Shimura, G.
Osaka J. Math.
1 (1964), 1-14.

ON PURELY TRANSCENDENTAL FIELDS OF AUTOMORPHIC FUNCTIONS OF SEVERAL VARIABLES

GORO SHIMURA

(Received December 2, 1963)

The purpose of this paper is to give some examples of arithmetically defined discontinuous groups Γ operating on a complex ball

$$H^r = \left\{(z_1, \cdots, z_r) \in \boldsymbol{C}^r \,\middle|\, |z_1|^2 + \cdots + |z_r|^2 < 1\right\}$$

such that the field of all automorphic functions[1] on H^r with respect to Γ is a purely transcendental extension of $\boldsymbol{C}$ of dimension r. To get such a Γ, we consider the field $K=\boldsymbol{Q}(\zeta)$ generated by a primitive m-th root of unity ζ, and take a hermitian matrix S of size $r+1$ with entries in K such that S itself has exactly r positive and one negative characteristic roots while all the other conjugates of S over $\boldsymbol{Q}$ are definite. Let $U_0(S)$ be the group of all complex matrices X such that ${}^t\bar{X}SX=S$. Let Γ be the subgroup of $U_0(S)$ consisting of the matrices whose entries are algebraic integers in K. Since H^r is isomorphic to the quotient space of $U_0(S)$ with respect to a maximal compact subgroup, Γ operates naturally on H^r. In our examples, the automorphic functions with respect to Γ give moduli of algebraic curves $Y: y^m=p(x)$, where $p(x)$ is a polynomial in $\boldsymbol{C}[x]$. Then the following table describes our examples.

	K	r	S	H^r/Γ	Y
(1)	$\boldsymbol{Q}(1^{1/3})$	2	diag $[1, 1, -1]$	non-compact	$y^3=p_4(x)$
(2)	$\boldsymbol{Q}(1^{1/3})$	3	diag $[1, 1, 1, -1]$	non-compact	$y^3=p_6(x)$
(3)	$\boldsymbol{Q}(1^{1/4})$	2	diag $[1, 1, -1]$	non-compact	$y^4=p_2(x)p_3(x)^2$
(4)	$\boldsymbol{Q}(1^{1/5})$	1	diag $[1, (1-\sqrt{5})/2]$	compact	$y^5=p_3(x)$
(5)	$\boldsymbol{Q}(1^{1/5})$	2	diag $[1, 1, (1-\sqrt{5})/2]$	compact	$y^5=p_5(x)$
(6)	$\boldsymbol{Q}(1^{1/7})$	1	diag $\left[1, -\frac{\sin(3\pi/7)}{\sin(2\pi/7)}\right]$	compact	$y^7=p_3(x)$

1) By an automorphic function, we always mean a *meromorphic* function which is invariant under the operation of the group in question.

Here $1^{1/m}$ denotes a primitive m-th root of unity, $\mathrm{diag}[a_1,\cdots,a_s]$ the diagonal matrix with diagonal elements $a_1,\cdots,a_s$, and $p_n(x)$ a polynomial of degree n and without multiple root.

Theorem. *In these six cases, the field of all automorphic functions on H^r with respect to Γ is a purely transcendental extension of $\boldsymbol{C}$ of dimension r.*

It would be worth while mentioning the following point. There was previously no known example of a discontinuous group Γ operating on a bounded symmetric domain D of dimension >1 such that D/Γ is compact and the field of all automorphic functions on D with respect to Γ is purely transcendental over $\boldsymbol{C}$. The case (5) gives actually such a discontinuous group.

Picard [3] investigated the curve $y^3=p_4(x)$ and observed that moduli of such curves give automorphic functions on H^2. But it seems that he did not determine the whole field of automorphic functions.

To prove our theorem, we consider the canonically polarized jacobian variety J of the algebraic curve Y. It turns out that J belongs to an analytic family Σ treated in our previous paper [6]. In the above cases, if Y is a generic curve of the given type, J is a generic member of Σ. Now the moduli of Y are, roughly speaking, the same as the moduli of J. Then the main theorem of [6] shows that the moduli of Y are given by the automorphic functions with respect to a certain discontinuous group Γ. In order to determine the explicit form of Γ, we need some analysis of lattices in a vector space over K with a hermitian form, which was one of the subjects investigated in [7]. In the Appendix, we give a supplement to it.

In the present paper, we treated the moduli of Y only at *generic* points. It would be interesting to study the moduli of Y in more detail, for example, from the view-point of Igusa [2], who investigated the moduli of algebraic curves of genus two.

1. First we recall some results of [6]. Let F be a totally real algebraic number field of degree g, and K a totally imaginary quadratic extension of F. We denote by ρ the complex conjugation. Let Φ be a representation of K by complex matrices of size h. We say that a triplet $\mathcal{P}=(A, \mathcal{C}, \theta)$ is a polarized abelian variety of type $\{K, \Phi, \rho\}$ if the following conditions are satisfied.

(i) A is an abelian variety of dimension h, defined over $\boldsymbol{C}$.

(ii) θ is an isomorphism of K into $\mathrm{End}_{\boldsymbol{Q}}(A)$; and the representation of $\theta(x)$ for $x\in K$ by an analytic coordinate system of A is equivalent to Φ.

(iii) $\mathcal{C}$ is a polarization of A; and the involution of $\mathrm{End}_{\boldsymbol{Q}}(A)$ determined by $\mathcal{C}$ coincides with $\theta(x)\to\theta(x^{\rho})$ on $\theta(K)$.

Let $\sigma_1,\cdots,\sigma_g$, $\sigma_1\rho,\cdots,\sigma_g\rho$ be all the isomorphisms of K into $\boldsymbol{C}$, and let r_ν (resp. s_ν) be the multiplicity of σ_ν (resp. $\sigma_\nu\rho$) in Φ. In order to insure the existence of $\mathcal{P}$ of type $\{K, \Phi, \rho\}$, the following relation should be satisfied [6, 2.1]:

$$h = g(r_\nu+s_\nu) \qquad (1\leqq\nu\leqq g). \tag{1.1}$$

Hereafter we assume (1.1) and put $u=h/g$.

