THE JOHNS HOPKINS UNIVERSITY PRESS

Modular Forms and Projective Invariants
Author(s): Jun-ichi Igusa
Source: *American Journal of Mathematics*, Vol. 89, No. 3 (Jul., 1967), pp. 817-855
Published by: The Johns Hopkins University Press
Stable URL: https://www.jstor.org/stable/2373243
Accessed: 09-09-2018 16:35 UTC

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.

Your use of the JSTOR archive indicates your acceptance of the Terms & Conditions of Use, available at https://about.jstor.org/terms

JSTOR

The Johns Hopkins University Press is collaborating with JSTOR to digitize, preserve and extend access to *American Journal of Mathematics*

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

MODULAR FORMS AND PROJECTIVE INVARIANTS.[1]

By JUN-ICHI IGUSA.

To Weil on his 60th birthday.

We shall denote by $\mathfrak{S}_g$ the Siegel upper-half plane of degree g and by $A(\Gamma_g(l))$ the graded ring of modular forms on $\mathfrak{S}_g$ belonging to the principal congruence group $\Gamma_g(l)$ of level l. Although modular forms are transcendental functions on $\mathfrak{S}_g$, the ring $A(\Gamma_g(l))$ is "algebraic" in the sense that it is of finite type over $\boldsymbol{C}$. This is a consequence of the theory of compactifications (cf. 1, 4). Furthermore, we can make an approximation of $A(\Gamma_g(l))$ by a ring of carefully chosen theta-constants in such a way that $A(\Gamma_g(l))$ will become the integral closure of the ring of theta-constants within its field of fractions. This is our fundamental lemma in [8]. Using this fact, we shall show that *there exists a ring homomorphism*

$$\rho: A(\Gamma_g(1)) \to S,$$

in which S is the graded ring of projective invariants of a binary form of degree $2g+2$, such that ρ increases the weight or the degree by a $\frac{1}{2}g$ ratio. Actually, we have a ring homomorphism ρ from the subring of $A(\Gamma_g(1))$ consisting of polynomials in the theta-constants (whose characteristics m satisfy $2m \equiv 0 \bmod 1$) to the ring S, and we can extend ρ to $A(\Gamma_g(1))$ provided that: if $A(\Gamma_g(1))$ contains an element of an odd weight, there exists at least one monomial ψ in the theta-constants defining an element of $A(\Gamma_g(2))$ of an odd weight such that $\psi(\tau) \neq 0$ at some point τ of $\mathfrak{S}_g$ associated with a hyperelliptic curve. It is defined for every odd g and at least for $g = 2, 4$. There are homomorphisms from $A(\Gamma_g(1))$ to other graded rings which are of considerable interest. We shall, however, confine ourselves to the homomorphism ρ, which has some immediate applications to the investigation of $A(\Gamma_g(1))$. The homomorphism ρ is bijective for $g = 1$, injective for $g = 2$, and the kernel is a principal ideal generated by a cusp form of weight 18 for $g = 3$. In this way, we can obtain the structure theorem of $A(\Gamma_g(1))$ for $g = 1, 2$. In the case when $g = 2$, we shall calculate the square of the cusp form of weight 35 as a polynomial in the four basic modular forms of even weights. In the case when $g = 3$, we shall show that there are no cusp

[1] This work was partially supported by the National Science Foundation.
Received May 20, 1966.

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

forms of weights less than twelve. This enables us to answer, without using "ungeheure Rechnung," a problem of Witt [21] concerning the numbers of representations of matrices of degree three by the well-known two classes of even quadratic forms of discriminant one in dimension 16. As a consequence, the difference of their analytic class invariants for $g=4$ will give a remarkable cusp form of weight 8, and it will play a significant role in the theory of modular varieties of genus four.

1. The group of characteristics. Let l denote an *even* positive integer and $\mathfrak{P}$ an abelian group of type $(l, l, \cdots, l)$. We assume that $\mathfrak{P}$ is put into duality with itself by a multiplicative, non-degenerate, alternating bilinear form

$$\mathfrak{P} \times \mathfrak{P} \ni (u, v) \to e_l(u, v) \in \mu_l,$$

in which μ_l is the cyclic group of l-th roots of unity (in some field of characteristic not dividing l). We recall that a multiplicative bilinear form is called alternating if it takes the value 1 along the diagonal. If we denote by ${}_2\mathfrak{P}$ the kernel of the duplication $u \to 2u$ of $\mathfrak{P}$ and if we put $b(\frac{1}{2}lu, \frac{1}{2}lv) = e_l(u, \frac{1}{2}lv)$, we get a multiplicative, non-degenerate, alternating bilinear form $(r, s) \to b(r, s)$ defined on ${}_2\mathfrak{P}$, and $b(r, s)$ is symmetric and μ_2-valued. Therefore, the rank of $\mathfrak{P}$ is even, say $2g$. Also $b(r, s)$ considered as a 2-cocycle of ${}_2\mathfrak{P}$ is the coboundary of a μ_2-valued 1-cochain $c(r)$ of ${}_2\mathfrak{P}$, i.e.,

$$c(r)c(s) = b(r, s)c(r+s), \quad c(r) = \pm 1$$

for r, s in ${}_2\mathfrak{P}$. We may say that $b(r, s)$ is the multiplicative bilinear form (or bi-character) associated with the multiplicative quadratic form (or character of the second degree) $c(r)$. We shall denote by T the set of all such 1-cochains. Actually, we consider T as the set of indices for the 2^{2g} cochains and denote them as $c_\alpha(r), c_\beta(r), \cdots$. If we define $\alpha + t$ for α in T and t in ${}_2\mathfrak{P}$ by

$$c_{\alpha+t}(r) = b(t, r)c_\alpha(r),$$

the union ${}_2\mathfrak{X}$ of ${}_2\mathfrak{P}$ and T becomes a vector space over $\boldsymbol{Z}/2\boldsymbol{Z}$ of dimension $2g+1$. We embed ${}_2\mathfrak{X}$ into an abelian group $\mathfrak{X}$ containing $\mathfrak{P}$ as a subgroup of index 2 such that ${}_2\mathfrak{X}$ becomes the kernel of the duplication of $\mathfrak{X}$. This is possible in one and only one way. We call $\mathfrak{X}$ the *group of characteristics* of degree g and of level l. Also, elements of $\mathfrak{P}$ are called *period-characteristics* and elements of $\mathfrak{X} - \mathfrak{P}$ are called *theta-characteristics.*

Now, we shall introduce a μ_2-valued function defined on T. We first observe that, for r, t in ${}_2\mathfrak{P}$ and α in T, we have

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

$$(\sum_r c_\alpha(r))^2 = 2^{2g} c_\alpha(0) = 2^{2g},$$

$$\sum_\alpha c_\alpha(r) = 2^{2g} \quad (r = 0), 0 \text{ (otherwise)}.$$

Using the first identity, we put

$$\sum_r c_\alpha(r) = 2^g e(\alpha),$$

and we say that α is *even* or *odd* according as $e(\alpha) = \pm 1$. One sees immediately that the number of even characteristics is $2^{g-1}(2^g + 1)$ and the number of odd characteristics is $2^{g-1}(2^g - 1)$. We can express $c_\alpha(r)$ in terms of $e(\alpha)$. In fact, we have

$$\begin{aligned} e(\alpha)e(\beta) &= (\tfrac{1}{2})^{2g} \sum_{r,t} c_\alpha(r+t) c_\beta(t) \\ &= (\tfrac{1}{2})^{2g} \sum_{r,t} b(t, \alpha+\beta-r) c_\alpha(r) \\ &= c_\alpha(\alpha+\beta). \end{aligned}$$

After these remarks, we shall consider the orthogonal group of $\mathfrak{P}$ with respect to the bilinear form $e_l(u, v)$ and denote it simply by $O(\mathfrak{X})$. An element M of $O(\mathfrak{X})$ is, therefore, an automorphism of $\mathfrak{P}$ with the property $e_l(M \cdot u, M \cdot v) = e_l(u, v)$ for all u, v in $\mathfrak{P}$.

THEOREM 1. *Every M in $O(\mathfrak{X})$ can be extended uniquely to an automorphism of $\mathfrak{X}$ such that $e(M \cdot \alpha) = e(\alpha)$ for all α in T. In this way $\mathfrak{X}$ becomes an $O(\mathfrak{X})$-module.*

Proof. We fix an element δ of T. We shall first prove the extendability. For a given M, consider the function $\chi: {}_2\mathfrak{P} \to \mu_2$ defined by

$$\chi(r) = c_\delta(M^{-1} \cdot r) c_\delta(r).$$

Then χ is a character of ${}_2\mathfrak{P}$ in the sense $\chi(r+s) = \chi(r)\chi(s)$. Hence there exists a uniquely determined element $r(M)$ of ${}_2\mathfrak{P}$ satisfying $\chi(r) = b(r(M), r)$ for every r in ${}_2\mathfrak{P}$. Put

$$M \cdot (\delta + u) = \delta + r(M) + M \cdot u$$

for all u in $\mathfrak{P}$. Then, the so-extended M gives an automorphism of the group $\mathfrak{X}$ keeping T stable. Moreover, we have

$$e(M \cdot (\delta + r)) e(\delta + r) = c_\delta(r(M))$$

for all r in ${}_2\mathfrak{P}$. Now, if we have $c_\delta(r(M)) = -1$, we will get $e(M \cdot \alpha) = -e(\alpha)$ for all α in T. This contradicts $\sum e(\alpha) = 2^g$. Therefore, we have $e(M \cdot \alpha)$

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

$= e(\alpha)$ for all α in T. We shall next prove the uniqueness of the extension. Suppose that M^* is an extension of M and put $M^* \cdot \delta = \delta + r^*(M)$. Then the condition that $e(M^* \cdot \alpha) = e(\alpha)$ for all α in T implies

$$b(r, r^*(M))\, c_\delta(M^{-1} \cdot r)\, c_\delta(r) = 1$$

for all r in ${}_2\mathfrak{P}$, and hence $r^*(M) = r(M)$. Finally, because of the uniqueness, the process of extension is a homomorphism of $O(\mathfrak{X})$ to the group of automorphisms of $\mathfrak{X}$. Therefore $\mathfrak{X}$ becomes an $O(\mathfrak{X})$-module. This completes the proof.

Once we have this theorem, we can interpret the classical theory of characteristics [cf. 11] as a theory of the $O(\mathfrak{X})$-module $\mathfrak{X}$. Since there is no difficulty in doing this, we shall mention only the following theorem of Frobenius, which can be reduced to the Witt theorem for the metric vector space ${}_2\mathfrak{P}$ over $\boldsymbol{Z}/2\boldsymbol{Z}$:

COROLLARY. *Suppose that we have two sequences of the same number of elements in T, say $\alpha_1, \alpha_2, \cdots$ and $\beta_1, \beta_2, \cdots$. Then, there exist an element M of $O(\mathfrak{X})$ with the property $M \cdot \alpha_1 = \beta_1$, $M \cdot \alpha_2 = \beta_2, \cdots$ if and only if, under the mapping $\alpha_i \to \beta_i$, linearly independent subsequences correspond to each other and the functions*

$$e(\alpha),\ e(\alpha, \beta, \gamma) = e(\alpha) e(\beta) e(\gamma) e(\alpha + \beta + \gamma)$$

take same values at corresponding elements and triples.

We can also decompose $\mathfrak{X}$ into domains of transitivity with respect to $0(\mathfrak{X})$. We recall a terminology introduced by Frobenius. We say that three elements α, β, γ of T are *syzygous* or *azygous* according as $e(\alpha, \beta, \gamma) = \pm 1$. A sequence is called azygous, say, if all triples in the sequence are azygous. There exists an azygous sequence of $2g + 1$ linearly independent elements in T, and they form a base, called an *azygous base*, of ${}_2\mathfrak{X}$. The equivalence of azygous bases can be determined by the above corollary.

Now, let ζ denote a generator of the cyclic group μ_l. A sequence of $2g$ elements $u_1', \cdots, u_g', u_1'', \cdots, u_g''$ of $\mathfrak{P}$ is called a *canonical base* of $\mathfrak{P}$ with respect to ζ if we have

$$e_l(u_i', u_i'') = \zeta,\ e_l(u_i'', u_i') = \zeta^{-1}$$

and $e_l(\text{other pair}) = 1$ for $i = 1, 2, \cdots, g$. If we map $u_1', u_2', \cdots$ to the elements $(1/l)^t(1, 0, 0, \cdots)$, $(1/l)^t(0, 1, 0, \cdots), \cdots$ of $\boldsymbol{Q}^{2g}$, we get an isomorphism $\mathfrak{P} \cong {}_l(\boldsymbol{Q}/\boldsymbol{Z})^{2g}$. If $m, n \bmod 1$ are the elements of $(\boldsymbol{Q}/\boldsymbol{Z})^{2g}$ which correspond to u, v in $\mathfrak{P}$, we have

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

$$e_l(u, v) = \zeta^{l^2({}^t m'n'' - {}^t m''n')}.$$

We also observe that, if M is an element of $O(\mathfrak{X})$, it transforms a canonical base to a canonical base. Therefore, if we introduce $g \times g$ matrices a, b, c, d with coefficients in $\mathbf{Z}$ as

$$\begin{pmatrix} M \cdot u' \\ M \cdot u'' \end{pmatrix} = \begin{pmatrix} au' + bu'' \\ cu' + du'' \end{pmatrix},$$

in which u' and u'' are column vectors determined by the canonical base, the $2g \times 2g$ matrix composed of a, b, c, $d \bmod l$ is an element of $Sp(g, \mathbf{Z}/l\mathbf{Z})$. We shall denote this matrix also by M. In this way, we get a well-defined correspondence $O(\mathfrak{X}) \to Sp(g, \mathbf{Z}/l\mathbf{Z})$, and it is an *isomorphism* of the two groups. We note that, if $m \bmod 1$ corresponds to u, then ${}^t Mm \bmod 1$ corresponds to $M \cdot u$.

On the other hand, if we fix an element δ of T, we get a bijection $\mathfrak{X} - \mathfrak{P} \to {}_l(\boldsymbol{Q}/\mathbf{Z})^{2g}$ by $\delta + u \to u \to m \bmod 1$. We shall call $m \bmod 1$ the *coordinate vector* of $\delta + u$ with respect to δ (and with respect to the canonical base of $\mathfrak{P}$).

LEMMA 1. *A canonical base of $\mathfrak{P}$ determines a unique even characteristic δ such that, if $m \bmod 1$ is the coordinate vector of an element α of T with respect to δ, we have*

$$e(\alpha) = (-1)^{4{}^t m'm''}$$

for every α.

