, so that ζ_0 is an isomorphism of $\mathcal{P}_0^*$ onto $\mathcal{P}_0'$. Then A_0^* is without defect for $\boldsymbol{p}_1$ and $\tilde{A}_0^*=\bar{\psi}^{-1}(\tilde{B}_0)=\varepsilon^{-1}(\tilde{B}_0)=\tilde{A}^p$, $\tilde{\zeta}_0=\varepsilon$. Hence $(\tilde{A}_0^*,\tilde{\theta}_0^*)$ coincides with $(\tilde{A}^p,\tilde{\theta}^p)$. Moreover, putting $\eta_0=\zeta_0^{-1}\circ\xi_0$, we have $\boldsymbol{p}_1(\eta_0\circ\lambda_0)=\tilde{\zeta}_0^{-1}\circ\tilde{\alpha}_0=\varepsilon^{-1}\circ\tilde{\alpha}_0=\pi$. Thus $\mathcal{P}_0^*=(A_0^*,\mathcal{C}_0^*,\theta_0^*)$ satisfies i-v) of our proposition. Consider now B_i for $i>0$. Let π_i' be the p-th power homomorphism of $\tilde{B}_i$ onto $\tilde{B}_i^p$. Then, by (3), there exists an isomorphism ε_i of $\tilde{B}_i^p$ onto $\tilde{A}$ such that $\tilde{\beta}_i=\varepsilon_i\circ\pi_i'$. By the same argument as above, we get $\tilde{X}\equiv\varepsilon_i(\tilde{Y}_i^p)$; it follows that $\tilde{Y}_i$ is ample. Therefore, by the same reasoning as above, we may assume that B_i is a projective transform of A_i and $\xi_i=$(a projective transformation)$+$const. Define a polarized abelian variety $\mathcal{P}_i'=(B_i,\mathcal{C}_i',\theta_i')$ so that ξ_i is an isomorphism of $\mathcal{P}_i$ onto $\mathcal{P}_i'$. Then, ε_i is an isomorphism of $\tilde{\mathcal{P}}_i'^p$ onto $\tilde{\mathcal{P}}$, so that $\varepsilon_i^{1/p}$ is an isomorphism of $\tilde{\mathcal{P}}_i'$ onto $\tilde{\mathcal{P}}^{1/p}$. In the same way as above, we can find, taking a suitable extension of $\{k_1,\boldsymbol{p}_1\}$, if necessary, a polarized abelian variety $\mathcal{P}_i^*=(A_i^*,\mathcal{C}_i^*,\theta_i^*)$ and an isomorphism ζ_i of $\mathcal{P}_i'$ onto $\mathcal{P}_i^*$ such that: i) $\zeta_i=$(a projective transformation)$+$const.; ii) A_i^* is without defect for $\boldsymbol{p}_1$ and $\tilde{A}_i^*=\tilde{A}^{1/p}$, $\tilde{\zeta}_i=\varepsilon_i^{1/p}$. Putting $\eta_i=\zeta_i\circ\xi_i$, we obtain $\mathcal{P}_i^*$ and η_i having the properties i-v); our proposition is thereby proved.

Now $\mathcal{P}_i^*$ being as in the above proposition, by [AF, Proposition 1], we have

$$\mathcal{T}(y_i) = \mathcal{T}(A_i, \theta_i) = \mathcal{T}(A_i^*, \theta_i^*)\,. \tag{6}$$

By Proposition 5.2, we get

$$\boldsymbol{p}_1(\mathcal{T}(A, \theta)) = \mathcal{T}(\tilde{A}, \tilde{\theta})\,, \tag{7}$$

$$\boldsymbol{p}_1(\mathcal{T}(A_i^*, \theta_i^*)) \supset \mathcal{T}(\tilde{A}_i^*, \tilde{\theta}_i^*)\,. \tag{8}$$

By iv) of Proposition 5.4 and by (6),

$$\mathcal{T}(\tilde{A}_0^*, \tilde{\theta}_0^*) = \mathcal{T}(\tilde{A}^p, \tilde{\theta}^p) = \mathcal{T}(\tilde{A}, \tilde{\theta})^p = \boldsymbol{p}(\mathcal{T}(y))^p\,, \tag{9}$$

$$\mathcal{T}(\tilde{A}_i^*, \tilde{\theta}_i^*)^p = \mathcal{T}(\tilde{A}_i^{*p}, \tilde{\theta}_i^{*p}) = \mathcal{T}(\tilde{A}, \tilde{\theta}) = \boldsymbol{p}(\mathcal{T}(y))\,. \tag{10}$$

The relations (6), (8), (9) lead to

$$\boldsymbol{p}(\mathcal{T}(y_0)) \supset \boldsymbol{p}(\mathcal{T}(y))^p\,.$$

As y is sufficiently generic, $\mathcal{T}(y)$ and $\mathcal{T}(y_0)$ have the same dimension and the same degree. Therefore we must have

$$\boldsymbol{p}(\mathcal{T}(y_0)) = \boldsymbol{p}(\mathcal{T}(y))^p\,. \tag{11}$$

By (6), (8), (10) and a similar consideration, we obtain

$$\boldsymbol{p}(\mathcal{T}(y_i))^p = \boldsymbol{p}(\mathcal{T}(y))\,. \tag{11'}$$

The relations (11) and (11′) prove the first two equalities of Theorem 3.

5.4. Let the notations be the same as in Proposition 5.4. For the sake of simplicity, we denote k_1 and $\boldsymbol{p}_1$ again by k and $\boldsymbol{p}$. The ambient space for A is denoted by P^n. By our construction of $\mathcal{P}(y_i)$, there exists an isomorphism ρ_i of a field of definition for $\mathcal{P}$ such that $\mathcal{P}^{\rho_i} = \mathcal{P}_i$, $V^{\rho_i} = V_i$, $h^{\rho_i} = h_i$. Extend ρ_0 to an isomorphism of k and denote it by ρ; put $M = kk^\rho$. We denote by K and K_i the fields of moduli of $\mathcal{P}$ and $\mathcal{P}_i$, respectively.