Let $\mathcal{P}=(A, \mathcal{C}, \theta)$ be of type $\{K, \Phi, \rho\}$. Take a complex torus $\boldsymbol{C}^h/D$ isomorphic to A, where D is a lattice in $\boldsymbol{C}^h$. We may choose the coordinate system of $\boldsymbol{C}^h$ so that $\theta(a)$ is represented by the matrix $\Phi(a)$ on $\boldsymbol{C}^h$ for every $a\in K$. Let K^u be the vector space of all u-dimensional row vectors with components in K. Then we find u vectors $x_1,\cdots,x_u$ in $\boldsymbol{C}^h$ such that $\boldsymbol{Q}D=\sum_{i=1}^{u}\Phi(K)x_i$. For every $a=(a_1,\cdots,a_u)$ in K^u, put $x(a)=\sum_{i=1}^{u}\Phi(a_i)x_i$. Then the mapping $a\to x(a)$ is an isomorphism of K^u onto $\boldsymbol{Q}D$. Let L be the inverse image of D by this mapping.

Let $E(x, y)$ be a Riemann form on $\boldsymbol{C}^h/D$ corresponding to a basic polar divisor in $\mathcal{C}$. Then there exists an anti-hermitian form $T(a, b)$ on K^u such that

$$E(x(a), \sqrt{-1}\,x(b)) = Tr_{K/\boldsymbol{Q}}(T(a, b)) \qquad ((a, b)\in K^u\times K^u). \tag{1.2}$$

The structure $\{K^u, T, L\}$ is uniquely determined by $\mathcal{P}$ up to isomorphism. We say that $\mathcal{P}$ is of type $\{K, \Phi, \rho; T, L\}$. We note that T can not be arbitrary; it must satisfy the following condition [6, p. 160, (25)]:

(1.3) *The hermitian matrix* $\sqrt{-1}\,T^{\sigma_\nu}$ *has the same signature as* $\begin{bmatrix}-1_{r_\nu} & 0\\ 0 & 1_{s_\nu}\end{bmatrix}$ *for every* ν, *where* 1_r *denotes the identity matrix of degree* r.

Let H_ν be the space of all complex matrices z with r_ν rows and s_ν columns such that $1-{}^t\bar{z}z$ is positive hermitian, and let

$$H = H_1\times\cdots\times H_g.$$

Then we get an analytic family $\Sigma(K, \Phi, \rho; T, L)=\{\mathcal{P}_z \mid z\in H\}$ of polarized abelian varieties $\mathcal{P}_z$ of type $\{K, \Phi, \rho; T, L\}$ parametrized by the point z on H. Every $\mathcal{P}$ of type $\{K, \Phi, \rho; T, L\}$ is isomorphic to a member of $\Sigma(K, \Phi, \rho; T, L)$.

Now we let every element of $M_u(K)$ operate on K^u on the right, and define a group $\Gamma(T, L)$ by

$$\Gamma(T, L) = \left\{X\in GL_u(K)\,\middle|\, T(aX, bX) = T(a, b),\ LX = L\right\}.$$

Then $\Gamma(T, L)$ gives a properly discontinuous group of transformations on H [6, 2.7]. In [6, Th. 3], we get meromorphic functions $f_1, \cdots, f_\kappa$ on H and an analytic subset W of H of codimension one, such that $\boldsymbol{Q}(f_1(z), \cdots, f_\kappa(z))$ is the field of moduli of $\mathcal{P}_z$ for every $z \in H - W$. As remarked in [6, p. 172], if $H/\Gamma(T, L)$ is compact, $\boldsymbol{C}(f_1, \cdots, f_\kappa)$ is the field of all automorphic functions on H with respect to $\Gamma(T, L)$. Even if $H/\Gamma(T, L)$ is not compact, the last statement is true in view of [6, Th. 4] and a recent result of Baily and Borel on the compactification of $H/\Gamma(T, L)$.

Proposition 1. *Let $\mathcal{P}$ be of type $\{K, \Phi, \rho; T, L\}$ and k_0 the field of moduli of $\mathcal{P}$. If $\dim_{\boldsymbol{Q}} k_0 = \sum_{\nu=1}^{g} r_\nu s_\nu$, then $\boldsymbol{Q}(f_1, \cdots, f_\kappa)$ is isomorphic to k_0.*

This follows from [6, Theorem 4, (iii)] and [5, Prop. 3.5 and p. 305, Remark].

2. Let m and n be positive integers. Let Y be an algebraic curve defined by $y^m = p(x)$, where $p(x)$ is a polynomial in $\boldsymbol{C}[x]$, of degree n and without multiple root. If d is the greatest common divisor of m and n, the genus h of Y is given by

$$h = \frac{1}{2}\left[(m-1)(n-1)-(d-1)\right].$$

The vector space of differential forms of the first kind on Y is spanned by the $x^a dx/y^b$ with integers a and b satisfying $0 \leqq a < n$, $0 < b < m$, $bn - am - m - d \geqq 0$.

If m divides $n+1$, take a complex number c so that $p(c) \neq 0$, and put $v = 1/(x-c)$, $n+1 = me$. Then we get $(v^e y)^m = v \cdot v^n p(v^{-1}+c)$. This shows that Y is birationally equivalent to the curve $y^m = q(x)$ with a polynomial $q(x)$ in $\boldsymbol{C}[x]$ of degree $n+1$ and without multiple root.

Hereafter we assume that m does not divide $n+1$, $h > 1$, and m is an odd prime number. Let J be the jacobian variety of Y, and φ a canonical mapping of Y into J. We fix a primitive m-th root of unity ζ. Let ζ_0 be the birational correspondence of Y with itself given by $(x, y) \to (x, \zeta y)$. Denote by $\theta(\zeta)$ the automorphism of J corresponding to ζ_0. We see that $\zeta \to \theta(\zeta)$ can be extended naturally to an isomorphim θ of $\boldsymbol{Q}(\zeta)$ into $\mathrm{End}_{\boldsymbol{Q}}(J)$. Let $\mathcal{C}$ be the canonical polarization of J, and ρ the automorphism of $\boldsymbol{Q}(\zeta)$ such that $\zeta^\rho = \zeta^{-1}$. The involution of $\mathrm{End}_{\boldsymbol{Q}}(J)$ determined by $\mathcal{C}$ gives the automorphism $\theta(a) \to \theta(a^\rho)$ on $\theta(\boldsymbol{Q}(\zeta))$. In this way we get a polarized abelian variety of type $\{\boldsymbol{Q}(\zeta), \Phi, \rho\}$ in the sense of § 1, for a certain representation Φ of degree h. In view of the explicit form of differential forms of the first kind given above, we see that, for every integer b such that $0 < b < m$, the matrix $\Phi(\zeta)$ has ζ^{-b} as

a characteristic root with multiplicity $[(bn-d)/m]$, where $[\alpha]$ denotes the largest non-negative integer $\leqq\alpha$.