Proof. Let δ denote an even characteristic and $\alpha = \delta + r$ an arbitrary element of T. Since $e(\alpha) = e(\alpha)e(\delta) = c_\delta(r)$ and since $r \to (-1)^{4{}^t m'm''}$ defines an element of T, there exists a uniquely determined element $n \bmod 1$ of ${}_2(\boldsymbol{Q}/\mathbf{Z})^{2g}$ such that we have

$$e(\alpha) = (-1)^{4({}^t m'm'' + {}^t m'n'' - {}^t m''n')}.$$

Furthermore, since we have

$$\sum_\alpha e(\alpha) = \sum_m (-1)^{4{}^t m'm''} = 2^g,$$

using again the fact that $r \to (-1)^{4{}^t m'm''}$ defines an element of T, i.e.,

$$4({}^t m'm'' + {}^t m'n'' - {}^t m''n') \equiv 4({}^t(m+n)'(m+n)'' + {}^t n'n'') \bmod 2,$$

we get $2{}^t n'n'' \equiv 0 \bmod 1$. Since the correspondence $\delta \to n \bmod 1$ is a bijection from the set of even characteristics to the set of $n \bmod 1$ in ${}_2(\boldsymbol{Q}/\mathbf{Z})^{2g}$ with this

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

property, there exists one and only one even characteristic δ which is mapped to $0 \bmod 1$. This completes the proof.

We note that, if we multiply $\frac{1}{2}l$ to the elements of a canonical base of $\mathfrak{P}$, we get a canonical base of ${}_2\mathfrak{P}$. The element δ in Lemma 1 depends only on this canonical base of ${}_2\mathfrak{P}$. Another remark is that, if M is an element of $O(\mathfrak{X})$ and if $m \bmod 1$ is the coordinate vector of an element $\delta + u$ of $\mathfrak{X} - \mathfrak{P}$ with respect to δ, the coordinate vector of $M^{-1} \cdot (\delta + u)$ with respect to the same δ is given by the following familiar expression

$$\begin{pmatrix} d & -c \\ -b & a \end{pmatrix} m + \frac{1}{2}\begin{pmatrix} (c^t d)_0 \\ (a^t b)_0 \end{pmatrix} \bmod 1.$$

After these preliminaries, we shall proceed to show that every principally polarized abelian variety possesses a group of characteristics of level l, which is intrinsically associated with the polarization, provided the characteristic of the universal domain, say $\boldsymbol{K}$, does not divide l. Let J denote a principally polarized abelian variety of dimension $g \geqq 1$ with X as its polar divisor (in the sense that it is positive and $l(X) = 1$, i. e., its g-fold intersection-number equal to $g!$). We shall assume that X is symmetric in the sense that it is invariant under $-id_J$, in which id_J denotes the identity automorphism of J. As before, we shall denote by l an even positive integer with the above assumption. Then ${}_lJ$ is an abelian group of type $(l, l, \cdots, l)$ and of rank $2g$. We introduce l^{2g} functions ϕ_u on J indexed by the points u of ${}_lJ$ as

$$(\phi_u) = l \cdot (X_u - X).$$

Then we introduce the same number of functions ψ_u on J as

$$(\psi_u) = (l \cdot id_J)^{-1}(X_u - X).$$

We observe that ϕ_u can be replaced by $a_u\phi_u$ with a_u in $\boldsymbol{K}^*$, the multiplicative group of $\boldsymbol{K}$. At any rate, once ϕ_u is chosen, we can normalize the constant factor in ψ_u so that we have $\psi_u(z)^l = \phi_u(lz)$, in which z is a generic point of J over a common field of definition of J, ϕ_u and ψ_u. The definition implies that we have

$$\phi_{u+v}(z) = c(u, v) \cdot \phi_u(z)\phi_v(z - u)$$

with $c(u, v)$ in $\boldsymbol{K}^*$ for all u, v in ${}_lJ$. Moreover $(u, v) \to c(u, v)$ is a 2-cocycle of ${}_lJ$ with coefficients in $\boldsymbol{K}^*$. Also, we have

$$\psi_v(z + u) = e_l(u, v) \cdot \psi_v(z)$$

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

with $e_l(u, v)$ in μ_l for all u, v in ${}_lJ$. Furthermore $(u, v) \to e_l(u, v)$ is a multiplicative, non-degenerate bilinear form, depending only on the polarization, such that

$$e_l(u, v) = c(u, v)/c(v, u).$$

All these are in Weil [17]. We call $e_l(u, v)$ the *canonical bilinear form* on ${}_lJ$. It is clear, by what we have said, that we can take ${}_lJ$ with its canonical bilinear form as $\mathfrak{P}$ and construct a group of characteristics $\mathfrak{X}$ of degree g and of level l. We shall show that elements of $\mathfrak{X} - \mathfrak{P}$ also admit a geometric interpretation.

For a moment, we shall assume that $l = 2$. Then, the divisor (ψ_r) is symmetric for every r in ${}_2J$, and hence we have

$$\psi_r(-z) = c_X(r) \cdot \psi_r(z)$$

with $c_X(r) = \pm 1$ depending only on X and r. If r' is a point of ${}_4J$ such that $2r' = r$ and if s is a point of ${}_2J$, using the identity defining $c(r, s)$, we get

$$\psi_{r+s}(z) = \text{const.}\, \psi_r(z)\psi_s(z - r').$$

We replace z by $-z + r$ in this identity, and we get

$$b(r, s)\, c_X(r + s) = c_X(r)\, c_X(s).$$

We shall also examine the dependence of $c_X(r)$ on X. We note that symmetric polar divisors on J are of the form X_t with t in ${}_2J$. We shall show that we have

$$c_{X_t}(r) = b(t, r)\, c_X(r).$$

If t' is a point of ${}_4J$ such that $2t' = t$, the divisor of the function $z \to \psi_r(z - t')$ is given by $(2 \cdot id_J)^{-1}(X_{r+t} - X_t)$. Moreover we have

$$\begin{aligned} \psi_r(-z - t') &= c_X(r) \cdot \psi_r(z + t') \\ &= c_X(r)\, b(t, r) \cdot \psi_r(z - t'), \end{aligned}$$

whence the assertion.

Going back to the case when l is an even positive integer, we see that we can identify T with the set of all symmetric polar divisors. Furthermore, the group structure in ${}_2\mathfrak{X}$ is given by $X + t = X_t$. Therefore, we can identify $\mathfrak{X} - \mathfrak{P}$ with the set of all X_u with u in $\mathfrak{P}$.

Now, we say that a *level l structure* is given in J if a canonical base of ${}_lJ$ is chosen. Then, we can summarize our results in the following way:

THEOREM 2. *Let l denote an even positive integer not divisible by the characteristic. Then a principally polarized abelian variety J possesses an*

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

intrinsically defined group of characteristics $\mathfrak{X}$ *such that* $\mathfrak{P} = {}_lJ$ *with its canonical bilinear form and* T *the set of* 2^{2g} *symmetric polar divisors. In particular, the concept of even and odd symmetric polar divisors is intrinsic and each level* 2 *structure in* J *determines a unique even symmetric polar divisor.*

The unique symmetric polar divisor in this theorem is the even characteristic denoted by δ in Lemma 1. We call this polar divisor simply the *theta-divisor* associated with the level 2 structure. We note that the number of even divisors is $2^{g-1}(2^g+1)$ and the number of odd divisors is $2^{g-1}(2^g-1)$. We note also that, if $J \to J'$ is a specialization of principally polarized abelian varieties with level l structures, the theta-divisor of J specializes uniquely to the theta-divisor of J' over this specialization.

Finally, if a level l structure is given in J and if $m, n \bmod 1$ are the coordinates of u, v in ${}_lJ$, we get a mutiplicative bilinear form $c'(u,v)$ on ${}_lJ$ as

$$c'(u,v) = \zeta^{l^2({}^tm'n'')}.$$

Since we have

$$c'(u,v)/c'(v,u) = e_l(u,v) = c(u,v)/c(v,u),$$

the 2-cocycles $c(u,v)$ and $c'(u,v)$ are in the same cohomology class [cf. 17, pp. 157-8]. Therefore, by replacing ϕ_u by $a_u\phi_u$ with a_u in $\boldsymbol{K}^*$, we can assume that we have $c(u,v) = c'(u,v)$. When we make this normalization, we have $c(u,v)^l = 1$ for all u, v in ${}_lJ$. In the following, especially in proving Theorem 3, we shall use only this property of the normalization (in the case when $l = 2$).

Now, we consider a vector bundle L over J for the divisor class containing $(l \cdot id_J)^{-1}(\Theta)$, in which Θ is the theta-divisor for some level l structure in J. Also, we fix a section θ of L such that the divisor of zeros of θ, which we shall denote by $(\theta)_0$, is $(l \cdot id_J)^{-1}(\Theta)$. Then, for every u in ${}_lJ$, we define a section θ_u of L by $\theta_u = \psi_u \cdot \theta$. It is clear that we have $(\theta_u)_0 = (l \cdot id_J)^{-1}(\Theta_u)$. The l^{2g} sections thus introduced form a base over $\boldsymbol{K}$ of the vector space of sections of L over J. Moreover, the l^{2g} elements $\theta_u(0)$ of the stalk L_0 are the algebraic analogue of the classical theta-constants, and hence we call them *algebraic theta-constants* of degree g and of level l evaluated at J. We refer to Mumford [13] for a general theory of theta-constants.

2. Hyperelliptic case. First we consider, in general, a non-singular curve C of genus $g \geqq 1$ and we denote by (J, ϕ) its jacobian variety. Also, we shall denote by W the image in J of the $(g-1)$-fold product of C and by $\mathfrak{k}$ a canonical divisor of C. Then J is a principally polarized abelian variety

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

with W_z as a polar divisor for every z on J. Moreover, the divisor $\phi^{-1}(W_z)$ is defined if and only if

$$z + \phi(\mathfrak{k}) = \sum_{i=1}^{g} \phi(P_i)$$

has a unique solution, and we have

$$\phi^{-1}(W_z) = \sum_{i=1}^{g} P_i.$$

This is a weak form of "Theorem 20" in [17]. Also, the divisor $X = W_c$ is symmetric if and only of the point c has the property

$$2c + \phi(\mathfrak{k}) = 0.$$

On the other hand, suppose that u, v are points of ${}_pJ$. Then, we can calculate $e_l(u, v)$ as follows. We take two divisors $\mathfrak{a}$, $\mathfrak{b}$ of degree zero on C with disjoint supports and with the property $\phi(\mathfrak{a}) = u$, $\phi(\mathfrak{b}) = v$. Let f, h denote functions on C defined by $(f) = l \cdot \mathfrak{a}$, $(h) = l \cdot \mathfrak{b}$. Then we have

$$h(\mathfrak{a})/f(\mathfrak{b}) = e_l(u, v).$$

We say that C is *hyperelliptic* if there exist two points P_1, P_2 on C with the property $l(P_1 + P_2) = 2$. We shall show that, if P_1', P_2' are another points of C with the same property, then

$$\mathfrak{a} = (g-2)(P_1 + P_2) + (P_1' + P_2')$$

is a canonical divisor. At any rate, it has the same degree as $\mathfrak{k}$. Moreover, we have $l(\mathfrak{k} - \mathfrak{a}) = l(\mathfrak{a}) - (g-1) \geqq 1$, and hence $\mathfrak{a}$ and $\mathfrak{k}$ are linearly equivalent. In particular, we have

$$(g-2)(P_1 + P_2) + (P_1' + P_2') \sim (g-1)(P_1 + P_2),$$

and hence $P_1' + P_2' \sim P_1 + P_2$. Therefore, the complete linear system $|P_1 + P_2|$ consists of all $P_1' + P_2'$ with the property $l(P_1' + P_2') = 2$. We shall denote this complete linear system by $\mathfrak{g}_2$. We note that $\mathfrak{g}_2$ converts C into a two-sheeted covering of the projective line $D = \boldsymbol{K} \cup \infty$. Moreover, the (numerical) function $x: C \to D$ is unique up to an automorphism of D. From now on, we shall assume that the characteristic of $\boldsymbol{K}$ is different from 2. Then, the different of the covering consists of $2g+2$ distinct points $Q_0, Q_1, \cdots, Q_{2g+1}$, say, and we have

$$(dx) = \sum_{i=0}^{2g+1} Q_i - 2(x)_\infty.$$

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

Since (dx) is a canonical divisor, by what we have said, it is linearly equivalent to $(g-1)(x)_\infty$. Consequently, there exists a function y on C with the property

$$(y) = \sum_{i=0}^{2g+1} Q_i - (g+1)(x)_\infty.$$

The function y is unique up to a constant factor and, if we assume that $a_i = x(Q_i) \neq 0, \infty$ for $i = 0, 1, \cdots, 2g+1$, we can normalize the constant factor so that we have

$$y^2 = \prod_{i=0}^{2g+1} (x - a_i).$$

We note that the function-field of C over $\boldsymbol{K}$ is $\boldsymbol{K}(x, y)$. For the sake of simplicity, we shall normalize ϕ by $\phi(Q_0) = 0$. Then we get $\phi(\mathfrak{k}) = 0$.

LEMMA 2. *Put $s_i = \phi(Q_i)$ for $i = 1, 2, \cdots, 2g+1$. Then these $2g+1$ points of ${}_2J$ have the following properties*

$$\sum_{i=1}^{2g+1} s_i = 0, \qquad b(s_i, s_j) = -1 \quad (i \neq j).$$

Proof. Since the first part is clear, we shall prove only the second part. If i_1, i_2, i_3, i_4 are distinct indices among $0, 1, \cdots, 2g+1$, we have

$$\begin{aligned} &b(\phi(Q_{i_1}) - \phi(Q_{i_2}), \phi(Q_{i_3}) - \phi(Q_{i_4})) \\ &\quad = ((x - a_{i_3})/(x - a_{i_4}))(Q_{i_1} - Q_{i_2})/((x - a_{i_1})/(x - a_{i_2}))(Q_{i_3} - Q_{i_4}), \end{aligned}$$

and this is 1. Therefore, taking $i_2 = 0$, we get $b(s_i, s_j) = b(s_i, s_k)$ whenever i, j, k are distinct indices among $1, \cdots, 2g+1$. We shall show that any $2g$ points among $s_1, s_2, \cdots, s_{2g+1}$ form a base of ${}_2J$. Otherwise, by changing indices, we will get $s_1 + \cdots + s_p = 0$ for some p satisfying $1 \leqq p \leqq 2g$. Consequently, there exists a function f on C with the property

$$f^2 = \prod_{i=1}^{p} (x - a_i/x - a_0).$$

Since $a_0, a_1, \cdots, a_p$ are distinct, clearly f itself is not contained in $\boldsymbol{K}(x)$. Since we have $[\boldsymbol{K}(x, y) : \boldsymbol{K}(x)] = 2$, we get $\boldsymbol{K}(x, f) = \boldsymbol{K}(x, y)$. Therefore, the different of $\boldsymbol{K}(x, f)/\boldsymbol{K}(x)$ has to be of degree $2g+2$, and hence $2g+2 = p$ or $p+1$ according as p is even or odd. But this contradicts $p \leqq 2g$. Now, suppose that we have $b(s_i, s_j) = 1$ for some $i \neq j$ satisfying $1 \leqq i, j \leqq 2g+1$. By changing indices, we can assume that $j = 2g+1$. Then, by what we have shown in the beginning, we get $b(s_i, s_{2g+1}) = 1$ for

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

$i=1,2,\cdots,2g$. Since $s_1, s_2, \cdots, s_{2g}$ form a base of ${}_2J$, this implies $s_{2g+1}=0$, but this is a contradiction. The lemma is thus proved.