Now fix a basis $\{r_\nu\}$ of $\mathfrak{o}$ over $\boldsymbol{Z}$, and consider the mapping T defined in §3.4; we use the same notation T for varieties in P^n and in $\tilde{P}^n$. Let φ be a projective transformation of P^n, generic over M, and $v_1, \cdots, v_d$ be independent generic points of A over $M(\varphi)$. Put

$$B = \varphi(A)\,, \quad z = T(\varphi, v_1, \cdots, v_d)\,.$$

Then, $M(z) \subset M(\varphi, v_1, \cdots, v_d)$; and $\mathcal{T}(A, \theta)$ is the locus of z over M, and hence over K. Let w be a generic point of B over $M(\varphi, v_1, \cdots, v_d)$. Put into B a structure of abelian variety by taking w as its origin; then, B is defined over $K(z, w)$ as abelian variety. We can find an isomorphism ξ of A onto B and a point a on B such that $\xi(x) = \varphi(x) + a$ for $x \in A$. Define a polarized abelian variety $\mathcal{P}' = (B, \theta', \mathcal{C}')$ of type $\mathfrak{o}$ so that ξ is an isomorphism of $\mathcal{P}$ onto $\mathcal{P}'$; then $\mathcal{P}'$ is defined over $K(z, w)$ (cf. [AF, Proof of Proposition 1]). Now extend ρ to an isomorphism of $k(\varphi, v_1, \cdots, v_d, w)$, which we denote again by ρ; we may assume that $(\varphi^\rho, v_1^\rho, \cdots, v_d^\rho, w^\rho)$ and $(\varphi, v_1, \cdots, v_d, w)$ are independent over M, and

$$\dim_M(\varphi^\rho, v_1^\rho, \cdots, v_d^\rho, w^\rho) = \dim_{k^\rho}(\varphi^\rho, v_1^\rho, \cdots, v_d^\rho, w^\rho).$$

Let $\mathfrak{p}$ be an extension of $\boldsymbol{p}$ in M. Let $\bar{\varphi}$ be a projective transformation of $\tilde{P}^n$, generic over $\tilde{M}$, and $\bar{v}_1, \cdots, \bar{v}_d$ be independent generic points of $\tilde{A}$ over $\tilde{M}(\bar{\varphi})$; and let $\bar{w}$ be a generic point of $\bar{\varphi}(\tilde{A})$ over $\tilde{M}(\bar{\varphi}, \bar{v}_1, \cdots, \bar{v}_d)$. Then, we obtain a specialization

$$(12) \qquad (\varphi, v_1, \cdots, v_d, w) \to (\bar{\varphi}, \bar{v}_1, \cdots, \bar{v}_d, \bar{w}) \text{ ref. } \mathfrak{p}.$$

Now consider A_i^* of Proposition 5.4. By ii) of the proposition, there exists a projective transformation ψ, defined over k, and a point b on A_0^* such that $\eta_0 = \psi + b$; we have then $A_0^* = \psi(A_0)$. Put $\chi = \varphi^\rho \circ \psi^{-1}$, $u_\nu = \eta_0(v_\nu^\rho) - b + \theta_0^*(r_\nu)b$. Then, we have $B^\rho = \chi(A_0^*)$; χ is generic over M, and $u_1, \cdots, u_d$ are independent generic on A_0^* over $M(\chi)$. Furthermore, we see easily

$$M(\varphi^\rho, v_1^\rho, \cdots, v_d^\rho) = M(\chi, u_1, \cdots, u_d);$$

by the definition of T and by our choice of u_ν, we obtain

$$(13) \qquad T(\chi, u_1, \cdots, u_d) = T(\varphi^\rho, v_1^\rho, \cdots, v_d^\rho) = z^\rho.$$

Note that: $\bar{\varphi}^p$ is generic over $\tilde{M}$; $\bar{v}_1^p, \cdots, \bar{v}_d^p$ are independent generic on $\tilde{A}_0^* = \tilde{A}^p$ over $\tilde{M}(\bar{\varphi}^p)$; $\bar{w}^p$ is generic on $\bar{\varphi}(\tilde{A})^p$ over $\tilde{M}(\bar{\varphi}^p, \bar{v}_1^p, \cdots, \bar{v}_d^p)$. We see easily that the following specialization holds.

$$(14) \qquad (\chi, u_1, \cdots, u_d, w^\rho) \to (\bar{\varphi}^p, \bar{v}_1^p, \cdots, \bar{v}_d^p, \bar{w}^p) \text{ ref. } \mathfrak{p}.$$

As $M(\varphi, v_1, \cdots, v_d, w)$ and $M(\chi, u_1, \cdots, u_d, w^\rho)$ are linearly disjoint over M, the specialization (12) and (14) are compatible:

$$(16) \quad (\varphi, v_1, \cdots, v_d, w, \chi, u_1, \cdots, u_d, w^\rho) \to (\bar{\varphi}, \bar{v}_1, \cdots, \bar{v}_d, \bar{w}, \bar{\varphi}^p, \bar{v}_1^p, \cdots, \bar{v}_d^p, \bar{w}^p) \text{ ref. } \mathfrak{p}.$$

Extend this to a place $\mathfrak{P}$ of $M(\varphi, v_1, \cdots, v_d, w, \chi, u_1, \cdots, u_d, w^\rho)$. We can easily verify $\xi^\rho \circ \lambda_0 \circ \xi^{-1} = \chi \circ \eta_0 \circ \lambda_0 \circ \varphi^{-1} + \text{const.}$, so that by (16) and v) of Proposition 5.4,

$$(17) \quad \mathfrak{P}(\xi^\rho \circ \lambda_0 \circ \xi^{-1}) = \bar{\varphi}^p \circ \pi \circ \bar{\varphi}^{-1} = \text{the } p\text{-th power homomorphism of } \mathfrak{P}(B).$$