3. Let Y^* be another curve defined by $y^m=p^*(x)$ for a polynomial $p^*(x)$ in $\boldsymbol{C}[x]$ of degree n and without multiple root. From Y^*, we obtain a polarized abelian variety $\mathcal{P}^*=(J^*, \mathcal{C}^*, \theta^*)$ of type $\{\boldsymbol{Q}(\zeta), \Phi, \rho\}$ in the same way as above; we note that the representation Φ is the same for fixed m and n. Let ζ_0^* be the birational correspondence of Y^* with itself given by $(x, y)\to(x, \zeta y)$.

Proposition 2. *$\mathcal{P}$ is isomorphic to $\mathcal{P}^*$ if and only if there exists a birational mapping λ of Y to Y^* such that $\lambda\zeta_0=\zeta_0^*\lambda$.*

The 'if' part is obvious. Let φ^* be a canonical mapping of Y^* to J^*. Suppose that there exists an isomorphism μ of $\mathcal{P}$ to $\mathcal{P}^*$. By Torelli's theorem, there exists a birational mapping λ of Y to Y^* such that $\varphi^*\lambda=\pm\mu\varphi+\boldsymbol{a}$, where a is a point of J^*. Since $\mu\theta(\zeta)=\theta^*(\zeta)\mu$, we see easily that $\lambda^{-1}\zeta_0^*\lambda$ and ζ_0 correspond to the same automorphism $\theta(\zeta)$ of J. By our assumption $h>1$, we must have $\lambda^{-1}\zeta_0^*\lambda=\zeta_0$. Our proposition is thereby proved.

Proposition 3. *Let k_0 be the composite of $\boldsymbol{Q}(\zeta)$ and the field of moduli of $\mathcal{P}$. Then k_0 is the subfield of $\boldsymbol{C}$ which is uniquely determined by the following properties.*

(M_1) If k is a field of definition for Y and ζ_0, then $k\supset k_0$. If furthermore σ is an isomorphism of k into $\boldsymbol{C}$, over $\boldsymbol{Q}(\zeta)$, then σ is the identity mapping on k_0 if and only if there exists a birational mapping λ of Y to Y^σ such that $\lambda\zeta_0=\zeta_0^\sigma\lambda$.

(M_2) $k_0\supset\boldsymbol{Q}(\zeta)$.

This follows immediately from Prop. 2 and the definition of the field of moduli of $\mathcal{P}$ [4, p. 110].

Proposition 4. *Let λ be a birational mapping of Y to Y^* such that $\lambda\zeta_0=\zeta_0^*\lambda$, and let $\lambda(x, y)=(u, v)$. Then u, v are rational expressions of x, y of the following form.*

(I) *If m divides n, $u=(ax+b)/(cx+d)$, $v=ey/(cx+d)^{n/m}$.*

(II) *If m does not divide n, $u=ax+b$, $v=ey$.*

Here a, b, c, d, e are complex numbers.

Let $u=\sum_{i=0}^{n-1} r_i(x)y^i$, $v=\sum_{i=0}^{n-1} s_i(x)y^i$ with $r_i(x)$ and $s_i(x)$ in $\boldsymbol{C}(x)$. Since $\lambda\zeta_0=\zeta_0^*\lambda$, we have $\sum_{i=0}^{n-1} r_i(x)\zeta^i y^i=\sum_{i=0}^{n-1} r_i(x)y^i$, $\sum_{i=0}^{n-1} s_i(x)\zeta^i y^i$

$=\zeta\sum_{i=0}^{m-1} s_i(x)y^i$, so that $u=r_0(x)$, $v=s_1(x)y$. Since λ is one-to-one, r_0 must be linear fractional: $r_0(x)=(ax+b)/(cx+d)$. Write $s_1(x)$ as $s_1(x)=s(x)/t(x)$ with polynomials $s(x)$ and $t(x)$ which are relatively prime. Then we get

$$s(x)^m(cx+d)^n p(x) = t(x)^m(cx+d)^n p^*((ax+b)/(cx+d)).$$

We see that $(cx+d)^n p^*((ax+b)/(cx+d))$ is a polynomial in x of degree n or $n-1$, without multiple root. It follows that $s(x)$ is a constant. Recall that we excluded the case $m|n+1$. Then we get easily our assertions.

Suppose that m divides n. We see easily that the transformation of (I) of Prop. 4 always gives a birational mapping of Y to another curve $v^m=p^*(u)$ with a polynomial $p^*(u)$ of degree n or $n-1$, without multiple root. If a/c is not a root of $p(x)$, $p^*(u)$ is of degree n.

If m does not divide n, it is clear that the transformation of (II) of Prop. 4 gives a birational mapping of Y to a curve of the same type.

4. Let q be a polynomial in $\boldsymbol{C}[x]$ of degree $\leqq n$, other than 0, and let $q(x)=\sum_{i=0}^{n} q_i x^i$. Let P^n be the projective space of dimension n. Denote by $[q]$ the point $(q_0,\cdots,q_n)$ in P^n. Let $\alpha=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a generic point of $GL_2(\boldsymbol{C})$ over $\boldsymbol{Q}(q_0,\cdots,q_n)$ and let q^α be the polynomial determined by

$$q^\alpha(x) = (cx+d)^n q((ax+b)/(cx+d)).$$

We denote by $W(q)$ the locus of $[q^\alpha]$ over $\boldsymbol{Q}(q_0,\cdots,q_n)$. It can be easily seen that $W(q)$ is a variety determined only by q, and independent of the choice of α. By Prop. 4 and by a standard argument, we get

Proposition 5. *Suppose that m divides n. Let Y and Y^* be as in §§ 2, 3. Then $W(p)=W(p^*)$ if and only if there exists a birational mapping λ of Y to Y^* such that $\lambda\zeta_0=\zeta_0^*\lambda$.*

From this and Prop. 3, we obtain

Proposition 6. *Suppose that m divides n. Let c be the Chow point of $W(p)$. Then $\boldsymbol{Q}(\zeta, c)$ is the field k_0 of Prop. 3.*

Let $p(x)=\sum_{i=0}^{n} p_i x^i$. If $p_0,\cdots,p_n$ are algebraically independent over $\boldsymbol{Q}$, we see easily that $\boldsymbol{Q}(c)$ is the field of all quotients of homogeneous invariants, in the classical sense, of the binary form $\sum_{i=0}^{n} p_i x^i y^{n-i}$. In particular, if $n=5$, it is known that every invariant is a polynomial of certain invariants A, B, C, R of degree 4, 8, 12, 18; and R^2 is a poly-

nomial of A, B, C [1]. Then it is clear that $\boldsymbol{Q}(c)=\boldsymbol{Q}(B/A^2, C/A^3)$. If $n=6$, by the same argument, the classical result [1] shows that $\boldsymbol{Q}(c)$ is a purely transcendental extension of $\boldsymbol{Q}$ of dimension 3 (cf. also [2]).