We note that, although we have shown in the course of the above proof that $2g$ of the points $s_1, s_2, \cdots, s_{2g+1}$ are linearly independent over $\boldsymbol{Z}/2\boldsymbol{Z}$, this fact is a consequence of Lemma 2. Actually, the lemma shows that the symmetric polar divisors W_{s_i} for $i=1,2,\cdots,2g+1$ form an *azygous base* of the group of characteristics of level 2 intrinsically attached to J. In particular, all symmetric polar divisors of J can be written as W_s with

$$s=s_{i_1}+s_{i_2}+\cdots+s_{i_k},$$

in which $1\leqq i_1<i_2<\cdots<i_k\leqq 2g+1$ and either we take $k=1,3,\cdots,2g+1$ or we can equally take $k=0,1,\cdots,g$. We shall use the second way of expressing all symmetric polar divisors.

LEMMA 3. *The polar divisor W does not contain points of ${}_2J$ of the form $s_{i_1}+\cdots+s_{i_g}$ with $1\leqq i_1<\cdots<i_g\leqq 2g+1$, but it contains all other points of ${}_2J$.*

Proof. A point of the form $s_{i_1}+\cdots+s_{i_k}$ is contained in W if and only if there exist $g-1$ points $P_1,\cdots,P_{g-1}$ on C satisfying

$$\phi(Q_{i_1}+\cdots+Q_{i_k})=\phi(P_1+\cdots+P_{g-1}).$$

The second part of the lemma follows from this fact. As for the first part, we have only to disprove the existence of $P_1,\cdots,P_{g-1}$ for $k=g$. In other words, we have only to prove

$$l(Q_{i_1}+\cdots+Q_{i_g}-Q_0)=0$$

or $l(Q_{i_1}+\cdots+Q_{i_g})=1$ for $1\leqq i_1<\cdots<i_g\leqq 2g+1$. Suppose that f is a function on C with the property $(f)+Q_{i_1}+\cdots+Q_{i_g}>0$. By changing indices, we may assume that $i_1=1,\cdots,i_g=g$. We can write f in the form

$$f=(A(x)+B(x)y)/D(x),$$

in which $A(x), B(x), D(x)$ are in $\boldsymbol{K}[x]$ without any common factor. Suppose that P is one of the $Q_0, Q_1, \cdots, Q_{2g+1}$. If we denote the multiplicities of $x-x(P)$ in $A(x), B(x), D(x)$ by a, b, d, we get

$$\mathrm{ord}_P(f)=\min(2a, 2b+1)-2d.$$

Since we have $\min(a,b,d)=0$, the only case when we have $d\geqq 1$ is the case when $P=Q_1,\cdots,Q_g$. It is possible, in this case, that we have $d=1$. Then necessarily we get $a\geqq 1$, $b=0$. On the other hand, suppose that P is

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

different from $Q_0, Q_1, \cdots, Q_{2g+1}$. Then f is finite at P and at its conjugate. In other words, both f and its conjugate are finite at P. Consequently $A(x)/D(x)$ and $B(x)y/D(x)$ are finite at P. In the case when $x(P) \neq \infty$, we also have $y(P) \neq \infty$, and $y(P) \neq 0$ by assumption. Therefore, we get $D(x(P)) \neq 0$. We have thus shown that $D(x)$ divides both $A(x)$ and $(x-a_1)\cdots(x-a_g)$. Put $A(x) = C(x)D(x)$ and consider the case when $x(P) = \infty$. The condition that $C(x)$ and $B(x)y/D(x)$ are finite at P means that $C(x) = \text{const.}$ and $\deg. B(x) + g + 1 - \deg. D(x) \leqq 0$. On the other hand, we have shown that $\deg. D(x) \leqq g$, and hence $B(x) = 0$. Therefore, we get $f = \text{const.}$, and this completes the proof.

We shall, now, incorporate the observations made in the previous section. In general, if X and Y are symmetric polar divisors not containing 0, we can replace z in $\psi_{X+Y}(-z) = c_X(X+Y)\cdot\psi_{X+Y}(z)$ by 0, and we have $\psi_{X+Y}(0) \neq 0, \infty$. Therefore, we get $c_X(X+Y) = 1$, and hence $e(X) = e(Y)$. Consequently, if we put

$$e(k) = e(W + s_{i_1} + \cdots + s_{i_k})$$

for $1 \leqq i_1 < \cdots < i_k \leqq 2g+1$, Lemma 3 shows that $e(g)$ does not depend on the sequence. Suppose that $1 < k \leqq g$ and assume that $e(k)$ does not depend on the sequence. Put

$$X = W + s_{i_1} + \cdots + s_{i_{k-2}}$$

and let i_{k+1} denote one of the $1, 2, \cdots, 2g+1$ different from $i_1, \cdots, i_k$. Then, we have

$$\begin{aligned} -1 = b(s_{i_k}, s_{i_{k-1}}) &= e(X)e(X + s_{i_{k-1}})e(X + s_{i_k})e(k) \\ &= b(s_{i_{k+1}}, s_{i_{k-1}}) = e(X)e(X + s_{i_{k-1}})e(X + s_{i_{k+1}})e(k), \end{aligned}$$

and hence $e(X + s_{i_k}) = e(X + s_{i_{k+1}})$. Using this formula, we see immediately that $e(k-1)$ does not depend on the sequence. Therefore $e(k)$ is well defined for $1 \leqq k \leqq g$ and also (trivially) for $k = 0$. The exact value of $e(k)$ will be given by the following lemma:

LEMMA 4. *We have*

$$e(k) = \begin{cases} 1 \\ -1 \end{cases} \quad \text{for} \quad \begin{matrix} k \equiv g \quad , g+1 \\ k \equiv g+2, g+3 \end{matrix} \mod 4.$$

Proof. We have observed already that $-1 = e(k-2)e(k)$ for $1 < k \leqq g$. The lemma will, therefore, be proved if we show that $e(g) = 1$, $e(g-1) = -1$. For this purpose, we take the sum of $e(X)$ for the 2^{2g} symmetric polar divisors X. Then we get

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

$$2^g = e(g)\left(\binom{2g+1}{g} - \binom{2g+1}{g-2} + \cdots\right) + e(g-1)\left(\binom{2g+1}{g-1} - \binom{2g+1}{g-3} + \cdots\right).$$

We observe that the coefficients of $e(g)$ and $e(g-1)$ in the above identity are positive integers Moreover, the former is equal to the latter plus 2^g. Therefore, the only possibility is $e(g)=1$, $e(g-1)=-1$. q. e. d.

Now, we divide the $2g+2$ points $Q_0, Q_1, \cdots, Q_{2g+1}$ into two sets, each consisting of $g+1$ points, in two different ways. We can write two such partitions as

$$((Q_{i_1}, \cdots, Q_{i_p}, Q_{i_1'}, \cdots, Q_{i_q'}),\ (Q_{j_1}, \cdots, Q_{j_p}, Q_{i_1''}, \cdots, Q_{i_q''}))$$
$$((Q_{i_1}, \cdots, Q_{i_p}, Q_{i_1''}, \cdots, Q_{i_q''}),\ (Q_{j_1}, \cdots, Q_{j_p}, Q_{i_1'}, \cdots, Q_{i_q'})),$$

in which $Q_{j_1} = Q_0$ and $p+q = g+1$. Then we necessarily have $1 \leqq p \leqq g$. For the sake of simplicity, we put

$$s' = \sum_{\alpha=1}^{q} \phi(Q_{i_\alpha'}), \qquad s'' = \sum_{\alpha=1}^{q} \phi(Q_{i_\alpha''}).$$

We take p independent generic points $M_1, \cdots, M_p$ of C over a common field of definition of C, ϕ, J and consider the function on C defined by $M_1 \to (\phi_{s'}/\phi_{s''})(\phi(M_1 + \cdots + M_p))$. Then, the divisor of this function can be determined. First of all, the divisor of the function $\phi_{s'}/\phi_{s''}$ on J is $2 \cdot (W_{s'} - W_{s''})$. Moreover, if we put

$$z = s' - \sum_{i=2}^{p} \phi(M_i),$$

then $\phi^{-1}(W_z)$ is defined and, if we denote by M_i' the conjugate of M_i, we have

$$\phi^{-1}(W_z) = \sum_{i=2}^{p} M_i' + \sum_{\alpha=1}^{q} Q_{i_\alpha'}.$$

This is a key point, and we have used the fact that $l(\sum_{\alpha=1}^{q} Q_{i_\alpha'}) = 1$ (cf. proof of Lemma 3) and "Proposition 8" in Weil [16]. Therefore, the divisor of the function in question is

$$2 \cdot \left(\sum_{\alpha=1}^{q} Q_{i_\alpha'} - Q_{i_\alpha''}\right),$$

and hence this function differs from

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

$$\prod_{\alpha=1}^{q}(x-a_{i_\alpha'}/x-a_{i_\alpha''})$$

by a constant factor (depending on $M_2,\cdots,M_p$). In this way, we get the following identity

$$(\phi_{s'}/\phi_{s''})\left(\sum_{i=1}^{p}\phi(M_i)\right)=c\cdot\prod_{i=1}^{p}\prod_{\alpha=1}^{q}(x(M_i)-a_{i_\alpha'}/x(M_i)-a_{i_\alpha''}),$$

in which c is a constant factor.

We recall that the divisor of the function $\phi_{s'}/\phi_{s''}$ on J is $2\cdot(W_{s'}-W_{s''})$. Moreover, if we put

$$s=\sum_{\alpha=1}^{p}\phi(Q_{i_\alpha}),\qquad t=\sum_{\alpha=1}^{p}\phi(Q_{j_\alpha}),$$

we have $s+s'+s''+t=0$. Therefore, by Lemma 3 we see that $(\phi_{s'}/\phi_{s''})(s)$ and $(\phi_{s'}/\phi_{s''})(t)$ are both defined and different from 0, ∞. After this remark, we replace $M_1,\cdots,M_p$ by $Q_{i_1},\cdots,Q_{i_p}$ and also by $Q_{j_1},\cdots,Q_{j_p}$ in the above identity, and take the products of both sides of the so-specialized identities. Then we get

$$(\phi_{s'}/\phi_{s''})(s)\ (\phi_{s'}/\phi_{s''})(t)=c^2\text{-times}$$

$$\prod_{\beta=1}^{p}\prod_{\alpha=1}^{q}(i_\beta i_\alpha')(j_\beta i_\alpha')/(i_\beta i_\alpha'')(j_\beta i_\alpha''),$$

in which (IJ) stands for a_I-a_J. We shall show that the left-hand side is ± 1. In general, if r, s, t are arbitrary points of ${}_2J$, we have

$$(\phi_{r+s}/\phi_{r+t})(z)=(c(r,s)/c(r,t))(\phi_s/\phi_t)(z-r).$$

In this identity, we replace r, s, t by s, s', s'' and also by t, s', s'', and take the products of both sides of the so specialized identities. Then, the left-hand side of the new identity is equal to 1. Moreover, it is permissible, by Lemma 3, to replace z by 0 in the right-hand side, and we get

$$(\phi_{s'}/\phi_{s''})(s)(\phi_{s'}/\phi_{s''})(t)=c(s,s'')c(t,s'')/c(s,s')c(t,s').$$

We now take into account of the normalization that we have introduced at the end of the previous section. Then, the right-hand side is simply ± 1, as asserted.

After this remark, we return to the identity involving c and we replace $M_1,\cdots,M_p$ by $Q_{i_1},\cdots,Q_{i_p}$. This is permissible and, combining all that we have said, we obtain the following identity

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

$$(\phi_{s+s'}/\phi_{s+s''})(0)^2 = (\phi_{s'}/\phi_{s''})(s)^2$$
$$= \pm \prod_{\beta=1}^{p} \prod_{\alpha=1}^{q} (i_\beta i_\alpha')(j_\beta i_\alpha'')/(i_\beta i_\alpha'')(j_\beta i_\alpha').$$

Before we state the theorem we have just proved, we shall recall some of the definitions introduced in this section.

The non-singular curve C is of genus $g \geqq 1$ and carries a complete linear system $\mathfrak{g}_2$ of degree two and of dimension one; the $2g+2$ points $Q_0, Q_1, \cdots, Q_{2g+1}$ are the points Q of C such that $2Q$ belong to $\mathfrak{g}_2$; (J, ϕ) is the jacobian variety of C with the canonical function ϕ normalized by $\phi(Q_0) = 0$, and $\phi(Q_i) = s_i$ for $i = 1, 2, \cdots, 2g+1$. In addition to these, we shall denote by Θ the theta-divisor for some level 2 structure in J, and by t the sum of s_i for which $e(\Theta_{s_i}) = -1$. Also, for $s = s_{i_1} + \cdots + s_{i_g}$ with $1 \leqq i_1 < \cdots < i_g \leqq 2g+1$, we shall denote by D_s the product of the discriminant of

$$(x - a_0)(x - a_{i_1}) \cdots (x - a_{i_g})$$

and the discriminant of its complementary factor in the product of all $x - a_k$ for $k = 0, 1, \cdots, 2g+1$. With these notations, we can state the following theorem:

THEOREM 3. *We have $\theta_{s+t}(0) \neq 0$ for s in ${}_2J$ if and only if s is of the form $s_{i_1} + \cdots + s_{i_g}$ with $1 \leqq i_1 < \cdots < i_g \leqq 2g+1$. Furthermore $\theta_{s+t}(0)^8$ and D_s are proportional in the sense that their ratio is independent of s.*

We have only to show that we have $W = \Theta_t$. Suppose that we define t by this. Then, by Lemma 4 we have

$$e(\Theta_{s_i}) c_{\Theta_{s_i}}(t) = e(\Theta_{t+s_i}) = e(\Theta_{t+s_j}) = e(\Theta_{s_j}) c_{\Theta_{s_j}}(t),$$

and hence $e(\Theta_{s_i}) b(s_i, t) = e(\Theta_{s_j}) b(s_j, t)$ for $i, j = 1, 2, \cdots, 2g+1$. Therefore, by Lemma 2 we have $e(\Theta_{s_i}) = e(\Theta_{s_j})$ if and only if s_i, s_j at the same time either appear or not appear in the expression of t as a partial sum of $s_1, s_2, \cdots, s_{2g+1}$. Since the sum of these $2g+1$ points is 0, we seee that t is equal to the sum of s_i for which $e(\Theta_{s_i}) = -1$. This is our previous definition of the point t.

We also note that the number of s_i such that $e(\Theta_{s_i}) = -1$ is congruent to $g \bmod 4$. At any rate, we can write t in the form $s_{i_1} + \cdots + s_{i_k}$ with $0 \leqq k \leqq g$ such that $e(\Theta_{s_i})$ takes the sign ϵ for $i = i_1, \cdots, i_k$ and the opposite sign for the remaining $2g+1-k$ indices. Then, we have $e(\Theta) = e(k) = 1$, and hence $k \equiv g,\ g+1 \bmod 4$. Also, we have $\epsilon = e(k-1)$. Therefore, if

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

$k \equiv g \bmod 4$, we get $\epsilon = -1$ and, if $k \equiv g+1 \bmod 4$, we get $\epsilon = 1$. In the second case, we have only to observe that $2g+1-k \equiv g \bmod 4$. This remark will be used later in proving Lemma 8.