Put $\mathfrak{P}(z) = \bar{z}$. We have then

$$(18) \qquad T(\bar{\varphi}, \bar{v}_1, \cdots, \bar{v}_d) = \bar{z}.$$

By the definition of T, we have $\bar{z} = c(\mathfrak{P}(B)) \times \cdots$, so that $\mathfrak{P}(B)$ is defined over $\tilde{\boldsymbol{Q}}(\bar{z})$ if we leave the structure of abelian variety out of consideration. Now by (13), (16), (18),

$$\mathfrak{P}(z^\rho) = \mathfrak{P}(T(\chi, u_1, \cdots, u_d)) = T(\bar{\varphi}^p, \bar{v}_1^p, \cdots, \bar{v}_d^p) = \bar{z}^p.$$

Hence

$$(19) \qquad \mathfrak{P}(z, w, z^\rho, w^\rho) = (\bar{z}, \bar{w}, \bar{z}^p, \bar{w}^p).$$

Put $f = c(\mathscr{F}(A, \theta))$, $\tilde{f} = \boldsymbol{p}(f)$. We have then $f^\rho = c(\mathscr{F}(A_0, \theta_0))$, $\boldsymbol{p}(f^\rho) = \tilde{f}^p$ by (11). By our assumption P3) and P4), $\tilde{f}$ is a generic point of $\tilde{U}$ over $\tilde{\boldsymbol{Q}} = \boldsymbol{Z}/p\boldsymbol{Z}$. By

(18), $\bar{z}$ is generic on $\mathcal{T}(\tilde{A}, \tilde{\theta})$ over $\tilde{M}$, and hence over $\tilde{\boldsymbol{Q}}(\tilde{f})$; and $\bar{w}$ is generic on $\bar{\varphi}(\tilde{A}) = \mathfrak{P}(B)$ over $\tilde{M}(\bar{z})$, and hence over $\tilde{\boldsymbol{Q}}(\tilde{f}, \tilde{z})$. Therefore, by Lemma R, the specialization

$$(f, z, w) \to (\tilde{f}, \bar{z}, \bar{w}) \text{ ref. } p$$

determines a place $\mathfrak{P}_1$ of $K(z, w)$. We see then easily that the specialization

$$(f^{\rho}, z^{\rho}, w^{\rho}) \to (\tilde{f}^{p}, \bar{z}^{p}, \bar{w}^{p}) \text{ ref. } p$$

determines a place $\mathfrak{P}_2$ of $K^{\rho}(z^{\rho}, w^{\rho})$, satisfying $\mathfrak{P}_2(a^{\rho}) = \mathfrak{P}_1(a)^p$ for *every* $a \in K(z, w)$. Now, by (19), $\mathfrak{P} = \mathfrak{P}_1$ on $K(z, w)$ and $\mathfrak{P} = \mathfrak{P}_2$ on $K^{\rho}(z^{\rho}, w^{\rho})$; hence, we have, for *every* $a \in K(z, w)$,

$$\mathfrak{P}(a^{\rho}) = \mathfrak{P}(a)^p . \tag{20}$$

Since V is defined over K, we have, by (20),

$$\mathfrak{P}(V_0) = \mathfrak{P}(V^{\rho}) = \mathfrak{P}(V)^p .$$

Put $g = h \circ \xi^{-1}$. By Proposition 2.2, (V, g) is a normalized Kummer variety of $\mathcal{P}'$; and by the property (K2) of normalized Kummer variety, g is defined over $K(z, w)$ since $\mathcal{P}'$ is defined over $K(z, w)$. By the assumption P6), g is everywhere defined on $\mathfrak{P}(B)$; and by (20), we have

$$\mathfrak{P}(g^{\rho}) = \mathfrak{P}(g)^p . \tag{21}$$

Therefore, if t is a point on A, rational over k, we have, by (17) and (21),

$$\boldsymbol{p}(h_0(\lambda_0 t)) = \mathfrak{P}(h^{\rho}(\lambda_0 t)) = \mathfrak{P}(g^{\rho}(\xi^{\rho}\lambda_0\xi^{-1}\xi t)) = \tilde{g}^p((\tilde{\xi}\tilde{t})^p) = \tilde{g}(\tilde{\xi}\tilde{t})^p = \boldsymbol{p}(h(t))^p .$$

This proves the third equality of Theorem 3. Consider now $\mathcal{P}_i$ for $i > 0$. Fix an $i > 0$ and put $\sigma = \rho_i$. By the same argument as above, we extend σ to $L = k(\varphi, v_1, \cdots, v_d, w)$ suitably and find an extension $\mathfrak{Q}$ of $\boldsymbol{p}$ in LL^{σ} such that: i) B and B^{σ} are without defect for $\mathfrak{Q}$; ii) $\mathfrak{Q}(\xi \circ \mu_i \circ (\xi^{\sigma})^{-1}) =$ the p-th power homomorphism of $\mathfrak{Q}(B^{\sigma})$; iii) $\mathfrak{Q}(g^{\sigma}) = \mathfrak{Q}(g)^{1/p}$. Then, for every point t on A, rational over k, putting $s = \xi^{\sigma}\lambda_i t$, we obtain

$$h(pt) = h(\mu_i\lambda_i t) = g(\xi\mu_i(\xi^{\sigma})^{-1}s) ,$$

so that

$$\boldsymbol{p}(h(pt)) = \mathfrak{Q}(g(\xi\mu_i(\xi^{\sigma})^{-1}s)) = \mathfrak{Q}(g^{\sigma}(s))^p = \mathfrak{Q}(h^{\sigma}((\xi^{\sigma})^{-1}s))^p = \boldsymbol{p}(h_i(\lambda_i t))^p .$$

This proves the fourth equality of Theorem 3 and completes the proof.

5.5. Congruence-relations. Fix an integral two-sided $\mathfrak{o}$-ideal $\mathfrak{a}$. We take a field k_0 of § 5.2 so that the points in $\mathfrak{g}(\mathfrak{a}, A)$ are rational over k_0. Put

$$b = c(\mathcal{T}(y)) \times h(t_1) \times \cdots \times h(t_m) ,$$

where $t_1, \cdots, t_m$ are the points in $\mathfrak{g}(\mathfrak{a}, A)$. Let F be the algebraic closure of $\boldsymbol{Q}$ in $K_{\mathfrak{a},y}$; and let $\mathfrak{B}$ be the locus of b over F. Then, for almost all p, the following assertions hold.