In the next place, suppose that m does not divide n. Choosing a suitable transformation of the type (II) of Prop. 4, we can transform Y to the curve $Y': y^m=x^n+x^{n-2}+\sum_{i=0}^{n-3} p_i x^{n-3-i}$. Suppose that the p_i are algebraically independent over $\boldsymbol{Q}$. Then, by Prop. 4, we see that $\boldsymbol{Q}(\zeta, p_0^2, p_1, p_2^2, p_3, \cdots)$ is the field k_0 of Prop. 3.

5. Let us now consider the curve $Y: y^m=p(x)$ in the special case $m=n=5$. Then $h=6$, and

$$y^{-2}dx,\ y^{-3}dx,\ xy^{-3}dx,\ y^{-4}dx,\ xy^{-4}dx,\ x^2y^{-4}dx$$

form a basis of the vector space of differential forms of the first kind. Let $(J, \mathcal{C}, \theta)$ be as in § 2. Define an isomorphism θ' of $\boldsymbol{Q}(\zeta)$ into $\mathrm{End}_{\boldsymbol{Q}}(J)$ so that $\theta'(\zeta)=\theta(\zeta^3)$. Hereafter we consider $\mathcal{P}'=(J, \mathcal{C}, \theta')$ instead of $\mathcal{P}$. $\mathcal{P}'$ is of type $\{\boldsymbol{Q}(\zeta), \Phi', \rho\}$, for a representation Φ' such that $\Phi'(\zeta)$ is the diagonal matrix with diagonal elements $\zeta, \zeta, \zeta^{-1}, \zeta^3, \zeta^3, \zeta^3$. It is easy to verify that $\mathcal{P}$ and $\mathcal{P}'$ have the same field of moduli. Let $K=\boldsymbol{Q}(\zeta)$, $\zeta=e^{2\pi i/5}$, and let σ_ν, for $\nu=1, 2$, be the automorphism of K such that $\zeta^{\sigma_\nu}=\zeta^\nu$. With the notation r_ν and s_ν of § 1, we have $r_1=2$, $s_1=1$, $r_2=0$, $s_2=3$. Define an anti-hermitian form T and a lattice L in K^3 as in § 1, for the present $\mathcal{P}'$. The family $\Sigma(K, \Phi', \rho; T, L)$ is parametrized by the point in a domain

$$H=\left\{(z, w)\in \boldsymbol{C}^2 \,\middle|\, |z|^2+|w|^2<1\right\}. \tag{5.1}$$

In view of (1.3), $\sqrt{-1}\,T^{\sigma_2}$ is positive definite. Hence $H/\Gamma(T, L)$ is compact.

Now take $p(x)=\sum_{i=0}^{5} p_i x^i$ so that the p_i are algebraically independent over $\boldsymbol{Q}$. Let k_0 be the field of moduli of $\mathcal{P}'$. By [8, 1.7], k_0 contains $K=\boldsymbol{Q}(\zeta)$. The consideration of § 4 shows that k_0 is a purely transcendental extension of $\boldsymbol{Q}(\zeta)$ of dimension 2. By Prop. 1, $\boldsymbol{Q}(f_1, \cdots, f_\kappa)$ is a purely transcendental extension of $\boldsymbol{Q}(\zeta)$ of dimension 2.

6. Our next task is to determine T and L explicitly. Let $\boldsymbol{C}^h/D$ and E be as in § 1. In our case of $\mathcal{P}'=(J, \mathcal{C}, \theta')$, it is essential that J is a jacobian variety. Since every jacobian variety is self-dual, we have

$$D=\left\{x\in \boldsymbol{C}^h \,\middle|\, E(x, D)\subset \boldsymbol{Z}\right\},$$

so that by (1.2),

(6. 1) $$L=\left\{a\in K^3 \,\middle|\, Tr_{K/\boldsymbol{Q}}(T(a,\,L))\subset \boldsymbol{Z}\right\}.$$

Put $\eta=\zeta^2-\zeta^{-2}$, $S=\eta^{-1}T$, $\mathfrak{r}=\boldsymbol{Z}[\zeta]$. We see that $\theta(\mathfrak{r})\subset \mathrm{End}(J)$, and hence L is an $\mathfrak{r}$-lattice in K^3. Since $\eta^3\mathfrak{r}$ is the different of K with respect to $\boldsymbol{Q}$, and since $\eta^4\mathfrak{r}=5\mathfrak{r}$, we have

$$L=\left\{a\in K^3 \,\middle|\, S(a,\,L)\subset 5^{-1}\mathfrak{r}\right\}.$$

From this relation we can derive the structure of S and L as follows. Let $\{e_1,\,e_2,\,e_3\}$ be a basis of K^3, and S_0 a hermitian form on K^3 represented by the diagonal matrix with diagonal elements $1, 1, (1-\sqrt{5})/2$ with respect to $\{e_i\}$. Then S_0 and S have the same signature at every infinite place of $\boldsymbol{Q}(\sqrt{5})$. Let $\mathfrak{a}=5^{-1/2}\mathfrak{r}$, $L_0=\mathfrak{a}e_1+\mathfrak{a}e_2+\mathfrak{a}e_3$. Then L_0 is an $\mathfrak{r}$-lattice in K^3, and we have

$$L_0=\left\{a\in K^3 \,\middle|\, S_0(a,\,L_0)\subset 5^{-1}\mathfrak{r}\right\}.$$

By Prop. 8 of Appendix, there exists a K-linear automorphism τ of K^3 such that $S_0(x\tau,\,y\tau)=S(x,\,y)$. Therefore we may put $S=S_0$ without loss of generality. By Prop. 6 of Appendix, L and L_0 are μ_0-maximal $\mathfrak{r}$-lattices and $\mu_0(L)=\mu_0(L_0)=5^{-1}\mathfrak{r}$. By Prop. 5 of Appendix, L and L_0 belong to the same genus with respect to $U(S_0)$. Now $\boldsymbol{Q}(\zeta)$ has the class number 1. Hence by [7, 5. 24, (i)], there exists an element α of $U(S_0)$ such that $L_0\alpha=L$. Therefore taking a suitable coordinate system, we may identify $\Gamma(T,\,L)$ with the group

$$\left\{\tau\in GL(K^3) \,\middle|\, S_0(x\tau,\,y\tau)=S_0(x,\,y),\ L_0\tau=L_0\right\}.$$

Combining this and the result of §5, we get the assertion of our main theorem in the case (5).