Finally, we shall make some observations which we shall use in Section 4. Suppose that J and J' are principally polarized abelian varieties with symmetric polar divisors X and X' such that (J', X') is a specialization of (J, X). Then, a point, say s', of ${}_2J'$ on X' which does not come from a point of ${}_2J$ on X over the above specialization is singular on X'. Suppose, in fact, that s' is simple on X'. Consider the graphs of $\pm id_J$ in the product $J \times J$ and restrict them to $X \times X$. Call the restrictions Δ, T; similarly for Δ', T'. Then $(\Delta', T', \Delta' \cdot T')$ is the unique specialization of $(\Delta, T, \Delta \cdot T)$ over the given specialization. In fact, we have only to apply the principle of conservation of number in its local form. Since $\Delta' \cap T'$ is zero-dimensional, the components of $\Delta' \cdot T'$ are precisely all points of $\Delta' \cap T'$ which are simple on $X' \times X'$; similarly for $\Delta \cdot T$. Therefore, by assumption $s' \times s'$ is in $\Delta' \cdot T'$. We already have a contradiction here. We note that Δ and T are transversal at every simple point of $X \times X$ in $\Delta \cap T$. The same is true for Δ' and T'. Therefore, if all points of X and X' are simple, the numbers of points of order two on X and on X' are same. Another remark is that, in the special case when $g = 3$, if the symmetric polar divisor has a singular point, the polarized abelian variety can not be the jacobian variety of a non-hyperelliptic curve. This is a simple consequence of "Proposition 18" in Weil [17].

3. The homomorphism ρ. From now on, we shall take the field $\boldsymbol{C}$ of all complex numbers as our universal domain. Let J denote a complex torus of (complex) dimension g and X a positive divisor on J. Then there exists a theta-function with X as its divisor of zeros. The precise meaning is as follows. The universal covering group $\mathfrak{Z}$ of J is a vector space over $\boldsymbol{C}$ of dimension g and the kernel D of the canonical homomorphism $\mathfrak{Z} \to J$ is a lattice in $\mathfrak{Z}$. A holomorphic function $z \to \theta(z)$ defined on $\mathfrak{Z}$ is called a theta-function belonging to D if it has the property

$$\theta(z+d) = e(L_d(z) + c_d) \cdot \theta(z)$$

for every d in D with a $\boldsymbol{C}$-linear form $L_d(z)$ and a constant c_d both depending on d. A theta-function determines a positive divisor on J, provided that it is not the constant zero. A fundamental existence theorem in the theory of theta-functions asserts that every positive divisor of J can be obtained in this way [cf. 19]. Now, we can extend $L_d(z)$ uniquely to a "quasi-hermitian form" on $\mathfrak{Z}$ as $(z, z') \to 2iL_{z'}(z)$ and its hermitian part is a Riemann form belonging to D. In particular, if we put

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

$$\langle z, z' \rangle = L_{z'}(z) - L_z(z'),$$

this alternating form is $\boldsymbol{Z}$-valued on D. If the divisor X has the property that $l(X) = 1$, all elementary divisors of the alternating form $\langle d, d' \rangle$ on D are equal to 1. Therefore, we can choose a base $d_1, \cdots, d_{2g}$ of D so that we get

$$(\langle d_i, d_j \rangle) = \begin{pmatrix} 0 & 1_g \\ -1_g & 0 \end{pmatrix}.$$

Then we choose a $\boldsymbol{C}$-linear isomorphism $\mathfrak{Z} \cong \boldsymbol{C}^g$ so that $(d_1 \cdots d_{2g})$ is mapped to $(\tau 1_g)$. This is always possible and we get a point τ of the Siegel upper-half plane $\mathfrak{S}_g$. We note that the choice of the base of D is not unique but, once it is chosen, the isomorphism $\mathfrak{Z} \cong \boldsymbol{C}^g$ is unique. In particular, the point τ is unique up to the modular transformation $\tau \to M \cdot \tau$ with M in $Sp(g, \boldsymbol{Z})$. Furthermore, we have

$$\theta(z) = \theta_0(z) \cdot \sum_{p \in Z^g} e(\tfrac{1}{2} \cdot {}^t(p + m')\tau(p + m') + {}^t(p + m')(z + m'')),$$

in which $\theta_0(z)$ is a "trivial theta-function," i.e., a function of the form $\exp(\textit{polynomial of degree two})$, and m', m'' are column vectors in $\boldsymbol{R}^g$. We shall denote the theta-series on the right-hand side by $\theta_m(\tau, z)$ in which m is the column vector composed of m' and m''. We note that the last normalization is unique only in the sense that $m \bmod 1$ is unique. We refer to [8] for basic properties of the theta-function $\theta_m(\tau, z)$ of characteristic m. We shall translate results in the previous sections into the language of theta-functions.

First of all, the complex torus J admits a projective embedding given by

$$z \to (\theta_m(\tau, lz))_{lm \equiv 0 \bmod 1}$$

for any $l \geqq 2$. In fact, this is true for every given point τ of $\mathfrak{S}_g$. Because of this fact, if there is no danger of confusion, we shall sometimes call J an abelian variety and use the language introduced for abelian varieties. For instance, we say that the above projective embedding is compatible with the principal polarization on J with X as a polar divisor. Also, we shall denote by Θ the divisor of J determined by $\theta_0(\tau, z)$. We fix an isomorphism ${}_lJ \cong {}_l(\boldsymbol{Q}/\boldsymbol{Z})^{2g}$ defined by $u = (\tau 1_g)m \bmod (\tau 1_g)\boldsymbol{Z}^{2g} \to m \bmod 1$. Then we have

$$\phi_u(z) = (\theta_{-m}(\tau, z)/\theta_0(\tau, z))^l$$
$$\psi_u(z) = \theta_{-m}(\tau, lz)/\theta_0(\tau, lz).$$

Therefore, we get

$$c(u, v) = e(l^t m' n'') \qquad (u, v \to m, n \bmod 1)$$
$$c_\Theta(r) = e(-2^t m' m'') \qquad (2r = 0; r \to m \bmod 1).$$

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

Consequently, the base of ${}_lJ$ giving rise to the above isomorphism ${}_lJ \cong {}_l(\boldsymbol{Q}/\boldsymbol{Z})^{2g}$ is canonical with respect to $\zeta = e(1/l)$. Moreover Θ is even and, in fact, it is the theta-divisor for the level 2 structure in J determined by this canonical base. It is now clear that the theta-constants $\theta_m(\tau) = \theta_m(\tau, 0)$ are indeed the theta-constants in the sense of Section 1. Furthermore, in the case when $l = 2$, the theta-function $\theta_m(\tau, z)$ is even or odd if Θ_r is even or odd, i.e., if $4^t m'm''$ is even or odd for $r \to m \bmod 1$.

Suppose, on the other hand, that a non-singular curve C of genus g is given. We take a base of the homology group $H_1(C, \boldsymbol{Z})$ so that the corresponding $2g \times 2g$ intersection-matrix takes the canonical form, i.e., becomes a matrix composed of 0, 1_g, -1_g, 0. Then we take g linearly independent differentials of the first kind on C such that the period-matrix takes the form $(\tau 1_g)$. This is always possible and we get a point τ of $\mathfrak{S}_g$. As before, the choice of the base of $H_1(C, \boldsymbol{Z})$ is not unique but, once it is chosen, the choice of the g differentials is unique. We shall denote by J the principally polarized abelian variety determined by the point τ. Then J is the jacobian variety of C. Moreover, the canonical function ϕ is given by the following integral

$$\phi(P) = \int_{P_0}^{P} dz \bmod (\tau 1_g)\boldsymbol{Z}^{2g},$$

in which dz denotes the column vector of the g differentials and P_0 a point of C. Furthermore, the image W by ϕ of the $(g-1)$-fold symmetric product of C is of the form Θ_k with a point k of J satisfying $2k = \phi(\mathfrak{k})$, in which $\mathfrak{k}$ is a canonical divisor of C. This is a consequence of the Riemann vanishing theorem.

There is a slightly different way to describe analytically a principally polarized abelian variety with a level l structure. Let τ denote a point of $\mathfrak{S}_g$ and consider the complex torus $\boldsymbol{C}^g/(\tau 1_g)(l\boldsymbol{Z})^{2g}$. Since this is complex-analytically isomorphic to $\boldsymbol{C}^g/(\tau 1_g)\boldsymbol{Z}^{2g}$ in an obvious way, we can consider $\boldsymbol{C}^g/(\tau 1_g)(l\boldsymbol{Z})^{2g}$ as a principally polarized abelian variety. There is a nice projective embedding compatible with the polarization, and it is given by

$$z \to \left(\theta \begin{pmatrix} n' \\ 0 \end{pmatrix} (2l\tau, 2z) \right)_{2ln' \equiv 0 \bmod 1}$$

by the kernel of the epimorphism $\boldsymbol{C}^g/(\tau 1_g)(l\boldsymbol{Z})^{2g} \to \boldsymbol{C}^g/(\tau 1_g)\boldsymbol{Z}^{2g}$ coming from the identity map of $\boldsymbol{C}^g$. We shall prove the following important lemma:

LEMMA 5. *For every $l \geqq 3$, there exist irreducible, non-singular, quasi projective varieties U, U^* over $\boldsymbol{C}$ and a morphism $f: U^* \to U$ such that:*

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

(i) *U is complex-analytically isomorphic to the quotient variety $\Gamma_g(l)\backslash\mathfrak{S}_g$,* (ii) *if T_f denotes the graph of the morphism f and if u denotes the point of U which corresponds to any given point τ of $\mathfrak{S}_g$, the cycle $J_u = f^{-1}(u)$ of U^* is well defined by the following intersection-product*

$$T_f \cdot (U^* \times u) = f^{-1}(u) \times u,$$

and its support is the principally polarized abelian variety with the level l structure which is complex-anaytically isomorphic to $\boldsymbol{C}^g/(\tau 1_g)(l\boldsymbol{Z})^{2g}$ and it has coefficient one, (iii) *there exist l^{2g} rational cross-sections for $f\colon U^* \to U$ such that their values at the point u of U are the points of ${}_l(J_u)$.*

Proof. We consider the so-called Satake compactification of the quotient variety $\Gamma_{g+1}(l)\backslash\mathfrak{S}_{g+1}$, which is the projective variety associated with the graded ring $A(\Gamma_{g+1}(l))$ [cf. 1, 4]. We then take its monoidal transform along the singular locus. We know that the image points in the compactification of all limits

$$\lim_{\mathrm{Im}(w)\to+\infty} \begin{pmatrix} \tau & z \\ {}^t z & w \end{pmatrix}$$

for τ in $\mathfrak{S}_g$ fill up a quasi projective variety U, which is complex-anaytically isomorphic to $\Gamma_g(l)\backslash\mathfrak{S}_g$. We denote by U^* the proper transform of U by the monoidal transformation and by f the restriction to U^* of the monoidal transformation. Then, they have the properties stated in the first part. As for (ii), if we take any point τ_0 of $\mathfrak{S}_g$ and if u_0 denotes the corresponding point of U, the variety U^* is complex-analytically isomorphic over a small neighborhood of u_0 to the variety determined by the following $N = (2l)^g$ rings

$$\boldsymbol{C}\langle\langle \tau - \tau_0 \rangle\rangle[\theta_1(\tau, z)/\theta_k(\tau, z), \cdots, \theta_N(\tau, z)/\theta_k(\tau, z)]$$

for $k = 1, 2, \cdots, N$, in which $\boldsymbol{C}\langle\langle \tau - \tau_0 \rangle\rangle$ is the ring of convergent power-series in the coefficients of $\tau - \tau_0$ and $\theta_1(\tau, z), \cdots, \theta_N(\tau, z)$ are the theta-functions

$$\theta \begin{pmatrix} n' \\ 0 \end{pmatrix} (2l\tau, 2z) \qquad 2ln' \equiv 0 \bmod 1$$

arranged in some order. We refer to [10] for its proof. This shows that the cycle $f^{-1}(u_0)$ calculated by the analytic theory of intersections is irreducible and it is complex-analytically isomorphic to the principally polarized abelian variety with the level l structure determined by the point τ_0. We have only to recall that, as far as algebraic cycles are concerned, the analytic and

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

algebraic theories of intersections are same. Finally, we shall prove the property (iii). Choose any vector x in $\boldsymbol{Z}^{2g}$. Then, to every point u of U, we associate the point $s(u)$ of J_u which corresponds to $(\tau 1_g)x \bmod (\tau 1_g)(l\boldsymbol{Z})^{2g}$ under the isomorphism $J_u \cong \boldsymbol{C}^g/(\tau 1_g)(l\boldsymbol{Z})^{2g}$. It is clear that $s(u)$ is uniquely determined by u and, in this way, we get a holomorphic cross-section s of $f: U^* \to U$. We observe that the inhomogeneous coordinates of s with reference to the ambient projective space of U^* are meromorphic (and algebraic) functions on U, and hence they are rational functions on U [cf. 1]. This shows that the cross-section s is rational. q. e. d.

An immediate consequence of Lemma 5 is that, if $h: W \to U$ is a morphism of a normal algebraic variety W to U and if we consider the fiber-product $W^* = U^* \times W$ over U, the projection $W^* \to W$ defines an "algebraic family" of principally polarized abelian varieties with level l structures, and every such family can be obtained in this way. In particular, the triple (U^*, U, f) is unique up to an isomorphism.

Before we shall apply this consideration to our problem, we introduce some terminology and notations. We shall denote by W the Zariski open subset of $\boldsymbol{C}^{2g+2}$ consisting of points with distinct coordinates. Then W is an irreducible (quasi projective) algebraic variety defined over $\boldsymbol{Q}$. Suppose that $a = (a_0, a_1, \cdots, a_{2g+1})$ is a point of W. Then a non-singular model C of the plane curve defined by the equation

$$y^2 = \prod_{i=0}^{2g+1} (x - a_i)$$

will be called a hyperelliptic curve associated with a. Also, the point τ of $\mathfrak{S}_g$ such that $\boldsymbol{C}^g/(\tau 1_g)\boldsymbol{Z}^{2g}$ is complex-analytically isomorphic to the jacobian variety of C will be called the point of $\mathfrak{S}_g$ associated with a.

LEMMA 6. *Let V denote a normal algebraic variety which is complex-analytically isomorphic to the quotient variety $\Gamma_g(2)\backslash\mathfrak{S}_g$. Then, there exists a morphism $h: W \to V$ such that, for every a in W, the image point $h(a)$ is the point of V which corresponds to one of the points of $\mathfrak{S}_g$ associated with a.*

Proof. We consider the triple (U^*, U, f) for some even level $l \geqq 4$. Then the finite group $\Gamma_g(2)/\Gamma_g(l)$ operates on U as a group of automorphisms and the corresponding quotient variety is isomorphic to V. Let $p: U \to V$ denote the associated epimorphism. We choose a field of definition, say K, of the data involved and pick a generic point a of W over K. Let τ denote one of the points of $\mathfrak{S}_g$ associated with a and u the corresponding point of U. Put $p(u) = v$. We shall show that v is rational over $K(a)$. Suppose that

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

(C', u', v') is a generic specialization of (C, u, v) with reference to the field $K(a)$. Then, there exists a point τ' of $\mathfrak{S}_g$ to which corresponds u'. Moreover $J_u = f^{-1}(u)$ specializes uniquely to $J_{u'} = f^{-1}(u')$ over the above specialization, and they are the jacobian varieties of C and C' respectively. We also note that the level l structure in J_u specializes uniquely to the level l structure in $J_{u'}$. On the other hand, because the specialization is taken over $K(a)$ and is generic, clearly C and C' are isomorphic. Therefore J_u and $J_{u'}$ are isomorphic. Furthermore, the images in $J_{u'}$ of the level 2 structure in J_u under the specialization on one hand and under the isomorphism on the other are same. Consequently, the point τ' is of the form $M \cdot \tau$ with M in $\Gamma_g(2)$, and hence $v' = v$. This shows that v is rational over $K(a)$. The rest is clear.