P7) $\mathfrak{B}$ is $\boldsymbol{p}_0$-simple.

P8) $\boldsymbol{p}_0(b)$ is generic on $\boldsymbol{p}_0(\mathfrak{B})$ over $\boldsymbol{p}_0(F)$.

Now let σ_i, for $0\leqq i\leqq p$, be the isomorphisms of $K_{\mathfrak{a},y}$ onto $K_{\mathfrak{a},y_i}$, determined by Proposition 4.4 for the ideals $\mathfrak{q}_i$ of § 5.3. Let τ_p be the automorphism of $K_{\mathfrak{a},y}$ over $K_{1,y}$ corresponding to the element p of $G_{\mathfrak{a}}$. By Theorem 3, if p satisfies P1$\sim$6) and is prime to $d(\Phi)\mathfrak{a}$, we have

$$(22)\qquad \boldsymbol{p}(b^{\sigma_0})=\boldsymbol{p}(b)^p\,,\quad \boldsymbol{p}(b^{\sigma_i})=\boldsymbol{p}(b^{\tau_p})^{1/p}\qquad (i>0)\,.$$

Let p_1 be the restriction of $\boldsymbol{p}$ on F. If p satisfies P7, 8), then, by Lemma R, the specialization

$$b\rightarrow\boldsymbol{p}(b)\ \text{ref. } p_1$$

determines a place of $F(b)=K_{\mathfrak{a},y}$; and the specializations

$$b^{\sigma_0}\rightarrow\boldsymbol{p}(b)^p\,,\quad b^{\sigma_i}\rightarrow\boldsymbol{p}(b^{\tau_p})^{1/p}\ \text{ref. } p_1$$

determine respectively places on $K_{\mathfrak{a},y_0}$ and on $K_{\mathfrak{a},y_i}$. These places are of course restrictions of the place $\boldsymbol{p}$. Therefore, we observe that, if p satisfies P1$\sim$8) and is prime to $d(\Phi)\mathfrak{a}$,

$$(23)\qquad \boldsymbol{p}(a^{\sigma_0})=\boldsymbol{p}(a)^p\,,\quad \boldsymbol{p}(a^{\sigma_i})=\boldsymbol{p}(a^{\tau_p})^{1/p}\qquad (i>0)$$

hold for *every* $a\in K_{\mathfrak{a},y}$.

Let L be a subfield of $K_{\mathfrak{a}}$ satisfying (29) of § 4.3 and $\{\mathfrak{C},u\}$ a model of L. For almost all p, the following assertions hold.

P9) $\mathfrak{C}$ is p-simple and $p(\mathfrak{C})$ has no multiple point.

P10) $\boldsymbol{p}_0(u)$ is a generic point of $p(\mathfrak{C})$ over $\boldsymbol{Z}/p\boldsymbol{Z}$.

Let p be a prime number which satisfies P1$\sim$10) and is prime to $d(\Phi)\mathfrak{a}$. Let $\mathfrak{q}$ be an integral left $\mathfrak{o}$-ideal such that $N(\mathfrak{q})=p$ and $X_{\mathfrak{q}}$ the modular correspondence on $\mathfrak{C}$ associated with $\mathfrak{q}$ (cf. § 4.3). Now we want to consider the reduction of $X_{\mathfrak{q}}$ modulo p. As $\mathfrak{C}$ is defined over $\boldsymbol{Q}$, $\tilde{\mathfrak{C}}$ is defined over $\boldsymbol{Z}/p\boldsymbol{Z}$. Let Π and Π' be respectively the loci of $\tilde{u}\times\tilde{u}^p$ and of $\tilde{u}^p\times\tilde{u}$ on $\tilde{\mathfrak{C}}\times\tilde{\mathfrak{C}}$ over $\boldsymbol{Z}/p\boldsymbol{Z}$. The relation (23) shows

$$\boldsymbol{p}(u^{\sigma_0})=\boldsymbol{p}(u)^p\,,\quad \boldsymbol{p}(u^{\sigma_i})=\boldsymbol{p}(u^{\tau_p})^{1/p}\qquad (i>0)\,,$$

so that, by (30) of §4.3 and by [**21**, Theorem 19], we have

$$\tilde{X}_{\mathfrak{q}}(\tilde{u})=\tilde{u}^p+p\tilde{Y}_p(\tilde{u})^{1/p}=\Pi(\tilde{u})+\Pi'\circ\tilde{Y}_p(\tilde{u})\,.$$

It follows that $\tilde{X}_{\mathfrak{q}}-(\Pi+\Pi'\circ\tilde{Y}_p)$ is of the form $\mathfrak{e}\times\tilde{\mathfrak{C}}$, where $\mathfrak{e}$ is a divisor on $\tilde{\mathfrak{C}}$. Since $\Pi+\Pi'\circ\tilde{Y}^p$ has no component of the form $e\times\tilde{\mathfrak{C}}$, we conclude that $\mathfrak{e}>0$. On the other hand, we have

$$d'(\tilde{X}_{\mathfrak{q}})=d'(X_{\mathfrak{q}})=p+1=d'(\Pi+\Pi'\circ Y_p)\,;$$

so we must have $\mathfrak{e}=0$. Thus we have proved:

THEOREM 4. *Notations being as above, let p be a prime number which satisfies* P1$\sim$10) *and is prime to $d(\Phi)\mathfrak{a}$. Then we have*

$$\tilde{X}_{\mathfrak{q}}=\Pi+\Pi'\circ\tilde{Y}_p$$

on the reduction $\tilde{\mathfrak{C}}$ *of the curve* $\mathfrak{C}$ *modulo* p.