7. We can treat the remaining cases by the same procedure, except the case (3). Let Y be the curve defined by $y^4=p(x)q(x)^2$, where p and q are polynomials without multiple root, and $\deg(p)=2$, $\deg(q)=3$; we assume that p and q have no common root. The genus of Y is 3, and $y^{-1}dx$, $q(x)y^{-3}dx$, $xq(x)y^{-3}dx$ form a basis of differential forms of the first kind. As in §2, from this Y we get $\mathcal{P}=(J,\,\mathcal{C},\,\theta)$ of type $\{Q(i),\,\Phi,\,\rho\}$, where $\Phi(i)$ is the diagonal natrix with diagonal elements $i,\,i,\,-i$. Define T and L as in §1. Then $\Sigma(\boldsymbol{Q}(i),\,\Phi,\,\rho\,;\,T,\,L)$ is again parametrized by H of (5. 1). Let $p(x)=\sum_{\lambda=0}^{2}p_\lambda x^\lambda$, $q(x)=\sum_{\mu=0}^{3}q_\mu x^\mu$, and let k_0 be the field of moduli of $\mathcal{P}$. Suppose that the p_λ and q_μ are algebraically independent

over $\boldsymbol{Q}$. Then we see easily that $\boldsymbol{Q}(i)\subset k_0\subset\boldsymbol{Q}(i, p_\lambda, q_\mu)$, $\dim_{\boldsymbol{Q}} k_0=2$. By virtue of Castelnuovo's theorem (cf. [9]), this, together with Prop. 1, shows that the field of automorphic functions on H with respect to $\Gamma(T, L)$ is purely transcendental over $\boldsymbol{C}$.

To determine T anp L, we employ the same argument as in § 6. In this case, 2 is the only prime ramified in $\boldsymbol{Q}(i)$. Therefore, the present situation is somewhat different from § 6. But the consideration in the last part of Appendix is sufficient to determine T and L explicitly from the relation similar to (6.1). Thus we get the whole result of our theorem.

Appendix

Let F be an algebraic number field of finite degree, and K a quadratic extension of F. We denote by $\mathfrak{g}$ and $\mathfrak{r}$ the ring of integers in F and in K respectively, and by ρ the non-trivial automorphism of K over F. Let V be a vector space over K of dimension n, and $S(x, y)$ a non-degenerate hermitian form: $V\times V\to K$, with respect to ρ. For every $\mathfrak{r}$-lattice L in V, we denote by $\mu(L)$ (resp. $\mu_0(L)$) the ideal in F (resp. K) generated by the elements $S(x, x)$ (resp. $S(x, y)$) for all $x\in L$ (resp. $x\in L$, $y\in L$). L is called *maximal* (resp. *μ_0-maximal*) if there is no $\mathfrak{r}$-lattice M in V, other than L, such that $L\subset M$ and $\mu(L)=\mu(M)$ (resp. $\mu_0(L)=\mu_0(M)$). For every prime ideal $\mathfrak{p}$ of F, let $\mathfrak{g}_\mathfrak{p}$ and $F_\mathfrak{p}$ denote the completions of $\mathfrak{g}$ and F with respect to $\mathfrak{p}$. Then we put $K_\mathfrak{p}=K\otimes_F F_\mathfrak{p}$, $\mathfrak{r}_\mathfrak{p}=\mathfrak{r}\mathfrak{g}_\mathfrak{p}$, $V_\mathfrak{p}=V\otimes_F F_\mathfrak{p}$; ρ and S can be extended naturally to $K_\mathfrak{p}$ and $V_\mathfrak{p}$. We can define similarly μ, μ_0, the maximality, and the μ_0-maximality for $\mathfrak{r}_\mathfrak{p}$-lattices in $V_\mathfrak{p}$. In [7] we investigated maximal lattices. Here we supply some results on μ_0-maximal lattices which are necessary for the proof of our theorem.

Let $\mathfrak{d}$ be the different of K with respect to F. By [7, 2.11], for every $\mathfrak{r}$-lattice L in V, we have

$$\mu(L)\mathfrak{r}\subset\mu_0(L)\subset\mu(L)\mathfrak{d}^{-1}, \tag{A.1}$$

$$Tr_{K/F}(\mu_0(L))\subset\mu(L). \tag{A.2}$$

Therefore, if $\mathfrak{p}$ is unramified in K, we have $\mu_0(L)_\mathfrak{p}=\mu(L)\mathfrak{r}_\mathfrak{p}$, and hence there is no distinction between maximality and μ_0-maximality for the $\mathfrak{r}_\mathfrak{p}$-lattices in $V_\mathfrak{p}$. If V is one-dimensional, it is clear that every $\mathfrak{r}$-lattice L is maximal and μ_0-maximal, and $\mu_0(L)=\mu(L)\mathfrak{r}$.

Proposition 1. *Let L be a μ_0-maximal $\mathfrak{r}_\mathfrak{p}$-lattice in $V_\mathfrak{p}$ such that $\mu_0(L)=\mu(L)\mathfrak{d}_\mathfrak{p}^{-1}$. Then L is maximal.*

Let M be an $\mathfrak{r}_\mathfrak{p}$-lattice such that $L \subset M$ and $\mu(M) = \mu(L)$. Then $\mu_0(L) \subset \mu_0(M) \subset \mu(M)\mathfrak{d}_\mathfrak{p}^{-1} = \mu(L)\mathfrak{d}_\mathfrak{p}^{-1} = \mu_0(L)$, so that $\mu_0(L) = \mu_0(M)$. Since L is μ_0-maximal, we get $L = M$; this shows that L is maximal.