We note that the morphism h in Lemma 6 is not intrinsic. In fact, we can combine h with any one of the elements of $\Gamma_g(1)/\Gamma_g(2)$ operating on V as a group of automorphisms. From now on, we shall consider the cases when $l = 1, 2$. We shall assume that the characteristic m in θ_m satisfies $2m \equiv 0 \bmod 1$.

After these preliminaries, we shall proceed to construct a homomorphism from the ring $A(\Gamma_g(1))$ of Siegel modular forms to the ring S of projective invariants of a binary form of degree $2g+2$. We recall that the ring $A(\Gamma_g(l))$ is the graded ring generated by holomorphic functions ψ on $\mathfrak{S}_g$ satisfying the functional equation

$$\psi(M \cdot \tau) = \det(c\tau + d)^k \cdot \psi(\tau)$$

for every M in $\Gamma_g(l)$ (plus a condition at infinity for $g = 1$). As for the ring S, it is defined in the following way. In general, consider a homogeneous polynomial of degree r in n variables $x_1, \cdots, x_n$

$$\sum u_{r_1 \cdots r_n} x_1^{r_1} \cdots x_n^{r_n}.$$

The group $SL(n, \boldsymbol{C})$ operates on the variable space "contragrediently" and, if we require that the above form is invariant, the same group operates on the coefficient space. In this way, we get an irreducible representation of $SL(n, \boldsymbol{C})$ of degree

$$\binom{r+n-1}{n-1}.$$

We consider the graded ring of polynomials in the $u_{r_1 \cdots r_n}$ with coefficients in $\boldsymbol{C}$ and operate $SL(n, \boldsymbol{C})$ on this graded ring using its action on its homogeneous part of degree one defined by the above representation. Then, the invariant subring, say $S(n, r)$, is a graded, integrally closed, integral domain

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

over $\boldsymbol{C}$. According to the first main theorem in the classical theory of invariants, it is of finite type over $\boldsymbol{C}$ [cf. 20]. We note that, if I is an element of $S(n,r)$, we can evaluate I at any special homogeneous polynomial of degree r in n variables or at any polynomial of degree r in $n-1$ variables. At any rate, with this notation, the ring S is given by $S(2,2g+2)$. In the special case when $n=2$, the following elementary lemma is useful:

LEMMA 7. *Let $\xi_1,\cdots,\xi_r$ denote independent variables over $\boldsymbol{C}$ and put $P_r(x)=(x-\xi_1)\cdots(x-\xi_r)$. Suppose that $f(\xi)$ is an element of the ring $\boldsymbol{C}[\xi_1,\cdots,\xi_r]$. Then, there exists a homogeneous element I_w of $S(2,r)$ of degree w satisfying $f(\xi)=I_w(P_r(x))$ if and only if* (i) *f satisfies the functional equation*

$$f(M\cdot\xi)=\Big(\prod_{i=1}^{r}(\gamma\xi_i+\delta)\Big)^{-w}\cdot f(\xi),$$

in which $(M\cdot\xi)_i=(\alpha\xi_i+\beta)(\gamma\xi_i+\delta)^{-1}$ for every M in $SL(2,\boldsymbol{C})$ with coefficients α, β, γ, δ, and if (ii) *f is symmetric in $\xi_1,\cdots,\xi_r$.*

We note that an expression of the form

$$(\xi_i-\xi_j)(\xi_k-\xi_l)\cdots,$$

in which every ξ_i appears w times, satisfies the condition (i). We also note that the graded subring of $\boldsymbol{C}[\xi_1,\cdots,\xi_r]$ generated by elements $f(\xi)$ satisfying the condition (i) is integrally closed in this ring. We leave the verification as an exercise to the reader.

Now, we take a point a of W and consider the point τ of $\mathfrak{S}_g$ associated with a. Then, exactly

$$\binom{2g+1}{g}=\tfrac{1}{2}\binom{2g+2}{g+1}$$

of the $\theta_m(\tau)$ are different from zero. On the other hand, there are same number of decompositions $P_I(x)P_{II}(x)$ of $P_{2g+2}(x)$ into products of two polynomials $P_I(x)$, $P_{II}(x)$ each of degree $g+1$. Theorem 3 states that, if $D(P_I)$, $D(P_{II})$ denote the discriminants of $P_I(x)$, $P_{II}(x)$ and put $D_s=D(P_I)D(P_{II})$, there exists a bijection from the set of $\theta_m(\tau)^8\neq 0$ to the set of D_s such that we have

$$\theta_m(\tau)^8=\mu^4\cdot D_s,$$

in which μ^4 is independent of $\theta_m(\tau)^8$. After this remark, we shall prove the following lemma:

LEMMA 8. *Let k denote a positive integer and consider a product*

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

$\theta_{m_1}\cdot\cdot\cdot\theta_{m_{2k}}$ such that $(\theta_{m_1}\cdot\cdot\cdot\theta_{m_{2k}})(\tau)\neq 0$ at the point τ of $\mathfrak{S}_g$ associated with a. Then, by replacing each $\theta_m(\tau)\neq 0$ by the corresponding $(D_s)^{1/8}$, we get a product of integral powers of $a_i - a_j$ if and only if $\theta_{m_1}\cdot\cdot\cdot\theta_{m_{2k}}$ defines a modular form of level 2.

Proof. In general, suppose that we have $l\equiv 2 \bmod 4$. Then $\theta_{m_1}\cdot\cdot\cdot\theta_{m_{2k}}$ with $lm_\alpha\equiv 0 \bmod 1$ defines a modular form of level l if and only if we have

$$(m_1\cdot\cdot\cdot m_{2k})^t(m_1\cdot\cdot\cdot m_{2k}) + (k/2l)\begin{pmatrix}0 & 1_g\\ 1_g & 0\end{pmatrix} \equiv (2/l)\text{-times a half-integer matrix.}$$

This is a consequence of our fundamental lemma in [8]. We shall consider the special case when $l=2$, and proceed to prove the if-part. We shall use C, J etc. to denote the hyperelliptic curve associated with a, its jacobian variety etc. Then, with respect to the level 2 structure in J that we have explained before, the points $s_i=\phi(Q_i)$ have coordinates in ${}_2(\boldsymbol{Q}/\boldsymbol{Z})^{2g}$. For the sake of simplicity, we shall denote them by $s_i \bmod 1$. Also, we put $t\equiv\Sigma' s_i \bmod 1$, in which the summation is extended over those s_i satisfying $4^t s_i' s_i''\equiv 1 \bmod 2$. Then we have $\theta_m(\tau)\neq 0$ if and only if we have

$$m\equiv s_{i_1}+\cdot\cdot\cdot+s_{i_g}+t \bmod 1$$

for some $1\leqq i_1<\cdot\cdot\cdot<i_g\leqq 2g+1$. This is a consequence of Theorem 3. On the other hand, if $\theta_{m_1}\cdot\cdot\cdot\theta_{m_{2k}}$ defines a modular form of level 2, we have

$${}^tx(m_1\cdot\cdot\cdot m_{2k})^t(m_1\cdot\cdot\cdot m_{2k})x+\tfrac{1}{2}k\cdot{}^tx'x''\equiv 0 \bmod 1$$

for every column vector x composed of x', x'' in $\boldsymbol{Z}^g$. We shall show that a_i-a_j appears with an integer exponent in the product of $(D_s)^{1/8}$ which corresponds to $\theta_{m_1}\cdot\cdot\cdot\theta_{m_{2k}}$. Put

$$x\equiv 2\begin{pmatrix}0 & 1_g\\ -1_g & 0\end{pmatrix}(s_i+s_j) \bmod 2$$

for $0\leqq i<j\leqq 2g+1$, in which we put $s_0\equiv 0 \bmod 1$. Then, for the above vector $m \bmod 1$, we have

$$e({}^txm)=b(s_i+s_j,\ s_{i_1}+\cdot\cdot\cdot+s_{i_g}+t).$$

Now, in the case when $i\geqq 1$, we have $b(s_i+s_j, s_{i_1}+\cdot\cdot\cdot+s_{i_g})=1$ if and only if $(a_i-a_j)^{\frac{1}{2}}$ appears in $(D_s)^{1/8}$. Moreover, a case-by-case examination shows that $b(s_i+s_j,t)=-e(\frac{1}{2}\cdot{}^tx'x'')$. Therefore, we get $e({}^txm)=1$, i.e., ${}^txm\equiv 0 \bmod 1$, if and only if either $(a_i-a_j)^{\frac{1}{2}}$ appears in $(D_s)^{1/8}$ and ${}^tx'x''\equiv 1 \bmod 2$ or $(a_i-a_j)^{\frac{1}{2}}$ does not appear in $(D_s)^{1/8}$ and ${}^tx'x''\equiv 0 \bmod 2$.

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

In the case when $i=0$, we have $(-1)^{g-1}b(s_j, s_{i_1}+\cdots+s_{i_g})=1$ if and only if $(a_i-a_j)^{\frac{1}{4}}$ appears in $(D_s)^{1/8}$. Also in this case, if we denote by p the number of i for which $4^t s_i' s_i'' \equiv 1 \bmod 2$ holds, we have $(-1)^{p-1}b(s_j, t) = -e(\frac{1}{2}{}^t x' x'')$. We have shown at the end of the previous section that we have $p \equiv g \bmod 4$. Therefore, the same conclusion as in the case when $i \geqq 1$ holds also in the case when $i=0$. After these preparations, let e denote the exponent of $(a_i-a_j)^{\frac{1}{4}}$ in the product of $(D_s)^{1/8}$ we are talking about. Then we get

$$\begin{aligned} &\tfrac{1}{4}(2k-e)+\tfrac{1}{2}k \equiv 0 \bmod 1, \text{ or} \\ &\tfrac{1}{4}e \qquad\qquad\quad \equiv 0 \bmod 1, \end{aligned}$$

according as ${}^t x' x'' \equiv 1$, or ${}^t x' x'' \equiv 0 \bmod 2$, and hence $e \equiv 0 \bmod 4$. This completes the proof of the if-part. As for the only-if part, since we do not have to use it in this paper, we shall leave it as an exercise to the reader.

We shall consider the subring of $A(\Gamma_g(2))$ consisting of polynomials in the theta-constants (with coefficients in $\boldsymbol{C}$). This ring is generated over $\boldsymbol{C}$ by a finite number of monomials, say $\psi_{k_1}, \psi_{k_2}, \cdots$, of respective degrees $2k_1, 2k_2, \cdots$ in the theta-constants. Then, we can find an algebraically closed subfield K of $\boldsymbol{C}$ such that we have

$$\boldsymbol{C}[\psi_{k_1}, \psi_{k_2}, \cdots] = \boldsymbol{C} \otimes_K K[\psi_{k_1}, \psi_{k_2}, \cdots].$$

Choose a generic point a of W over K and let τ denote one of the points of $\mathfrak{S}_g$ associated with a. Then we have

$$\psi_{k_i}(\tau) = \mu^{k_i} \cdot \rho_2(\psi_{k_i})(a),$$

in which $\rho_2(\psi_{k_i})(a)$ is contained in $K[a]$ for $i=1, 2, \cdots$. Therefore, each $\rho_2(\psi_{k_i})$ defines a polynomial function on W, and we can define $\rho_2(\psi)$ for every ψ in $K[\psi_{k_1}, \psi_{k_2}, \cdots]$ so that ρ_2 gives rise to a ring homomorphism. Then we extend ρ_2 to $\boldsymbol{C}[\psi_{k_1}, \psi_{k_2}, \cdots]$ by linearity. If we introduce $2g+2$ letters $a_0^*, a_1^*, \cdots, a_{2g+1}^*$, the ring of all polynomial functions on $\bar{W} = \boldsymbol{C}^{2g+2}$ can be identified with $\boldsymbol{C}[a^*] = \boldsymbol{C} \otimes_K K[a]$. Moreover, if ψ_k is a monomial in the theta-constants of degree $2k$ contained in $A(\Gamma_g(2))$, then $\rho_2(\psi_k)$ is a product of $a_i^* - a_j^*$ in which every a_i^* appears $\frac{1}{2}gk$ times. In particular, the image or the range of ρ_2 is contained in the subring of $\boldsymbol{C}[a^*]$ defined by the condition (i) of Lemma 7 (after an obvious change of notations). We observe that ρ_2 is not intrinsic. In fact, we can combine ρ_2 with any one of the elements of $\Gamma_g(1)/\Gamma_g(2)$ operating on $A(\Gamma_g(2))$ as a group of automorphisms, because it keeps the domain of ρ_2 stable.

We shall try to extend ρ_2 to the entire ring $A(\Gamma_g(2))$. We first observe

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

that, if k is an even non-negative integer, there always exists an element ψ_k of $A(\Gamma_g(2))_k$ which is a polynomial in the theta-constants satisfying $\rho_2(\psi_k) \neq 0$. For instance, we can take the $2k$-th power of a suitable theta-constant as ψ_k. After this remark, let ψ denote an arbitrary element of $A(\Gamma_g(2))_{k'}$ for any given positive integer k'. We shall *assume* that there exists an element ψ_k of $A(\Gamma_g(2))_k$ which is a polynomial in the theta-constants satisfying $\rho_2(\psi_k) \neq 0$ for some $k \equiv k' \bmod 2$. According to the above remark, this is *not* an assumption in the case when k' is even. By the same reason, we can assume that k is at least equal to k'. Pick an element $\psi_{k''}$ of $A(\Gamma_g(2))_{k''}$ which is a polynomial in the theta-constants satisfying $\rho_2(\psi_{k''}) \neq 0$ for $k'' = k - k'$. This is always possible. Now, we may assume that the morphism h in Lemma 6 is compatible with the homomorphism ρ_2 in the sense that they are both defined by using the same point τ of $\mathfrak{S}_g$ associated with the given generic point a of W over K. Then, Lemma 6 shows that the correspondence $a \to (\psi\psi_{k''}/\psi_k)(\tau)$ defines a rational function on W, and it can be identified with an element, say Ψ, of $\boldsymbol{C}(a^*)$. On the other hand, both $\rho_2(\psi_k)$ and $\rho_2(\psi_{k''})$ are elements of $\boldsymbol{C}[a^*]$ different from zero. Therefore, if we put $\rho_2(\psi) = \Psi\rho_2(\psi_k)/\rho_2(\psi_{k''})$, this will be an element of $\boldsymbol{C}(a^*)$, and we have

$$\psi(\tau) = \mu^{k'} \cdot \rho_2(\psi)(a).$$

In particular, we see that $\rho_2(\psi)$ does not depend on the choice of ψ_k and $\psi_{k''}$. On the other hand, we know that ψ is integral over the domain of the original ρ_2. This implies that $\rho_2(\psi)$ is integral over the range of the original ρ_2, and this is a subring of $\boldsymbol{C}[a^*]$. Therefore $\rho_2(\psi)$ is also contained in $\boldsymbol{C}[a^*]$. In this way, we can extend ρ_2 at least to the subring of $A(\Gamma_g(2))$ generated by homogeneous elements of even weights[2] so that ρ_2 remains to be a ring homomorphism to $\boldsymbol{C}[a^*]$. Furthermore, the range of ρ_2 is still contained in the subring, say S^*, of $\boldsymbol{C}[a^*]$ defined by the condition (i) of Lemma 7. The reason is that the range of the extended ρ_2 is a subring of $\boldsymbol{C}[a^*]$ and it is integral over S^*, and we know that S^* is integrally closed in $\boldsymbol{C}[a^*]$.