Now suppose that $\mathfrak{a}$ is prime to $d(\Phi)$; let L_N be the subfield of $K_{\mathfrak{a},y}$ given in § 4.3, and $\{\mathfrak{C}_N, u\}$ a model of L_N. Notations being as in Proposition 4.8, consider the case $n=p$. We observe then $\tilde{Z}^p\circ\tilde{Y}_p=\tilde{Z}$, so that

$$\tilde{Z}'\circ\Pi'\circ\tilde{Z}=\tilde{Z}'\circ\Pi'\circ\tilde{Z}^p\circ\tilde{Y}_p=\tilde{Z}'\circ\tilde{Z}\circ\Pi'\circ\tilde{Y}_p=\Pi'\circ\tilde{Y}_p\,.$$

We obtain thus:

THEOREM 5. *Notations being as above, we have*

$$\Pi'\circ\tilde{Y}_p=\tilde{Z}'\circ\Pi'\circ\tilde{Z}$$

on $\tilde{\mathfrak{C}}_N$.

5.6. Let J_N be a jacobian variety of $\mathfrak{C}_N$, and φ a canonical mapping of $\mathfrak{C}_N$ onto J_N. As $\mathfrak{C}_N$ is defined over $\boldsymbol{Q}$, we may assume that J_N is defined over $\boldsymbol{Q}$; φ may not be defined over $\boldsymbol{Q}$; but we may assume that $\varphi^\sigma=\varphi+\text{const.}$ for any isomorphism σ over $\boldsymbol{Q}$. Every correspondence X on $\mathfrak{C}_N$ determines an endomorphism ξ of J_N by the relations

$$X(x)=\sum_\nu x_\nu\,,\quad \xi(\varphi(x))=\sum_\nu\varphi(x_\nu)+\text{const.}$$

(cf. [**29**, no. 43]). We see easily that ξ is defined over any field of definition for X. Let ξ_p, η_p, ζ be the endomorphisms of J_N determined by $X_{\mathfrak{q}}$, Y_p, Z, respectively. Now J_N is without defect for almost all p, and $\tilde{J}_N$ is a jacobian variety of $\tilde{\mathfrak{C}}_N$; more precisely, as remarked by Igusa, Chow's construction of jacobian is compatible with the specialization; so we may assume that J_N is without defect and $\tilde{J}_N$ is a jacobian variety of $\tilde{\mathfrak{C}}_N$ for every prime p satisfying P9). Let π be the p-th power endomorphism of $\tilde{J}_N$ and $\pi'=p\pi^{-1}$. Then, Theorems 4 and 5 yield the relations

$$\tilde{\xi}_p=\pi+\pi'\circ\tilde{\eta}_p\,, \tag{24}$$

$$\pi'\circ\tilde{\eta}_p=\tilde{\zeta}^{-1}\circ\pi'\circ\tilde{\zeta}\,. \tag{25}$$

§ 6. The zeta-functions of algebraic curves.

6.1. Transference to the upper half plane. Let $\mathfrak{a}=N\mathfrak{o}$ be an integral two-sided $\mathfrak{o}$-ideal which is prime to $d(\Phi)$. Γ_N being as in § 1.3, let $\mathfrak{K}_N$ denote the field of automorphic functions with respect to Γ_N. Put

$$\mathfrak{F}_N=\boldsymbol{Q}(f_i(z),\ g_j(N^{-1}\beta,z)\,|\,1\leqq i\leqq m,\ 1\leqq j\leqq M,\ \beta\in\mathfrak{o})\,,$$

where the f_i and the g_j are the functions determined by (3) of § 3.1 and (4) of § 3.2. We have seen that $\boldsymbol{C}\mathfrak{F}_N=\mathfrak{K}_N$; and if y is sufficiently generic, the mapping $f(z)\to f(y)$ gives an isomorphism of $\mathfrak{F}_N$ onto $K_{\mathfrak{a},y}$. Let $\mathfrak{L}_N$ be the subfield of $\mathfrak{F}_N$ corresponding to the subfield L_N of $K_{\mathfrak{a},y}$. We have then

$$\mathfrak{L}_N(\zeta_N)=\mathfrak{F}_N\,, \quad \boldsymbol{C}\mathfrak{L}_N=\mathfrak{K}_N\,,$$

where ζ_N is a primitive N-th root of unity. For every $f\in\mathfrak{F}_N$, define a function f_1 on $\mathfrak{C}_N$ by $f_1(u)=f(y)$. Identifying f_1 with f, $\mathfrak{L}_N$ is regarded as the field of functions on the curve $\mathfrak{C}_N$ defined over $\boldsymbol{Q}$; and then $\mathfrak{K}_N$ is identified with the field of functions on $\mathfrak{C}_N$, the universal domain being $\boldsymbol{C}$.

Let α be an element of $\mathfrak{o}$ such that $N(\alpha)>0$; suppose that α is prime to N. Let the notations be as in Propositions 4.3 and 4.4. Consider the coordinates of the points $c(\mathcal{F}(y))$ and $h_y(\theta(\beta)t)$ for $t=\Lambda(N^{-1}e(y),y)$. We see easily that

$$f_j(y)^{\sigma_\nu}=f_j(\alpha_\nu[y])\,, \quad g_j(N^{-1}\beta,y)^{\sigma_\nu}=g_j(N^{-1}\beta\alpha_\nu',\alpha_\nu[y])\,,$$

where the α_ν are representatives for $\Gamma_N\backslash\Gamma_N\alpha\Gamma_N$; namely we have

$$\Gamma_N\alpha\Gamma_N=\bigcup_{\nu=1}^{m}\Gamma_N\alpha_\nu\,.$$

As $\alpha_\nu'\equiv\alpha'$ mod. $N\mathfrak{o}$, we have $g_j(N^{-1}\beta\alpha_\nu',\alpha_\nu[y])=g_j(N^{-1}\beta\alpha',\alpha_\nu[y])$. By Theorem 2 of § 4.1, there exists an automorphism ρ of $\mathfrak{F}_N$ over $\mathfrak{F}_1$ defined by $g_j(N^{-1}\beta,z)^\rho=g_j(N^{-1}\beta\alpha',z)$. Then, for every $f\in\mathfrak{F}_N$,