Proposition 2. *If $\mathfrak{p}$ does not divide 2, every maximal $\mathfrak{r}_\mathfrak{p}$-lattice in $V_\mathfrak{p}$ is μ_0-maximal.*

By our assumption, for every ideal $\mathfrak{a}_\mathfrak{p}$ in $K_\mathfrak{p}$, we have

$$Tr_{K_\mathfrak{p}/F_\mathfrak{p}}(\mathfrak{a}_\mathfrak{p}) = \mathfrak{a}_\mathfrak{p} \cap F_\mathfrak{p}. \tag{A. 3}$$

Hence, from (A. 1) and (A. 2), we obtain, for every $\mathfrak{r}_\mathfrak{p}$-lattice L in $V_\mathfrak{p}$,

$$Tr_{K_\mathfrak{p}/F_\mathfrak{p}}(\mu_0(L)) = \mu_0(L) \cap F_\mathfrak{p} = \mu(L). \tag{A. 4}$$

Then our assertion is obvious.

Proposition 3. *Suppose that $n = 2$, $\mathfrak{p}$ does not divide 2, and S is anisotropic in $V_\mathfrak{p}$. Then every μ_0-maximal $\mathfrak{r}_\mathfrak{p}$-lattice in $V_\mathfrak{p}$ is maximal.*

If $\mathfrak{p}$ is unramified in K, there is no problem; so we assume that $\mathfrak{p}$ is ramified in K. Let L be a μ_0-maximal $\mathfrak{r}_\mathfrak{p}$-lattice in $V_\mathfrak{p}$. Since $\mathfrak{p}$ does not divide 2, the relation (A. 1) implies that $\mu_0(L) = \mu(L)\mathfrak{r}_\mathfrak{p}$ or $\mu_0(L) = \mu(L)\mathfrak{d}_\mathfrak{p}^{-1}$. If $\mu_0(L) = \mu(L)\mathfrak{d}_\mathfrak{p}^{-1}$, L is maximal by virtue of Prop. 1. Assume that $\mu_0(L) = \mu(L)\mathfrak{r}_\mathfrak{p}$. Then there exists an element x of L such that $\mu_0(L) = (S(x, x))$. Put $L' = \{y \in L \mid S(x, y) = 0\}$. We can easily verify that $L = \mathfrak{r}_\mathfrak{p} x + L'$. Since V is two-dimensional, we have $L' = \mathfrak{r}_\mathfrak{p} y$ for some y. Since L is μ_0-maximal and $\mathfrak{p}$ is ramified in K, we must have $(S(y, y)) = \mu_0(L)$. Now put $M = \{u \in V \mid S(u, u) \in \mu(L)\}$. By [7, 4. 5], M is a maximal $\mathfrak{r}_\mathfrak{p}$-lattice in $V_\mathfrak{p}$. We have clearly $L \subset M$. Let $u = ax + by \in M$ with a, b in $K_\mathfrak{p}$. Then

$$aa^\rho S(x, x) + bb^\rho S(y, y) \in \mu(L) = (S(x, x)).$$

Put $c = S(x, x)^{-1}S(y, y)$. Then c is a unit in $\mathfrak{g}_\mathfrak{p}$, and $aa^\rho + bb^\rho c \in \mathfrak{g}_\mathfrak{p}$. Let π be a prime element of $\mathfrak{r}_\mathfrak{p}$. Assume that $u \notin L$. Then $\pi^e a$ and $\pi^e b$ are units in $\mathfrak{r}_\mathfrak{p}$ with a positive integer e, and

$$(\pi^e a)(\pi^e a)^\rho + (\pi^e b)(\pi^e b)^\rho c \equiv 0 \mod (\pi\pi^\rho)^e \mathfrak{g}_\mathfrak{p}.$$

It follows that $-c$ is the norm of an element in $K_\mathfrak{p}$. But this is a contradiction, since S is anisotropic in $V_\mathfrak{p}$. Therefore $u \in L$, and hence $M = L$. This proves our proposition.

Proposition 4. *Suppose that $\mathfrak{p}$ does not decompose in K. When $\mathfrak{p}$ divides 2, suppose further that $\mathfrak{p}$ is unramified in K. Let L be a μ_0-*

maximal $\mathfrak{r}_\mathfrak{p}$*-lattice in* $V_\mathfrak{p}$. *Put* $\mathfrak{b}=\mu_0(L)$. *Then there exists a Witt decomposition* $V_\mathfrak{p}=\sum_{i=1}^{m}(K_\mathfrak{p}x_i+K_\mathfrak{p}y_i)+W$ (cf. [7, 4.3]) *such that* $L=\sum_{i=1}^{m}(\mathfrak{r}_\mathfrak{p}x_i+\mathfrak{b}y_i)+M$, *where* M *is a maximal* $\mathfrak{r}_\mathfrak{p}$*-lattice in* W *given by* $M=\{z\in W\,|\,S(z,z)\in\mu(L)\}$. *Conversely, let* $\mathfrak{b}$ *be an ideal in* $K_\mathfrak{p}$, *and* $V_\mathfrak{p}=\sum_{i=1}^{m}(K_\mathfrak{p}x_i+K_\mathfrak{p}y_i)+W$ *be a Witt decomposition. Let*

$$M=\left\{z\in W\,\middle|\,S(z,z)\in\mathfrak{b}\cap F_\mathfrak{p}\right\},\quad L=\sum_{i=1}^{m}(\mathfrak{r}_\mathfrak{p}x_i+\mathfrak{b}y_i)+M.$$

Then L *is a* μ_0*-maximal* $\mathfrak{r}_\mathfrak{p}$*-lattice in* $V_\mathfrak{p}$.