LEMMA 9. *Let ψ denote an element of $A(\Gamma_g(1))$ for which $\rho_2(\psi)$ is defined. Then $\rho_2(\psi)$ is contained in the ring S.*

Proof. We may assume that ψ is a homogeneous element of weight k, say. We observe that $\rho_2(\psi)$ is unique up to the factor $i^{\alpha k}$ for $\alpha = 0, 1, 2, 3$, and hence the conclusion does not depend on the choice of ρ_2. We shall denote

[2] We note that, if we are satisfied with defining ρ_2 *only* on this subring, we can dispense with our Lemma 8. In fact, we can define ρ_2 on the subring of $A(\Gamma_g(2))$ generated by the biquadrates of theta-constants without using Lemma 8. Then we have only to extend ρ_2 using Lemma 7 (and using our fundamental lemma).

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

the elementary symmetric functions of $(\theta_m)^8$ by $\Sigma_4, \Sigma_8, \cdots$. We know that they are homogeneous elements of $A(\Gamma_g(1))$ of respective weights $4, 8, \cdots$ [cf. 8]. Furthermore, if a is a point of W and if τ is one of the points of $\mathfrak{S}_g$ associated with a, then $\Sigma_{4k}(\tau)$ becomes the k-th elementary symmetric function of $\theta_m(\tau)^8 \neq 0$ for $k = 1, 2, \cdots$ up to $\frac{1}{2} \cdot (2g+2)!/((g+1)!)^2$. Consequently, we see by Lemma 7 that $I_{2gk} = \rho_2(\Sigma_{4k})$ is a homogeneous element of S of weight $2gk$ for $k = 1, 2, \cdots$. Furthermore, if we denote by $P_{2g+2}(x)$ the product of all $x - a_i$, we have

$$\Sigma_{4k}(\tau) = \mu^{4k} \cdot I_{2gk}(P_{2g+2}(x)),$$

in which $\mu^4 \neq 0$ is unique (although μ itself is not unique). On the other hand, we have $I_{2g}(P_{2g+2}(x)) \neq 0$ as long as the point a is not very special. In fact, if $P_{g+1}(x) = x^{g+1} + \cdots$ is an arbitrary polynomial of degree $g+1$ with distinct roots, we have $I_{2g}(P_{g+1}(x)^2) = 2^g \cdot D(P_{g+1}(x))^2 \neq 0$, in which $D(P_{g+1}(x))$ denotes the discriminant of $P_{g+1}(x)$. Consequently, we have $\Sigma_4(\tau) \neq 0$ as long as a is not very special. After these remarks, we shall consider the plane curve defined by the equation $y^2 = P_{2g+2}(x)$. We then consider the following differentials

$$dx/y, xdx/y, \cdots, x^{g-1}dx/y.$$

On the non-singular model C of the above plane curve, they define linearly independent differentials of the first kind. Finally, we take a base of the homology group $H_1(C, \boldsymbol{Z})$ so that the corresponding $2g \times 2g$ intersection-matrix takes the canonical form. We take representatives of the members of the base so that their images on the plane curve do not pass through the points of ramification. If we integrate the column vector of the above g linearly independent differentials along the $2g$ representatives, we get a $g \times 2g$ period-matrix. Furthermore, it can be written in the form $w(\ 1_g)$ with a $g \times g$ non-degenerate matrix w. The matrix τ is one of the points of $\mathfrak{S}_g$ associated with the point a. Now, if we put $\rho_2(\psi) = I$, we have $\psi(\tau) = \mu^k \cdot I(a)$ with an element I of the subring S^* of $\boldsymbol{C}[a^*]$. The problem is to show that I is symmetric in $a_0^*, a_1^*, \cdots, a_{2g+1}^*$. It is sufficient to show that it is invariant under all transpositions, i.e., permutations interchanging only two indices. Suppose that the given transposition permutes a_{2g} and a_{2g+1}, say. We choose a smooth Jordan curve passing through a_{2g} and a_{2g+1} such that the corresponding closed Jordan domain does not contain other points of ramification. We can then move both a_{2g} and a_{2g+1} in the same direction on the Jordan curve keeping other points of ramification fixed. At the same time, we deform the hyperelliptic curve C together with the $2g$ representative

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

1-cycles, and we get $2g$ representative 1-cycles of a new base of $H_1(C, \mathbf{Z})$ with a similar property. The new base (written as a column vector) is obtained by a left multiplication of an element of $\Gamma_g(1)$ to the original base. Therefore, the left-hand side of

$$\psi(\tau)^4/\Sigma_4(\tau)^k = I(a)^4/I_{2g}(P_{2g+2}(x))^k$$

goes back to its original value after the said deformation. Since $I_{2g}(P_{2g+2}(x))$ is a symmetric function of $a_0, a_1, \cdots, a_{2g+1}$, we see that $I(a)^4$ is invariant under the said transposition. Hence it is invariant under the symmetric group. Since the symmetric group has only two representations of degree one, i.e., the principal character and "sgn," we see that $I(a)$ is either symmetric or alternating. We shall show that the second possibility has to be rejected. We observe that the left-hand side of

$$\psi(\tau)/\det(w)^k = (\mu/\det(w))^k \cdot I(a)$$

goes back to the original value after the deformation we are talking about. Consequently $(\mu/\det(w))^k$ changes its sign at the same time with $I(a)$ by the deformation.[3] In order to examine this situation more closely, we choose a base of $H_1(C, \mathbf{Z})$ so that the representative 1-cycle of the $(g+1)$-th member of the base is a smooth Jordan curve containing a_{2g}, a_{2g+1} such that the corresponding closed Jordan domain does not contain other points of ramification, the representative 1-cycle of the first member of the base is a smooth Jordan curve such that the intersection of the corresponding two closed Jordan domains is a closed Jordan domain containing a_{2g} only, and other representative 1-cycles are all outside the closed Jordon domain containing a_{2g}, a_{2g+1}. For the sake of simplicity, we shall assume that the point 0 is in the Jordan domain containing a_{2g} and a_{2g+1}. We then join a_{2g} and a_{2g+1} by a smooth curve passing through 0 in the Jordan domain. Under these assumptions, we move a_{2g} and a_{2g+1} toward the point 0 on the curve keeping other points of ramification fixed. Then the $g \times 2g$ period-matrix will approach to a matrix of the following form

$$\begin{pmatrix} \infty & * & w'' & * \\ * & w'\tau' & 0 & w' \end{pmatrix},$$

in which $w'(\tau' 1_{g-1})$ is the analogue of $w(\tau 1_g)$ for the plane curve defined by the equation $y^2 = P_{2g}(x) = (x - a_0) \cdots (x - a_{2g-1})$, and w'' is the loga-

[3] According to a formula of Thomae [15], we have $\det(w)^4 = (2\pi i)^{4g}\mu^4$. If we use this formula, we can skip the subsequent argument, which will be used, however, for some other purpose.

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

rithmic period of the differential $dx/x(P_{2g}(x))^{\frac{1}{2}}$ at the point $x=0$. In particular, the point τ approaches to

$$\begin{pmatrix} \infty & * \\ * & \tau' \end{pmatrix}$$

while $\det(w)$ approaches to $\det(w')\cdot w''\neq 0$. We shall show that $(\mu/\det(w))^k$ has a finite limit different from zero. For this purpose, we consider

$$\Sigma_4(\tau)/\det(w)^4 = (\mu/\det(w))^4\cdot I_{2g}(P_{2g+2}(x)).$$

Then, by the limit process we are considering, the left-hand side approaches to $2\cdot\Sigma_4'(\tau')/(\det(w')\cdot w'')^4$ while $I_{2g}(P_{2g+2}(x))$ approaches to $I_{2g}(x^2P_{2g}(x))$. We are denoting by Σ_4' the analogue of Σ_4 for the degree $g-1$. Therefore, the left-hand side is finite and different from zero. On the other hand, we have seen that $I_{2g}(x^2P_{2g}(x))$ is different from zero as long as $P_{2g}(x)$ is not very special. Now, suppose that $I(a)$ is alternating. Then $(\mu/\det(w))^k$ has to approach either to 0 or to ∞ under the limit process. We have shown, however, that this is not the case. Therefore $I(a)$ is symmetric, and this completes the proof.

As a consequence of Lemma 9, we see that the restriction of ρ_2 to $A(\Gamma_g(1))$ gives rise to a homomorphism $\rho=\rho_1$ from $A(\Gamma_g(1))\cap$(domain of ρ_2) to S. We shall state our results in the following way:

THEOREM 4. *Let $A(\Gamma_g(1))$ denote the graded ring of Siegel modular forms of degree g and of level one, and let S denote the graded ring of projective invariants of a binary form of degree $2g+2$. Then, there exists a ring homomorphism*

$$\rho\colon \textit{a subring of } A(\Gamma_g(1))\to S,$$

which increases the weight by a $\frac{1}{2}g$ ratio. The homomorphism ρ is uniquely defined except for the freedom $\rho\to i^{\alpha k}\rho$ on the homogeneous part $A(\Gamma_g(1))_k$ of weight k for $\alpha=0,1,2,3$. The subring, i.e., the domain of ρ, contains all elements of even weights as well as all polynomials contained in $A(\Gamma_g(1))$ in the theta-constants. An element ψ of $A(\Gamma_g(1))$ belongs to the kernel of ρ if and only if ψ vanishes at every point of $\mathfrak{S}_g$ associated with a hyperelliptic curve.

We note that the domain of ρ coincides with $A(\Gamma_g(1))$ for every odd g. Furthermore, since ρ is injective for $g=2$, the theorem and our fundamental lemma show that the domain of ρ coincides with $A(\Gamma_g(1))$ in this case. Actually, we know a *sufficient condition* for the domain of ρ to coincide with $A(\Gamma_g(1))$ when g is even and when $A(\Gamma_g(1))$ actually contains a homogeneous

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

element of an odd weight. The condition is that there exists an element ψ of $A(\Gamma_g(2))_k$ for an odd k which is a polynomial in the theta-constants and which satisfies $\psi(\tau) \neq 0$ for at least one point τ associated with a hyperelliptic curve. We note that this condition is satisfied for $g = 4$. In this case, there exist 126 theta-constants θ_m satisfying $\theta_m(\tau) \neq 0$, and the product of such θ_m defines an element of $A(\Gamma_4(2))_{63}$. We shall also remark that we have certain information concerning the image of ρ. In general, if S is any graded integral domain, we shall denote by $F(S)$ the subfield of the field of fractions of S consisting of homogeneous elements of degree zero, i.e., quotients of homogeneous elements of S of the same degree.

SUPPLEMENT 1. *The domain of ρ coincides with $A(\Gamma_g(1))$ for every odd g and for $g = 2, 4$. The range or the image of ρ is large enough that we have $F(\mathrm{Im}(\rho)) = F(S)$.*

Suppose that $F(S)$ is strictly larger than $F(\mathrm{Im}(\rho))$. Then we can find two general hyperelliptic curves which are birationally equivalent to the plane curves defined by $y^2 = P_{2g+2}(x)$ and $y^2 = P_{2g+2}{}^*(x)$ such that $P_{2g+2}(x)$ and $P_{2g+2}{}^*(x)$ are not projectively equivalent but the jacobian varieties of the hyperelliptic curves are isomorphic (as principally polarized abelian varieties). According to the Torelli theorem [cf. 18], if that is so, the two hyperelliptic curves have to be isomorphic, and hence $P_{2g+2}(x)$ and $P_{2g+2}{}^*(x)$ have to be projectively equivalent. We thus have a contradiction.

SUPPLEMENT 2. *Let χ denote a cusp form of $A(\Gamma_g(1))$ for which $\rho(\chi)$ is defined. Then $\rho(\chi)$ is divisible in the ring S by the discriminant of a binary form of degree $2g+2$, which has weight $2(2g+1)$.*

We shall use the same notations as in the proof of Lemma 9. Then we have

$$\chi(\tau)^4/\Sigma_4(\tau)^k = \rho(\chi)\,(P_{2g+2}(x))/I_{2g}(P_{2g+2}(x)).$$

By the limit process $a_{2g}, a_{2g+1} \to 0$, this relation will specialize to the following relation

$$0 = \rho(\chi)\,(x^2 P_{2g}(x))/I_{2g}(x^2 P_{2g}(x)),$$

and hence $\rho(\chi)$ vanishes for $a_{2g}{}^* - a_{2g+1}{}^* = 0$. Therefore $\rho(\chi)$ is divisible by $a_{2g}{}^* - a_{2g+1}{}^*$ in $\boldsymbol{C}[a^*]$. Since $\rho(\chi)$ is symmetric, it is divisible by the product of all $a_i{}^* - a_j{}^*$ for $i \neq j$. Since the corresponding quotient is alternating, it is divisible by the same product. Therefore $\rho(\chi)$ is divisible by the discriminant.

A consequence of this supplement is that, if the weight of the cusp form χ is smaller than $8 + 4/g$, we necessarily have $\rho(\chi) = 0$. We shall see that the smallest g for which such χ exists is 4.