$$(1) \qquad f(y)^{\sigma_\nu}=f^\rho(\alpha_\nu[y])\,.$$

Now define an isomorphism σ_ν of $\mathfrak{F}_N$ by

$$f^{\sigma_\nu}(z)=f^\rho(\alpha_\nu[z])\,.$$

Then, (1) shows, for every $f\in\mathfrak{F}_N$,

$$(2) \qquad f^{\sigma_\nu}(y)=f(y)^{\sigma_\nu}\,.$$

Now fix an isomorphism of $\mathfrak{o}/N\mathfrak{o}$ onto $\boldsymbol{M}_2(\boldsymbol{Z}/N\boldsymbol{Z})$ and define with respect to this isomorphism the set $\Delta_{\mathfrak{a}}^*$ of § 1.4 and the field L_N of § 4.3. Then, if $\alpha\in\Delta_{\mathfrak{a}}^*$, the automorphism ρ is the identity on $\mathfrak{L}_N$; hence, for every $f\in\mathfrak{L}_N$,

$$f^{\sigma_\nu}(z)=f(\alpha_\nu[z])\,.$$

If we denote by the prime the derivation with respect to z, we obtain

$$(f^{\sigma_\nu})'(z)=f'(\alpha_\nu[z])j(\alpha_\nu,z)^{-2}N(\alpha)\,.$$

New let gdf be a differential form on $\mathfrak{C}_N$ of the first kind, f and g being elements of $\mathfrak{K}_N$; $g(z)f'(z)$ is then a cusp-form of degree 2 with respect to Γ_N, namely, $f(z)g'(z)\in S_2(\Gamma_N)$. Conversely, every element of $S_2(\Gamma_N)$ is obtained in this manner. If f and g are contained in $\mathfrak{L}_N$, we have

$$(3) \qquad gf'\,|\,(\Gamma_N\alpha\Gamma_N)_2=N(\alpha)\sum_\nu g(\alpha_\nu[z])f'(\alpha_\nu[z])j(\alpha_\nu,z)^{-2}=\sum_\nu g^{\sigma_\nu}(f^{\sigma_\nu})'\,.$$

Let $\mathcal{D}_0(\mathfrak{C}_N)$ and $\mathcal{D}_0(J_N)$ denote the sets of differential forms of the first kind, of degree 1, on $\mathfrak{C}_N$ and J_N, respectively. Then, φ being a canonical mapping of $\mathfrak{C}_N$ onto J_N, $\omega\rightarrow\omega\circ\varphi$ gives an isomorphism of $\mathcal{D}_0(J_N)$ onto $\mathcal{D}_0(\mathfrak{C}_N)$. Put $\omega\circ\varphi=gdf$. Then, by (2), (3) and [**25**, § 2.9, Proposition 9], we observe that

$fg' \mid (\Gamma_N \alpha \Gamma_N)_2$ corresponds to $\omega \circ \xi \circ \varphi$, where ξ denotes the endomorphism of J_N determined by $X_{\mathfrak{q}}$ for $\mathfrak{q} = \mathfrak{o}\alpha$. Therefore, if we denote by $M^d(\xi)$ the representation of $\xi \in \mathcal{A}(J_N)$ in $\mathcal{D}_0(J_N)$, we have, for a suitable choice of bases,

$$M^d(\xi) = \mathfrak{T}_2(\Gamma_N \alpha \Gamma_N). \tag{4}$$

Let γ be an element of Γ such that $\gamma \equiv \begin{pmatrix} p^{-1} & 0 \\ 0 & p \end{pmatrix}$ mod. $\mathfrak{a}$. Let τ_p be the automorphism of $\mathfrak{F}_N$ over $\mathfrak{F}_1$ defined by

$$g_j(N^{-1}\beta, z)^{\tau_p} = g_j(N^{-1}\beta p, z).$$

By Proposition 3.2 and by the definition of L_N, we see easily

$$f^{\tau_p}(z) = f(\gamma[z])$$

for every $f \in \mathfrak{L}_N$. It follows that $\Gamma_N \gamma \Gamma_N$ corresponds to Y_p defined in § 4.3; and hence

$$M^d(\eta_p) = \mathfrak{T}_2(\Gamma_N \gamma \Gamma_N) = R_2(p\,;\mathfrak{a}), \tag{5}$$

notations being as in § 1.5.

6.2. The zeta-function of $\mathfrak{C}_N$. Let p be a prime number satisfying P9) for $\mathfrak{C} = \mathfrak{C}_N$. Denote by $\zeta(s, \mathfrak{C}_N, p)$ the zeta-function of $p(\mathfrak{C}_N)$ over $\boldsymbol{Z}/p\boldsymbol{Z}$; we have

$$\zeta(s, \mathfrak{C}_N, p) = \frac{\det[1 - M_l(\pi_p)p^{-s}]}{(1-p^{-s})(1-p^{1-s})},$$

where π_p is the p-th power endomorphism of $p(J_N)$ and M_l is an l-adic representation of $\mathcal{A}_0(\tilde{J}_N)$. Now the zeta-function of the algebraic curve $\mathfrak{C}_N$ over $\boldsymbol{Q}$ is defined by

$$\zeta(s, \mathfrak{C}_N) = \prod{}' \zeta(s, \mathfrak{C}_N, p),$$

where the product is extended over all the prime numbers p satisfying P9) for $\mathfrak{C} = \mathfrak{C}_N$. U being an indeterminate, the relations (24) and (25) of § 5.6 imply

$$1 - M_l(\tilde{\xi}_p)U + M_l(\tilde{\eta}_p)pU^2 = [1 - M_l(\pi_p)U][1 - M_l(\tilde{\zeta}^{-1}\pi_p'\tilde{\zeta})U]. \tag{6}$$

By the same argument as in [**22**, § 5], we obtain

$$\det[1 - M_l(\pi_p)p^{-s}] = \det[1 - M^d(\xi_p) + M^d(\eta_p)p^{1-2s}].$$

By (4) and (5), the right hand side is equal to

$$\det[1 - \mathfrak{T}_2(p\,;\mathfrak{a})p^{-s} + R_2(p\,;\mathfrak{a})p^{1-2s}].$$

Therefore we obtain the following result.