The converse part can be proved in a straightforward way. The proof of the direct part is similar to the proof of [7, 4.7]; so here we only sketch a proof. Assume that S is isotropic in $V_\mathfrak{p}$. Then we can find an element x in $V_\mathfrak{p}$ such that $S(x,x)=0$ and $\mathfrak{r}_\mathfrak{p}=\{a\in K_\mathfrak{p}\,|\,ax\in L\}$. Put $\mathfrak{a}=S(x,L)$. We get easily $\mu_0(\mathfrak{a}^{-1}\mathfrak{b}x+L)=\mu_0(L)$, so that $\mathfrak{a}^{-1}\mathfrak{b}x+L=L$ by virtue of the μ_0-maximality of L. We have therefore $L\supset\mathfrak{a}^{-1}\mathfrak{b}x$, and hence $\mathfrak{a}^{-1}\mathfrak{b}\subset\mathfrak{r}_\mathfrak{p}$. It follows that $S(x,L)=\mathfrak{b}$. Therefore we find an element $u\in L$ such that $\mathfrak{b}=(S(x,u))$. Our assumption implies $\mu(L)=Tr_{K_\mathfrak{p}/F_\mathfrak{p}}(\mathfrak{b})=Tr_{K_\mathfrak{p}/F_\mathfrak{p}}(S(x,u)\mathfrak{r}_\mathfrak{p})$. Using this fact, we can find an element λ of $\mathfrak{r}_\mathfrak{p}$ such that $S(x+\lambda u,\,x+\lambda u)=0$. Put $y=x+\lambda u$, $L'=\{z\in L\,|\,S(x,z)=S(y,z)=0\}$. Then we have $L=\mathfrak{r}_\mathfrak{p}x+\mathfrak{b}y+L'$. Applying induction to L', we get our assertion, in view of Prop. 3.

Let $U(S)$ be the group of all K-linear automorphisms σ of V such that $S(x\sigma,y\sigma)=S(x,y)$. As in [7, 5.18] we define genera of $\mathfrak{r}$-lattices in V.

Proposition 5. *Suppose that every prime factor of* 2 *in* F *is unramified in* K. *Let* L *be a* μ_0*-maximal* $\mathfrak{r}$*-lattice in* V. *Then the genus of* L *with respect to* $U(S)$ *consists of all* μ_0*-maximal* $\mathfrak{r}$*-lattices* M *such that* $\mu_0(M)=\mu_0(L)$.

This follows directly from [7, 3.3] and Prop. 4 by the same argument as in the proof of [7, 5.25].

Proposition 6. *Suppose that every prime factor of* 2 *in* F *is unramified in* K. *Let* $\mathfrak{a}$ *be an ideal in* F, *and* L *an* $\mathfrak{r}$*-lattice in* V. *Suppose that* $L=\{x\in V\,|\,S(x,L)\subset\mathfrak{a}\mathfrak{r}\}$. *Then* L *is* μ_0*-maximal, and* $\mu_0(L)=\mathfrak{a}\mathfrak{r}$.

Our assertion is clear if $n=1$. Suppose that $n>1$. For every $\mathfrak{r}$-lattice M in V, define M^* by $M^*=\{x\in V\,|\,S(x,M)\subset\mathfrak{a}\mathfrak{r}\}$. We see that $M\subset M^*$ if and only if $\mu_0(M)\subset\mathfrak{a}\mathfrak{r}$. Since $L=L^*$, we have $\mu_0(L)\subset\mathfrak{a}\mathfrak{r}$. If $M_1\subset M_2$, then $M_1^*\supset M_2^*$. Now let $L\subset M$, $\mu_0(M)\subset\mathfrak{a}\mathfrak{r}$. Then we have $M^*\subset L^*=L\subset M\subset M^*$, so that $L=M$. This shows that L is μ_0-maximal.

By [7, 3.2] and by Prop. 4, we can easily find a μ_0-maximal $\mathfrak{r}$-lattice L' such that $L \subset L'$ and $\mu_0(L') = \mathfrak{a}\mathfrak{r}$. Then the above argument shows again $L = L'$. This proves our proposition.

Proposition 7. *Let $\mathfrak{p}$ be a prime ideal in F which remains prime in K. Suppose that there exist an ideal $\mathfrak{a}$ in $F_\mathfrak{p}$ and an $\mathfrak{r}_\mathfrak{p}$-lattice L in $V_\mathfrak{p}$ such that $L = \{x \in V_\mathfrak{p}^* \mid S(x, L) \subset \mathfrak{a}\mathfrak{r}_\mathfrak{p}\}$. Then the structure $(V_\mathfrak{p}, S)$ is uniquely determined by $\mathfrak{a}$. More precisely, if n is odd and $\mathfrak{a} = a\mathfrak{g}_\mathfrak{p}$, $d(S)$ is the class of $(-1)^{(n-1)/2}a$ modulo $N_{K_\mathfrak{p}/F_\mathfrak{p}}(K_\mathfrak{p}^*)$* (cf. [7, 2.1 and 4.2]). *If n is even, S is maximally isotropic in $V_\mathfrak{p}$, namely, $V_\mathfrak{p}$ has the trivial kernel subspace with respect to S* (cf. [7, 4.3]).

By Prop. 4, we find a Witt decomposition $V_\mathfrak{p} = \sum_{i=1}^m (K_\mathfrak{p} x_i + K_\mathfrak{p} y_i) + W$ such that $L = \sum_{i=1}^m (\mathfrak{r}_\mathfrak{p} x_i + \mathfrak{b} y_i) + M$, $M = \{u \in W \mid S(u, u) \in \mathfrak{a}\}$. By our assumption on L, we have

$$M = \left\{ u \in W \,\middle|\, S(u, M) \subset \mathfrak{a}\mathfrak{r}_\mathfrak{p} \right\}. \tag{A.5}$$

If n is odd, we have $W = K_\mathfrak{p} z$, $W = \mathfrak{r}_\mathfrak{p} z$ for some z. Hence (A.5) implies that $\mathfrak{a} = S(z, z)\mathfrak{g}_\mathfrak{p}$. Since $\mathfrak{p}$ is unramified in K, every unit in $\mathfrak{g}_\mathfrak{p}$ is the norm of an element of $K_\mathfrak{p}$. Therefore we get our assertion for odd n. Next assume that n is even and W is two-dimensional. Since $\mu_0(M) = \mu(M)\mathfrak{r}_\mathfrak{p} = \mathfrak{a}\mathfrak{r}_\mathfrak{p}$, we find, using the argument of the proof of Prop. 3, an expression $M = \mathfrak{r}_\mathfrak{p} u + \mathfrak{r}_\mathfrak{p} v$ with $S(u, v) = 0$. On account of (A.5), we see that $\mathfrak{a} = S(u, u)\mathfrak{g}_\mathfrak{p} = S(v, v)\mathfrak{g}_\mathfrak{p}$; hence $S(u, u)^{-1}S(v, v)$ is a unit in $\mathfrak{g}_\mathfrak{p}$. Therefore we find an element c in $K_\mathfrak{p}$ such that $cc^\rho = -S(u, u)^{-1}S(v, v)$. Then we get $S(cu + v, cu + v) = 0$, which is a contradiction. Hence S must be maximally isotropic in $V_\mathfrak{p}$.