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

4. Applications. *The reason why the homomorphism ρ is of some use is that the ring S is easier to examine than the ring $A(\Gamma_g(1))$.* For instance, the generating function of the graded ring $S(n,r)$ can be calculated. In general, if N_w denotes the dimension of the homogeneous part of degree w of a graded ring generated over $\boldsymbol{C}$ by a finite number of homogeneous elements of positive degrees, the *generating function* of the ring is the power-series $1+N_1t+N_2t^2+\cdots$. The series is convergent for $|t|<1$, and it has a rational function of t as its analytic continuation such that the denominator is a product of a certain number of polynomials of the form $1-t^p$. In the present case where $S(n,r)$ is the given graded ring, because of the complete reducibility of representations, the dimension N_w is the number of the trivial representation contained in the representation of $SL(n,\boldsymbol{C})$ on the vector space of homogeneous polynomials of degree w in the $u_{r_1\cdots r_n}$ with coefficients in $\boldsymbol{C}$. Therefore, if we denote by $\Phi_1,\cdots,\Phi_m$ the weights of the representation for $w=1$, we have

$$N_w=(1/n!)\int_0^1\cdots\int_0^1\sum e(i_1\Phi_1+\cdots+i_m\Phi_m)\cdot\Delta\bar{\Delta}\,d\phi_1\cdots d\phi_{n-1},$$

in which the summation is extended over non-negative integer solutions of $i_1+\cdots+i_m=w$ and in which $\phi_1+\cdots+\phi_n=0$ and

$$\Delta=\prod_{i<j}(e(\phi_i)-e(\phi_j)).$$

We refer to Weyl [20] for this formula. Passing to the generating function, we get

$$\sum_{w=0}^{\infty}N_wt^w=(1/n!)\int_0^1\cdots\int_0^1\prod_{i=1}^{m}(1-e(\Phi_i)t)^{-1}\cdot\Delta\bar{\Delta}\,d\phi_1\cdots d\phi_{n-1}.$$

In the special case when $n=2$, the $m=r+1$ weights are simply $r\phi$, $(r-2)\phi$, $\cdots$, $-r\phi$. Therefore, the integral for N_w will give the difference of two numbers of partitions while the integral for the generating function can be calculated using residue symbols. For $r=2g+2$ we have

$$\begin{aligned}\sum_{w=0}^{\infty}N_wt^w&=(1/2(1-t))\cdot\mathrm{Res}_{|z|<1}((1-z^2)(1-z^{-2})\\&\qquad\cdot(z\prod_{k=1}^{g+1}(1-z^{2k}t)(1-z^{-2k}t))^{-1}dz)\\&=(1/2(-t)^{g+1}(1-t))\cdot\mathrm{Res}_{|z|\geqq1}((z^2-1)^2z^{g^2+3g-1}\\&\qquad\cdot(\prod_{k=1}^{g+1}(z^{2k}-t)(z^{2k}-t^{-1}))^{-1}dz).\end{aligned}$$

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

The residue at $z=\infty$ exists only in the case when $g=0$, and we get $\mathrm{Res}_\infty=-1$. Other residues exist at $z=t^{-1/2\alpha}$ for $\alpha=1,\cdots,g+1$, and there the residue is given by

$$(-1/2\alpha)(1-t^{1/\alpha})^2 t^{-((g^2+3g+4)/2\alpha)+1} \cdot \Big(\prod_{k=1}^{g+1}(t-t^{-k/\alpha})\cdot\prod_{k\neq\alpha}(t^{-1}-t^{-k/\alpha})\Big)^{-1}.$$

Consequently, for $g=0,1,2,3$ the generating function is given by

$$1/(1-t^2),\quad 1/(1-t^2)(1-t^3)$$
$$(1+t^{15})/(1-t^2)(1-t^4)(1-t^6)(1-t^{10})$$
$$(1+t^8+t^9+t^{10}+t^{18})/\prod_{p=2}^{7}(1-t^p).$$

We shall, now, consider each case separately. We shall denote the roots of $P_{2g+2}(x)$ by $\xi_1,\xi_2,\cdots,\xi_{2g+2}$ and, for the sake of simplicity, put $(ij)=\xi_i-\xi_j$. We note that for $g=1$, 2 the homomorphism ρ is injective. Suppose first that $g=1$. Then we get two elements of $A(\Gamma_1(1))$ as

$$2\cdot\psi_4=\sum(\theta_m)^8,\qquad 2\cdot\psi_6=\sum\pm(\theta_m)^8(\theta_n)^4,$$

in which $(\theta_m)^8(\theta_n)^4$ with ${}^tm=(0\,0)$, ${}^tn=(0\,\frac{1}{2})$ has $+1$ as its coefficient. The ρ-image of $2\cdot\psi_4$ and $2\cdot\psi_6$ are I_2 and I_3 with the following irrational expressions

$$I_2(P_4(x))=\sum(12)^2(34)^2$$
$$I_3(P_4(x))=\sum(12)^2(34)^2(13)(24).$$

The form of the generating function of S shows that we have $S=\boldsymbol{C}[I_2,I_3]$, and hence

$$A(\Gamma_1(1))=\boldsymbol{C}[\psi_4,\psi_6].$$

The homomorphism ρ is, therefore, a bijection decreasing the weight by a $\frac{1}{2}$ ratio. We note also that the ρ-image I_6 of the cusp form of the smallest weight

$$(2^2/3^3)((\psi_4)^3-(\psi_6)^2)=\prod(\theta_m)^8$$

is the discriminant of $P_4(x)$.

We shall next consider the case when $g=2$. There are five elements of $A(\Gamma_2(1))$ to be examined, and they are

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

$$2^2 \cdot \psi_4 = \sum (\theta_m)^8$$

$$2^2 \cdot \psi_6 = \sum_{\text{syzygous}} \pm (\theta_{m_1}\theta_{m_2}\theta_{m_3})^4$$

$$-2^{14} \cdot \chi_{10} = \prod (\theta_m)^2$$

$$2^{17}3 \cdot \chi_{12} = \sum (\theta_{m_1}\theta_{m_2} \cdots \theta_{m_6})^4$$

$$2^{39}5^3 i \cdot \chi_{35} = (\prod \theta_m)\Big(\sum_{\text{azygous}} \pm (\theta_{m_1}\theta_{m_2}\theta_{m_3})^{20}\Big).$$

In the second symmetrization, the monomial $(\theta_{m_1}\theta_{m_2}\theta_{m_3})^4$ with ${}^t m_1 = (0\,0\,0\,0)$, ${}^t m_2 = (0\,0\,0\,\frac{1}{2})$, ${}^t m_3 = (0\,0\,\frac{1}{2}\,0)$ has $+1$ as its coefficient. In the definition of χ_{12}, the summation is extended over fifteen complements of the so-called Göpel quadruples. A Göpel quadruple consists of four distinct even characteristics which form a syzygous sequence. In the definition of χ_{35}, the symmetrization of $\pm (\theta_{m_1}\theta_{m_2}\theta_{m_3})^{20}$ is taken by the stabilizer of $\prod \theta_m$ in $Sp(2, \boldsymbol{Z})$ modulo the stabilizer of $(\theta_{m_1}\theta_{m_2}\theta_{m_3})^{20}$ with ${}^t m_1 = (0\,0\,0\,0)$, ${}^t m_2 = (0\,0\,0\,\frac{1}{2})$, ${}^t m_3 = (0\,\frac{1}{2}\,0\,0)$. Incidentally, we are assuming that this monomial has $+1$ as its coefficient and also that the coefficients of m in $\prod \theta_m$ are $0, \frac{1}{2}$. We shall denote the ρ-images of $2^2 \cdot \psi_4$, $2^2 \cdot \psi_6, \cdots$ by $I_4, I_6, \cdots$. We observe that the graded ring S is generated by homogeneous elements A, B, C, D, E of respective degrees 2, 4, 6, 10, 15 such that E^2 is a polynomial of A, B, C, D. This is a consequence of the form of the generating function of S. We can take

$$A(P_6(x)) = \sum (12)^2(34)^2(56)^2$$

$$B(P_6(x)) = \sum (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2$$

$$C(P_6(x)) = \sum (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2(14)^2(25)^2(36)^2$$

$$D(P_6(x)) = (12)^2(13)^2 \cdots (56)^2$$

$$E(P_6(x)) = \prod \det \begin{pmatrix} 1 & \xi_1 + \xi_2 & \xi_1\xi_2 \\ 1 & \xi_3 + \xi_4 & \xi_3\xi_4 \\ 1 & \xi_5 + \xi_6 & \xi_5\xi_6 \end{pmatrix},$$

and we get

$$I_4 = B, \quad I_6 = (\tfrac{1}{2}) \cdot (AB - 3C), \quad I_{10} = D$$

$$I_{12} = AD, \quad I_{35} = 5^3 \cdot D^2 E.$$

Similar calculations were made by Bolza [3] nearly eighty years ago.

Now, if ψ_k is an arbitrary element of $A(\Gamma_2(1))_k$, its ρ-image is a *polynomial* in A, B, C, D, E with coefficients in $\boldsymbol{C}$. Therefore ψ_k can be written in the form

$$F_0(\psi_4, \psi_6, \chi_{10}, \chi_{12}) + \sum_{p \geqq 1} F_p(\psi_4, \psi_6, \chi_{12})\,(\chi_{12}/\chi_{10})^p,$$

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

multiplied by $\chi_{35}/(\chi_{10})^2$ if k is odd, in which F_p denote polynomials in ψ_4, ψ_6, χ_{10}, χ_{12} with coefficients in $\boldsymbol{C}$. On the other hand, the restrictions of ψ_4, ψ_6, χ_{12} to $\epsilon = \tau_{12} = 0$ are algebraically independent over $\boldsymbol{C}$ and

$$\chi_{12}/\chi_{10} = (\pi\epsilon)^{-2} + \cdots$$
$$\chi_{35}/\chi_{10} = e(\tau_1)e(\tau_2)(e(\tau_1) - e(\tau_2))(\pi\epsilon)^{-1} + \cdots,$$

in which τ_j is the (j,j)-coefficient of τ for $j = 1, 2$. Therefore, unless $F_p = 0$ for all $p \geqq 1$, the modular form ψ_k will have a pole along $\epsilon = 0$. Furthermore, in the case when k is odd, we can write ψ_k in the form

$$G_0(\psi_4, \psi_6, \chi_{10}, \chi_{12})\chi_{35} + \sum_{p=1,2} G_p(\psi_4, \psi_6, \chi_{12})(\chi_{35}/(\chi_{10})^p),$$

in which G_p denote polynomials in ψ_4, ψ_6, χ_{10}, χ_{12} with coefficients in $\boldsymbol{C}$. Again, unless $G_p = 0$ for $p = 1, 2$, the modular form ψ_k will have a pole along $\epsilon = 0$. We have thus obtained the following result

$$A(\Gamma_2(1)) = \boldsymbol{C}[\psi_4, \psi_6, \chi_{10}, \chi_{12}, \chi_{35}].$$

This is our second proof for the structure theorem of $A(\Gamma_2(1))$ and the third for the structure of its subring $A(\Gamma_2(1))^{(2)}$ generated by modular forms of even weights [cf. 9]. Again, in the above proof, the exact analysis of the zeros of χ_{10} is not necessary, while this is essential in the proofs of Freitag [5] and Hammond [6] for the structure of $A(\Gamma_2(1))^{(2)}$.

We also note that an explicit form of E^2 as a polynomial of A, B, C, D can be calculated by a finite (admittedly rather tedious) process. The result can be translated into the language of modular forms, and it is as follows:

$$\begin{aligned}
(\chi_{35})^2 = {} & (1/2^{12}3^9)\cdot\chi_{10}\cdot(2^{24}3^{15}(\chi_{12})^5 - 2^{13}3^9(\psi_4)^3(\chi_{12})^4 \\
& - 2^{13}3^9(\psi_6)^2(\chi_{12})^4 + 3^3(\psi_4)^6(\chi_{12})^3 \\
& - 2\cdot 3^8(\psi_4)^3(\psi_6)^2(\chi_{12})^3 - 2^{14}3^8(\psi_4)^2\psi_6\chi_{10}(\chi_{12})^3 \\
& - 2^{23}3^{12}5^2\psi_4(\chi_{10})^2(\chi_{12})^3 + 3^3(\psi_6)^4(\chi_{12})^3 \\
& + 2^{11}3^637(\psi_4)^4(\chi_{10})^2(\chi_{12})^2 + 2^{11}3^65\cdot 7\psi_4(\psi_6)^2(\chi_{10})^2(\chi_{12})^2 \\
& - 2^{23}3^95^3\psi_6(\chi_{10})^3(\chi_{12})^2 - 3^2(\psi_4)^7(\chi_{10})^2\chi_{12} \\
& + 2\cdot 3^2(\psi_4)^4(\psi_6)^2(\chi_{10})^2\chi_{12} \\
& + 2^{11}3^55\cdot 19(\psi_4)^3\psi_6(\chi_{10})^3\chi_{12} \\
& + 2^{20}3^85^311(\psi_4)^2(\chi_{10})^4\chi_{12} - 3^2\psi_4(\psi_6)^4(\chi_{10})^2\chi_{12} \\
& + 2^{11}3^55^2(\psi_6)^3(\chi_{10})^3\chi_{12} - 2(\psi_4)^6\psi_6(\chi_{10})^3 \\
& - 2^{12}3^4(\psi_4)^5(\chi_{10})^4 + 2^2(\psi_4)^3(\psi_6)^3(\chi_{10})^3
\end{aligned}$$

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

$$+2^{12}3^45^2(\psi_4)^2(\psi_6)^2(\chi_{10})^4+2^{21}3^75^4\psi_4\psi_6(\chi_{10})^5$$
$$-2(\psi_6)^5(\chi_{10})^3+2^{32}3^95^5(\chi_{10})^6).$$

Finally, we shall consider the case when $g=3$. We shall first prove the following lemma which is not restricted to this case:

LEMMA 10. *The product of* $2^{g-1}(2^g+1)$ *even theta-constants is an element of* $A(\Gamma_g(1))$ *for* $g\geqq 3$.

Proof. We shall show that the product, say θ, is a modular form of level 2 for $g\geqq 2$. If the coefficients of m are 0, $\frac{1}{2}$, we have

$$\sum(m_i')^2=\sum(m_i'')^2=2^{2g-4}$$
$$\sum m_i'm_j'=\sum m_i''m_j''=2^{2g-5} \qquad (i\neq j)$$
$$\sum m_i'm_j''=\begin{cases}2^{g-4}(2^{g-1}-1) & (i=j)\\ 2^{2g-5} & (i\neq j),\end{cases}$$

in which the summations are taken over the $2^{g-1}(2^g+1)$ even characteristics. Therefore θ satisfies the condition in [8] to define a modular form of level 2 for $g\geqq 2$. In order to show that θ is actually a modular form of level one, we observe that, if M is an element of $Sp(g,\boldsymbol{Z})$, we have $M\cdot\theta=\epsilon(M)\cdot\theta$ with some $\epsilon(M)$ in $\boldsymbol{C}$. Clearly $M\to\epsilon(M)$ gives rise to a representation of $Sp(g,\boldsymbol{Z}/2\boldsymbol{Z})$ of degree one. On the other hand, it is well known that this group is simple for $g\geqq 3$. Therefore, in this case, we have $\epsilon(M)=1$ for every M in $Sp(g,\boldsymbol{Z})$. This completes the proof.

We know that the product θ does not define a modular form of level one for $g=1,2$. In fact, we have to take its eighth power, square respectively.

Now, suppose that J^* and J are principally polarized abelian varieties such that J is a specialization of J^* over some field. Assume that J^* is a jacobian variety. Then J is either a jacobian variety or a product of jacobian varieties. This is a theorem of Hoyt [7]. We shall explain the second case more generally. If a principally polarized abelian variety J is a product of abelian varieties A_1, A_2 with a polar divisor of the form $X_1\times A_2+A_1\times X_2$, each A_i can be considered as a principally polarized abelian variety with X_i as its polar divisor for $i=1,2$. In particular, if A_i is a jacobian variety (with X_i as a polar divisor), we say that J is a product of the jacobian varieties A_1, A_2. Of course, this can be extended to the case of several factors. On the other hand, suppose that τ and τ_i are points of $\mathfrak{S}_g$ and $\mathfrak{S}_{g_i}$ associated with J and A_i for $i=1,2$. Then τ is equivalent with respect to $Sp(g,\boldsymbol{Z})$ to the following point

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

$$\begin{pmatrix} \tau_1 & 0 \\ 0 & \tau_2 \end{pmatrix}.$$

The point τ may, therefore, be called a reducible point.