MAIN THEOREM. *Let Φ be an indefinite quaternion algebra over $\boldsymbol{Q}$, and $\mathfrak{o}$ a maximal order in Φ. Let N be a positive integer which is prime to the discriminant of Φ, and Γ_N be the group of units γ of $\mathfrak{o}$, with positive reduced norm, satisfying $\gamma \equiv 1$ mod. $N\mathfrak{o}$. Regarding Γ_N as a Fuchsian group on the upper half plane, we can find an algebraic curve $\mathfrak{C}_N$ defined over $\boldsymbol{Q}$, such that: the field of* *functions on $\mathfrak{C}_N$ is the field of automorphic functions with respect to Γ_N; and the zeta-function of $\mathfrak{C}_N$ over $\boldsymbol{Q}$ is written in the form*

$$\zeta(s, \mathfrak{C}_N) = f(s)\zeta(s)\zeta(s-1)D(s)^{-1},$$
$$D(s) = \det\Big[\sum_{(n,N)=1} \mathfrak{T}_2(n; N\mathfrak{o})n^{-s}\Big],$$

where $f(s)$ is a product of rational functions of p^{-s} for a finite number of primes p, $\zeta(s)$ is Riemann's zeta-function, and $\mathfrak{T}_2(n; N\mathfrak{o})$ is a representation of a certain algebraic correspondence by cusp-forms of degree 2 with respect to Γ_N, given in § 1.5.

By Theorem 1, and by Hecke's theory in the case $\Phi = \boldsymbol{M}_2(\boldsymbol{Q})$, we can conclude:

COROLLARY. *The zeta-function of $\mathfrak{C}_N$ over $\boldsymbol{Q}$ is meromorphic on the whole s-plane and satisfies a functional equation.*

Our theorem is a generalization of the previous results of [**6**, **22**], obtained in the case where $\Phi = \boldsymbol{M}_2(\boldsymbol{Q})$.

The relation (24) together with the argument of [**22**, no. 20] gives also in a general case the following result.[2]

THEOREM 6. *Notations and assumptions being as in Main Theorem, the absolute values of the characteristic roots of $\mathfrak{T}_2(p; N\mathfrak{o})$ do not exceed $2\sqrt{p}$ for almost all prime numbers p.*

In the case $\Phi = \boldsymbol{M}_2(\boldsymbol{Q})$, a more precise result is obtained by Igusa [**13**].

6.3. Concluding remarks. I) We begin with an interpretation of the congruence-relations. Let l be a prime number and $\mathfrak{g}_l$ the set of points on J_N whose orders are powers of l; and let k_l be the extension of $\boldsymbol{Q}$ generated by the coordinates of all $t \in \mathfrak{g}_l$. We denote by G_l the Galois group of k_l over $\boldsymbol{Q}$. Then, as every element of G_l induces an automorphism of $\mathfrak{g}_l$, we obtain a representation $\mathfrak{M}_l$ of G_l by matrices whose coefficients are l-adic integers. Let p be a prime number different from l and $\mathfrak{p}$ its extension in k_l; let $\sigma_\mathfrak{p}$ be a Frobenius substitution for $\mathfrak{p}/p$. Then, as is shown in [**25**, **27**], if J_N is without defect for p, then p is unramified in k_l; and we obtain, for a suitable choice of l-adic coordinates,

$$\mathfrak{M}_l(\sigma_\mathfrak{p}) = M_l(\pi_p),$$

where π_p is the p-th power endomorphism of $p(J_N)$. Hence $D(s) = \prod \det[1 - M_l(\pi_p)p^{-s}]^{-1}$ gives an analogue of Artin's L-function for the infinite extension k_l of $\boldsymbol{Q}$. By (6) of § 6.2, tr $M_l(\pi_p)^n$ is easily obtained from the trace of certain modular correspondences. Therefore, if we know the trace of $\mathfrak{T}_2(\Gamma_N \alpha \Gamma_N)$, this determines the characteristic polynomial of $\mathfrak{M}_l(\sigma_\mathfrak{p})$; and the former is obtained by the trace-formula of Eichler and Selberg. Thus the congruence-relations,

[2] In [**22**, no. 20], the relation (25) was needed. But this is not necessary; only the relation (24) proves the inequality, in view of the relation $\eta_p'\eta_p = 1$.

or the above main theorem, may be regarded as a reciprocity-law for the extensions k_l over $\boldsymbol{Q}$, which are not necessarily abelian, even may be non-solvable.

II) There are many systems of polarized abelian varieties whose moduli are given by the automorphic functions with respect to some discontinuous groups. Our method is certainly applicable to those systems. Even in the case of dimension one, we have more Fuchsian groups, defined arithmetically, than treated in the present paper. In fact, take an algebraic number field k whose conjugates are all real, and take a quaternion algebra $\mathfrak{A}$ over k which is unramified at exactly one infinite prime spot of k. The unit-groups obtained from $\mathfrak{A}$ in the same way as for Φ, yield also Fuchsian groups; and we can attach to them certain analytic systems of abelian varieties. Some new difficulties may arise in treating them; it is sure, however, that we can investigate in detail the arithmetic of the curves uniformized by the automorphic functions with respect to those groups, by using modular correspondences.

The theory of modular correspondences, with their congruence-relations, is the only tool, which we know at present, to calculate the zeta-function of algebraic curves in a certain degree of generality. This connection does not seem accidental, though one may find another approach to it. Therefore, it is important to determine the algebraic curves which are uniformized by automorphic functions "defined arithmetically". This would be a difficult problem; but a recent work of Selberg [**19**] and Weil [**33**] suggest that one may anticipate something in this direction.

III) The zeta-function of the curve $\mathfrak{C}_N$ is concerned only with the cusp-forms of degree 2. Now, in [**24**], it was shown that, for each even degree κ, we can define an abelian variety by means of the "periods" of certain integrals attached to cusp-forms of degree κ. This abelian variety admit doubtlessly an algebro-geometric interpretation; and what arithmetic does it dominate? We can expect from this not only a solution of Ramanujan's conjecture but also something more interesting; and needless to say, a similar problem in the case of automorphic forms with more than one variables is no less important.

University of Tokyo.