Proposition 8. *Suppose that there is no or only one prime ideal in F which is ramified in K. Suppose that there exist an ideal $\mathfrak{a}$ in F and an $\mathfrak{r}$-lattice L such that $L = \{x \in V \mid S(x, L) \subset \mathfrak{a}\mathfrak{r}\}$. Then the structure (V, S) is uniquely determined, up to isomorphism, by $\mathfrak{a}$ and the signature of S at infinite prime spots of F.*

Let $\mathfrak{q}$ be a possible prime ideal in F which is ramified in K. By Prop. 7, the structure $(V_\mathfrak{p}, S)$ is uniquely determined by $\mathfrak{a}$ if $\mathfrak{p} \neq \mathfrak{q}$. If we assign a fixed signature to each infinite prime spot of F, then the structure $(V_\mathfrak{q}, S)$ is automatically determined by virtue of the product formula of norm residue symbol. This proves our proposition.

If a prime factor of 2 in F is ramified in K, we can not apply Prop. 5. However, under a suitable condition, we may treat such a case.

For example, let us consider the case where $F=\boldsymbol{Q}$, $K=\boldsymbol{Q}(i)$, $i^2=-1$, $n=3$. Let $\mathfrak{p}=(2)$, $\mathfrak{P}=(1+i)$, and let L be an $\mathfrak{r}_\mathfrak{p}$-lattice in $V_\mathfrak{p}$ such that

$$L=\left\{x \middle| S(x, L)\subset(2^{-1})\right\}. \tag{A. 6}$$

Assume that S is represented in $V_\mathfrak{p}$ by the diagonal matrix with diagonal elements 1, 1, -1. Now by [7, 4. 15], the following two cases may occur.

(I) $L=\mathfrak{r}_\mathfrak{p}x+\mathfrak{r}_\mathfrak{p}y+\mathfrak{r}_\mathfrak{p}z$, $S(x, y)=S(y, z)=S(z, x)=0$.

(II) $L=\mathfrak{r}_\mathfrak{p}x+\mathfrak{r}_\mathfrak{p}y+\mathfrak{r}_\mathfrak{p}z$, $S(x, z)=S(y, z)=0$,
$S(x, x)\in\mathfrak{P}S(x, y)$, $S(y, y)\in\mathfrak{P}S(x, y)$.

Put $S(x, x)=a$, $S(y, y)=b$, $S(z, z)=c$, $S(x, y)=d$. In the case (I), by (A. 6), we have $(a)=(b)=(c)=(2^{-1})$. Put $2a=a'$, $2b=b'$, $2c=c'$. By our assumption on S, $-a'b'c'$ must be the norm of an element of $K_\mathfrak{p}$ (cf. [7, 4. 2]). Since -1 is not a norm residue, we may assume, exchanging the order of x, y, z if necessary, that $a'=b'=c'=-1$ or $a'=b'=1$, $c'=-1$. The former case can be reduced to the latter case by the transformation $u=e^{-1}(x-(1+i)y)$, $v=e^{-1}((1-i)x+y)$, $w=z$, where e is an element of $\mathfrak{r}_\mathfrak{p}$ such that $ee^\rho=-3$.

In the case (II), by (A. 6), we have $(c)=(d)=(2^{-1})$, so that $a\in\mathfrak{g}_\mathfrak{p}$, $b\in\mathfrak{a}_\mathfrak{p}$. Hence $dd^\rho-ab$ is the norm of an elemet of $K_\mathfrak{p}$. Therefore, by [7, 4. 1], S is isotropic in $K_\mathfrak{p}x+K_\mathfrak{p}y$. It follows that c is the norm of an element of $K_\mathfrak{p}$, on account of our assumption on S. Hence we may assume $\mathfrak{r}_\mathfrak{p}z=\mathfrak{P}^{-1}w$ with $S(w, w)=1$. Put $M=\mathfrak{r}_\mathfrak{p}x+\mathfrak{r}_\mathfrak{p}y$. Then $\mu(M)\subset\mathfrak{g}_\mathfrak{p}=2\mu_0(M)\subset\mu(M)$, so that $2\mu_0(M)=\mu(M)$. Applying the argument of the proof of Prop. 6 to M, we see that M is μ_0-maximal, so that by Prop. 1, M is maximal. By [7, 4. 7], we have $M=\mathfrak{P}^{-1}u+\mathfrak{P}^{-1}v$ with $S(u, u)=S(v, v)=0$, $S(u, v)=1$. Put $r=u+w$, $s=v-w$, $t=u-v+w$. Then $S(r, r)=S(s, s)=1$, $S(t, t)=-1$, $S(r, s)=S(s, t)=S(t, r)=0$, $L=\mathfrak{P}^{-1}r+\mathfrak{P}^{-1}s+\mathfrak{P}^{-1}t$. Therefore L is reduced to the case (I).

This result, combined with Prop. 4 and a localization of Prop. 6, shows that every r-lattice L in V satisfying (A. 6) belongs to one and the same genus with respect to $U(S)$.

OSAKA UNIVERSITY AND PRINCETON UNIVERSITY

References

[1] A. Clebsch: Theorie der binären algebraischen Formen, Leipzig, 1872.
[2] J. Igusa: *Arithmetic variety of moduli for genus two*, Ann. of Math. 72 (1960), 612-649.

[3] E. Picard: *Sur des fonctions de deux variables indépendantes analogues aux fonctions modulaires*, Acta Mathematica **2** (1883), 114–135.

[4] G. Shimura: *On the theory of automorphic functions*, Ann. of Math. **70** (1959), 101–144.

[5] ————: *On the zeta-functions of the algebraic curves uniformized by certain automorphic functions*, J. Math. Soc. Japan **13** (1961), 275–331.

[6] ————: *On analytic families of polarized abelian varieties and automorphic functions*, Ann. of Math. **78** (1963), 149–192.

[7] ————: *Arithmetic of unitary groups*, Ann. of Math. **79** (1964), 369–409.

[8] ————: *On the field of definition for a field of automorphic functions*, Ann. of Math. **80** (1964), 160–189.

[9] O. Zariski: *On Castelnuovo's criterion of rationality $p_a=P_2=0$ of an algebraic surface*, Illinois J. Math. **2** (1958), 303–315.