After these remarks, we shall consider the special case when $g=3$. We shall denote the modular form introduced in Lemma 10 by χ_{18} for $g=3$. Observe that χ_{18} is a cusp form of weight 18. We shall show that the kernel of the homomorphism ρ is the principal ideal of $A(\Gamma_3(1))$ generated by χ_{18}. In general, let τ denote a point of $\mathfrak{S}_g$ associated with a hyperelliptic curve. Then

$$2^{g-1}(2^g+1)-\binom{2g+1}{g}=0,0,1,10,\cdots$$

even theta-constants vanish at the point τ. Consequently, the product of all even theta-constants is in the kernel of ρ for $g\geqq 3$, and hence $\rho(\chi_{18})=0$. In the following lemma, the modular form Σ_{140} is the thirty-fifth elementary symmetric function of $(\theta_m)^8$:

LEMMA 11. *Let τ denote an arbitrary point of $\mathfrak{S}_3$. Then it corresponds to a non-hyperelliptic jacobian variety when $\chi_{18}(\tau)\neq 0$. It corresponds to a hyperelliptic jacobian variety when $\chi_{18}(\tau)=0$, $\Sigma_{140}(\tau)\neq 0$, and it is reducible when $\chi_{18}(\tau)=\Sigma_{140}(\tau)=0$.*

Proof. Before we start proving the lemma, we shall make it clear that it depends heavily on Lemma 5. Using the notations there, let u^* denote a generic point of U over some common field of definition, say K, of U, U^* and T_f. Also, let u denote the point of U which corresponds to τ. Then $J^*=f^{-1}(u^*)$ is a non-hyperelliptic jacobian variety (with a level l structure). Moreover $J=f^{-1}(u)$ is the unique specialization of J^* over the specialization $u^*\to u$ with reference to K. Therefore J is either a jacobian variety or a product of jacobian varieties. In the second case, we have seen that the point τ is reducible. On the other hand, if J is a hyperelliptic jacobian variety, exactly one even theta-constant vanishes at τ, and hence $\chi_{18}(\tau)=0$, $\Sigma_{140}(\tau)\neq 0$. Moreover, if τ is irreducible, at least six even theta-constants vanish at τ, and hence $\chi_{18}(\tau)=\Sigma_{140}(\tau)=0$. Suppose that we have $\chi_{18}(\tau)=0$. Then, the symmetric polar divisor of J will carry at least 29 points of order two. A remark at the end of Section 2 shows that the symmetric polar divisor has a singular point. Another remark there shows that J can not be a non-hyperelliptic jacobian variety. This completes the proof.

We believe that Lemma 11 answers a question raised by L. Bers in a satisfactory manner. Stated in a very weak form, the lemma says that, *if a*

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

point τ of $\mathfrak{S}_3$ is not reducible, it corresponds to a jacobian variety of a curve (of genus three).

Suppose now that ψ is a homogeneous element in the kernel of the homomorphism ρ. Then ψ vanishes at every point of $\mathfrak{S}_3$ associated with a hyperelliptic curve. Therefore ψ vanishes along every (irreducible) component of the divisor (χ_{18}) of the zeros of χ_{18}. Consequently, the quotient ψ/χ_{18} is holomorphic in $\mathfrak{S}_3$, and hence will define a modular form, provided that the divisor (χ_{18}) has no multiple component. We observe that all components of (χ_{18}) are conjugate with respect to $Sp(3, \boldsymbol{Z})$. On the other hand, if τ_0 is a point of $\mathfrak{S}_2$, where no even theta-constants vanish, and if w is a point of $\mathfrak{S}_1$, we can expand $\chi_{18}(\tau)$ with

$$\tau = \begin{pmatrix} \tau_0 & z \\ {}^t z & w \end{pmatrix}$$

into a power-series in the coefficients z_1, z_2 of z. Moreover, the leading form of this expansion is of degree six, and it is given by

$$-(\tfrac{1}{2})^6 \cdot \Big(\prod_{m_0} \theta_{m_0}(\tau_0)\Big)^3 \Big(\prod_{n_0} \theta_{n_0}(w)\Big)^{16} \cdot \prod_{m_0} \big((\partial\theta_{m_0}/\partial z_1)_0 z_1 + (\partial\theta_{m_0}/\partial z_2)_0 z_2\big),$$

in which the first two products are extended over ten and three even characteristics while the third product is extended over six odd characteristics. We are also putting

$$(\partial\theta_{m_0}(\tau_0, z)/\partial z_j)_{z=0} = (\partial\theta_{m_0}/\partial z_j)_0$$

for $j = 1, 2$. By our previous assumption on the point τ_0, this sextic form is different from zero, and the six linear forms are distinct. Actually, this sextic form defines a hyperelliptic curve of genus two, and the point τ_0 is one of the points of $\mathfrak{S}_2$ associated with this hyperelliptic curve [cf. 12]. We note that the fact that the divisor (χ_{18}) has no multiple component can also be proved by a different method.

THEOREM 5. *The homomorphism ρ is bijective for $g = 1$, injective for $g = 2$, and the kernel is the principal ideal of $A(\Gamma_3(1))$ generated by the cusp form χ_{18} of weight 18 for $g = 3$. In the case when $g = 2$, the graded ring S is generated over the image ring by χ_{12}/χ_{10} and $\chi_{35}/(\chi_{10})^2$. In the case when $g = 3$, there are no cusp forms of weights less than twelve. Moreover, the $\boldsymbol{C}$-base of $A(\Gamma_3(1))_{2k}$ for $k = 1, 2, \cdots, 5$ is given by 0, ψ_4, ψ_6, $(\psi_4)^2$, $\psi_4\psi_6$ and ψ_{10} such that ψ_4, ψ_6, ψ_{10} have ψ_4, ψ_6, χ_{10} for degree two as their images under the Φ-operator.*

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

Proof. The first parts are already proved. We shall, therefore, prove the second parts. Suppose that χ is a cusp form (different from the constant zero) of weight $2k$ for $k \leqq 5$. Then $\rho(\chi)$ is a projective invariant of a binary octavic of weight $3k$. Since χ is not divisible by χ_{18}, we have $\rho(\chi) \neq 0$. On the other hand, Supplement 2 to Theorem 4 shows that $\rho(\chi)$ is divisible by the discriminant, which is a projective invariant of weight 14. The only possibility is that $k = 5$. But then the corresponding quotient will become a projective invariant of weight one, a contradiction. We shall prove the last part. By what we have shown, the dimensions of $A(\Gamma_3(1))_{2k}$ for $k = 1, 2, \cdots, 5$ are at most 0, 1, 1, 1, 2. We shall construct modular form ψ_4, ψ_6, ψ_{10} of weights 4, 6, 10 which generate $A(\Gamma_3(1))_{2k}$ for $k \leqq 5$. We simply take

$$\psi_4 = (\tfrac{1}{2})^3 \cdot \sum (\theta_m)^8.$$

As for ψ_6, we take

$$\psi_6 = (\tfrac{1}{2})^3 \cdot \sum{}' M \cdot \Big(\sum_{m''} \theta_{\binom{0}{(m'')}}^4\Big)\Big(\prod_{m''} \theta_{\binom{0}{(m'')}}\Big),$$

in which $M \bmod 2$ runs over $Sp(3, \mathbf{Z}/2\mathbf{Z})$ modulo its subgroup of index 135 defined by "$c = 0$." As for ψ_{10}, we denote the product of eight θ_m with $m' = 0$ by P_1 and by P_2 the product of θ_m such that $m_3' = m_3'' = 0$ and such that $m_0 = {}^t(m_1' m_2' m_1'' m_2'')$ runs over the set of six even characteristics in degree two in which $m_0' \not\equiv 0 \bmod 1$. Then we consider

$$-2^{14} \cdot \psi_{10} = (1/2^5 3 \cdot 5) \cdot \sum{}' M \cdot P_1 (P_2)^2,$$

in which $M \bmod 2$ runs over $Sp(3, \mathbf{Z}/2\mathbf{Z})$ modulo its subgroup of index 30240 consisting of matrices which are composed of $M_0 \bmod 2$ in $Sp(2, \mathbf{Z}/2\mathbf{Z})$ and of 1_2 such that "$c_0 = 0$" in M_0. It is easy to verify that ψ_4, ψ_6, ψ_{10} thus constructed have the required properties. This completes the proof.

Actually, we know considerably more about the graded ring $A(\Gamma_3(1))$. The whole difficulty lies in the fact that *this ring is complicated* and not in the inadequacy of our method in any sense. We shall publish our results on some other occasion. Instead, we shall discuss a problem raised by E. Witt in [21].[4]

As it has been observed by Witt, if σ denotes a half-integer, positive, non-degenerate matrix with the property $\det(2\sigma) = 1$, its degree is necessarily

[4] We have been informed by Professors Siegel and Witt that this problem has been settled by M. Kneser in his forthcoming paper entitled, "Lineare Relationen zwischen Darstellungsanzahlen quadratischer Formen."

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

of the form $8k$ and, for every non-negative integer g, the corresponding theta-series

$$f_\sigma(\tau) = \sum_u e(\mathrm{tr}(\sigma u \tau {}^t u))$$

for τ in $\mathfrak{S}_g$ defines an element of $A(\Gamma_g(1))_{4k}$. We note that the above summation is taken over the set of all $8k \times g$ integer matrices. Clearly, if we apply the Φ-operator to f_σ for the degree g, we get f_σ for the degree $g-1$, and $f_\sigma = 1$ for $g = 0$. Moreover, if we expand f_σ into Fourier series as

$$f_\sigma(\tau) = \sum_{\sigma'} A(\sigma, \sigma') e(\mathrm{tr}(\sigma'\tau)),$$

in which σ' runs over the set of all half-integer, positive matrices of degree g, the coefficient $A(\sigma, \sigma')$ gives the number of representations of σ' by σ.

Now, if we consider the lattice in $\boldsymbol{R}^{8k}$ consisting of vectors x with coefficients x_i satisfying $x_i \equiv 0 \bmod \frac{1}{4}$, $x_i \equiv x_j \bmod \frac{1}{2}$, $\sum x_i \equiv 0 \bmod 1$, the euclidean metric restricted to this lattice gives rise to an equivalence class of such σ for any given k. We shall denote its representative by σ_k. On the other hand, the class number of all possible σ is known for $k = 1, 2$, and it is $1, 2$. For $k = 2$, if we denote the direct sum of two σ_1 by σ_{11}, then σ_{11} and σ_2 form a complete set of representatives. The *problem of Witt* is whether we have $A(\sigma_{11}, \sigma') = A(\sigma_2, \sigma')$ for all σ' of degree 3, i.e., whether we have $f_{\sigma_{11}} = f_{\sigma_2}$ for $g = 3$. Theorem 5 shows that the answer is affirmative. Moreover, we have

$$A(\sigma_{11}, 1_4) - A(\sigma_2, 1_4) = 2^{12}3^3 5 \cdot 7 \cdot 53.$$

We shall state this fact in the following way:

COROLLARY. *The difference* $\chi_8 = f_{\sigma_{11}} - f_{\sigma_2}$ *for the degree* $g = 4$ *is a cusp form of weight* 8 (different from the constant zero).

We note that, in the case when $g = 3$, the unique modular form of weight 8 has four different expressions, one as an Eisenstein series (in the sense of Siegel), the second as $f_{\sigma_{11}}$ and the third as f_{σ_2}, and the fourth as a homogeneous polynomial of degree two in $(\theta_m)^8$. The resulting identities seem to be of highly non-trivial nature.

THE JOHNS HOPKINS UNIVERSITY.

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms

REFERENCES.

[1] W. L. Baily, "Satake's compactification of V_n," *American Journal of Mathematics*, vol. 80 (1958), pp. 348-364.

[2] ———, "On the theory of θ-functions, the moduli of abelian varieties, and the moduli of curves," ***Annals of Mathematics*, vol. 75 (1962)**, pp. 342-381.

[3] O. Bolza, "Darstellung der rationalen ganzen Invarianten der Binärform sechsten Grades durch die Nullwerthe der zugehörigen θ-Functionen," *Mathematische Annalen*, vol. 30 (1887), pp. 478-495.

[4] Séminaire H. Cartan, *Fonctions automorphes*, E. N. S. (1957-58).

[5] E. Freitag, "Zur Theorie der Modulformen zweiten Grades," *Göttingen Nachrichten*, Nr. 11 (1965), pp. 151-157.

[6] W. F. Hammond, "On the graded ring of Siegel modular forms of genus two," *American Journal of Mathematics*, vol. 87 (1965), pp. 502-506.

[7] W. L. Hoyt, "On products and algebraic families of Jacobian varieties," *Annals of Mathematics*, vol. 77 (1963), pp. 415-423.

[8] J. Igusa, "On the graded ring of theta-constants," *American Journal of Mathematics*, vol. 86 (1964), pp. 219-246; (II), *ibid.*, vol. 88 (1966), pp. 221-236.

[9] ———, "On Siegel modular forms of genus two," *American Journal of Mathematics*, vol. 84 (1962), pp. 175-200; (II), *ibid.*, vol. 86 (1964), pp. 392-412.

[10] ———, "A desingularization problem in the theory of Siegel modular functions," *Mathematische Annalen*, vol. 168 (1967), pp. 228-260.

[11] A. Krazer, *Lehrbuch der Thetafunctionen*, Leipzig (1903).

[12] A. Krazer-W. Wirtinger, "Abelsche Funktionen und algemeine Thetafunktionen," *Enzyklopädie der Mathematischen Wissenschaften*, II B 7, pp. 604-873.

[13] D. Mumford, "On the equations defining abelian varieties," *Inventiones math.*, vol. 1 (1966), pp. 287-354.

[14] C. L. Siegel, "Moduln Abelscher Funktionen," *Göttingen Nachrichten*, Nr. 25 (1964), pp. 365-427.

[15] J. Thomae, "Beitrag zur Bestimmung von $\theta(0,0,\cdots,0)$ durch die Klassenmoduln algebraischer Funktionen," *Crelles Journal*, vol. 71 (1870), pp. 201-222.

[16] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Scientifiques et Industrielles, Paris (1948).

[17] ———, *Variétés abéliennes et courbes algébriques*, Actualités Scientifiques et Industrielles, Paris (1948).

[18] ———, "Zum Beweis des Torellischen Satzes," *Göttingen Nachrichten*, Nr. 2 (1957), pp. 33-53.

[19] ———, *Introduction à l'études des variétés kähleriennes*, Actualités Scientifiques et Industrielles, Paris (1958).

[20] H. Weyl, *The classical groups* (their invariants and representations), Princeton (1946).

[21] E. Witt, "Eine Identität zwischen Modulformen zweiten Grades," *Abhandlungen aus dem Mathematischen Seminar der Hansischen Universität*, vol. 14 (1941), pp. 323-337.

This content downloaded from 129.15.14.45 on Sun, 09 Sep 2018 16:35:25 UTC
All use subject to https://about.jstor.org/terms