References

[1] W. L. Chow, Abelian varieties over function-fields, Trans. Amer. Math. Soc., **78** (1955) 253-275.

[2] M. Deuring, Algebren, Berlin, 1935.

[3] M. Deuring, Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins, I, II, III, IV, Nachr. Akad. Wiss. Göttingen, (1953), 85-94; (1955), 13-42; (1956),

37-76; (1957), 55-80.

[4] M. Eichler, Allgemeine Kongruenzklasseneinteilungen der Ideale einfacher Algebren über algebraischen Zahlkörpern und ihre L-Reihen, J. Reine Angew. Math., **179** (1938), 227-251.

[5] M. Eichler, Über die Idealklassenzahl hyperkomplexer Systeme, Math. Z., **43** (1938), 481-494.

[6] M. Eichler, Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion, Arch. Math., **5** (1954), 355-366.

[7] M. Eichler, Modular correspondences and their representations. J. Indian Math. Soc., **20** (1956), 163-206.

[8] M. Eichler, Eine Verallgemeinerung der Abelschen Integrale, Math. Z., **67** (1957), 267-298.

[9] G. Fujisaki, On the zeta-function of the simple algebra over the field of rational numbers, J. Fac. Sci. Univ. Tokyo. Sec. I, vol. VII, Part 5 (1958), 567-604.

[10] R. Godement, Les fonctions ζ des algèbres simples II, Séminaire Bourbaki (février 1959, 176), 1-20.

[11] E. Hecke, Über die Bestimmung Dirichletscher Reihen durch ihre Funktionalgleichung, Math. Ann., **112** (1936), 664-699.

[12] E. Hecke, Über Modulfunktionen und die Dirichletschen Reihen mit Eulerscher Produktentwicklung, I, II, Math. Ann., **114** (1937), 1-28, 316-351.

[13] J. Igusa, Kroneckerian model of fields of elliptic modular functions, Amer. J. Math., **81** (1959), 561-577.

[14] S. Koizumi and G. Shimura, On specializations of abelian varieties, Sci. Papers. Coll. Gen. Ed. Univ. Tokyo, **9** (1959), 187-211.

[15] T. Matsusaka, Polarized varieties, fields of moduli and generalized Kummer varieties of polarized abelian varieties, Amer. J. Math., **80** (1958), 45-82.

[16] M. Nishi, Some results on abelian varieties, Nat. Sci. Rep., Ochanomizu Univ., **9** (1958), 1-12.

[17] H. Petersson, Konstruktion der sämtilichen Lösungen einer Riemannschen Funktionalgleichung durch Dirichlet-Reihen mit Eulerscher Produktentwickelung, I, II, III, Math. Ann., **116** (1939), 401-412; **117** (1940), 39-64, 277-300.

[18] A. Selberg, Harmonic analysis and discontinuous groups in weakly symmetric Riemannian spaces with applications to Dirichlet series, J. Indian Math. Soc., **20** (1956), 47-87.

[19] A. Selberg, On discontinuous groups in higher-dimensional symmetric spaces, Contributions to Function Theory, Tata Institute of Fundamental Research, Bombay, 1960, 147-164.

[20] J.-P. Serre, Groupes algébriques et corps de classes, Hermann, Paris, 1959.

[21] G. Shimura, Reduction of algebraic varieties with respect to a discrete valuation of the basic field, Amer. J. Math., **77** (1955), 134-176.

[22] G. Shimura, Correspondances modulaires et les fonctions ζ de courbes algébriques, J. Math. Soc. Japan, **10** (1958), 1-28.

[23]=[AF] G. Shimura, On the theory of automorphic functions, Ann. Math., **70** (1959), 101-144.

[24] G. Shimura, Sur les intégrales attachées aux formes automorphes, J. Math. Soc. Japan, **11** (1959), 291-311.

[25] G. Shimura and Y. Taniyama, Complex multiplication of abelian varieties and its applications to number theory, Publ. Math. Soc. Japan, No. 6, 1961.

[26] T. Tamagawa, On ζ-functions of a division algebra, to appear in Amer. J. Math.

[27] Y. Taniyama, *L*-functions of number fields and zeta functions of abelian varieties, J. Math. Soc. Japan, **9** (1957), 330-366.

[28] A. Weil, Sur les courbes algébriques et les variétés qui s'en déduisent Hermann, Paris 1948.

[29] A. Weil, Variétés abéliennes et courbes algébriques, Hermann, Paris, 1948.

[30] A. Weil, Jacobi sums as "Grössencharaktere", Trans. Amer. Math. Soc., **73** (1952), 487-495.

[31] A. Weil, On the theory of complex multiplication, Proc. Int. Symp. Alg. Nb. Th., Tokyo-Nikko, 1955, 9-22.

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

[33] A. Weil, On discrete subgroups of Lie groups, Ann. Math. **72** (1960), 369-384,

[34] A. Weil, Adèles and algebraic groups, Lecture note, The Institute for Advanced Study, Princeton, 1961.

Added in proof. Theorem 1 of § 1 lacks the explicit form of functional equation in the case $\mathfrak{a} \neq \mathfrak{o}$; it is given only by (27), which includes terms of the form $\mathrm{Re}\,(i^k \boldsymbol{f}(z))$. It is not difficult to make it into the form containing only holomorphic functions; then a more explicit form can be obtained. Furthermore, it is better to deal rather with the representations of $\mathfrak{G}_{\mathfrak{a}}$ than with those of $\mathfrak{S}_{\mathfrak{a}}$. Thus, in this respect, the view-point of Godement [**10**] will be a more appropriate one. The author would like to give a treatment for this in a more general case on some occasion. Recently, in the case $\Phi = \boldsymbol{M}_2(\boldsymbol{Q})$, the relation between Hecke's Euler-product and Artin's *L*-function for the extension $\mathfrak{F}_N/\mathfrak{F}_1(\zeta_N)$ is investigated in the paper: Rangachari, Modulare Korrespondenzen und *L*-Reihen, J. Reine Angew. Math., **205** (1961), 119-155. A similar consideration seems also meaningful in the case of division quaternion algebras.