JACOBI SUMS AS "GRÖSSENCHARAKTERE"

BY

ANDRÉ WEIL

Let $\mathfrak{o}$ be the ring of integers of an algebraic number-field k of degree d; let $\mathfrak{m}$ be an ideal in $\mathfrak{o}$; a complex-valued function $f(\mathfrak{a})$, defined and $\neq 0$ for all ideals $\mathfrak{a}$ prime to $\mathfrak{m}$ in $\mathfrak{o}$, is a "Grössencharakter" according to Hecke's definition if $f(\mathfrak{a}\mathfrak{b}) = f(\mathfrak{a})f(\mathfrak{b})$ whenever $\mathfrak{a}$, $\mathfrak{b}$ are prime to $\mathfrak{m}$ and if there are rational integers e_λ and complex numbers c_λ $(1 \leqq \lambda \leqq d)$ with the following property: if α is in $\mathfrak{o}$ and is $\equiv 1 \pmod{\mathfrak{m}}$, and if $\alpha_1 = \alpha, \alpha_2, \cdots, \alpha_d$ are the conjugates of α, then $f((\alpha)) = \prod_\lambda \alpha_\lambda^{e_\lambda} |\alpha|_\lambda^{c_\lambda}$. The ideal $\mathfrak{m}$ is called a defining ideal for f. Two such characters are called equivalent if they coincide whenever they are both defined; among the defining ideals of all the characters which are equivalent to a given one, there is one which divides all the others; it is called the conductor of that class of equivalent characters. It is easily seen that classes of equivalent characters are in a one-to-one correspondence with the representations of the group of idèle-classes of k into the multiplicative group of complex numbers; Hecke has shown that one can use them in order to build up L-series which have all the usual properties of the ordinary L-series. Those classes of characters which are of finite order in the group of all such classes are those which occur in the classical classfield theory and in the ordinary L-series; they correspond to the characters of the group of idèle-classes which take the value 1 on the connected component of the neutral element in that group; Artin's law of reciprocity states that they are the same as the characters defined by the cyclic extensions of k. No such arithmetic interpretation is known for the more general characters of Hecke, and to discover one may well be considered as one of the major tasks of modern number-theory.

Here I shall deal with a very special case of this problem by showing that the Jacobi sums are characters (in the sense of Hecke) of cyclotomic fields; Jacobi sums are certain sums of roots of unity, closely related to Gaussian sums(1). This will at the same time be a contribution to the old problem of the determination of the argument for Jacobi sums and Gaussian sums; it will be shown that it also contains the proof for a special case of an interesting conjecture of Hasse on "zeta-functions of algebraic curves over algebraic number-fields".

1. **Jacobi sums.** Let m be any integer >1 and ζ a primitive m-th root of

Received by the editors February 25, 1952.

(1) For a bibliography on this subject, see my article *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. vol. 55 (1949) p. 497; the numbers in brackets will refer to the bibliography at the end of that paper, which will be quoted as NF.

unity over the field $\boldsymbol{Q}$ of rational numbers (e.g. $\zeta = e^{2\pi i/m}$). If t is any integer prime to m, $\zeta \rightarrow \zeta^t$ determines an automorphism σ_t of $\boldsymbol{Q}(\zeta)$ over $\boldsymbol{Q}$; the Galois group of $\boldsymbol{Q}(\zeta)$ over $\boldsymbol{Q}$ consists of all σ_t and therefore is isomorphic with the multiplicative group of integers prime to m modulo m.

Let $\mathfrak{p}$ be any prime ideal prime to m in $\boldsymbol{Q}(\zeta)$, and put $q = N\mathfrak{p}$; then $q \equiv 1 \pmod{m}$. The m-th roots of unity ζ^a, for $0 \leqq a < m$, are all incongruent to each other mod $\mathfrak{p}$ and therefore are all the roots of the congruence $X^m \equiv 1 \pmod{\mathfrak{p}}$ in $\boldsymbol{Q}(\zeta)$. For every integer x prime to $\mathfrak{p}$ in $\boldsymbol{Q}(\zeta)$, $x^{(q-1)/m}$ is a root of that congruence, and so there is one and only one m-th root of unity $\chi_{\mathfrak{p}}(x)$ satisfying the condition

$$\chi_{\mathfrak{p}}(x) \equiv x^{(q-1)/m} \pmod{\mathfrak{p}}.$$

For $x \equiv 0 \pmod{\mathfrak{p}}$ we put $\chi_{\mathfrak{p}}(x) = 0$. Then $\chi_{\mathfrak{p}}$ is a multiplicative character of order m of the field of q elements consisting of the congruence classes in $\boldsymbol{Q}(\zeta)$ mod $\mathfrak{p}$.

Let r be any integer $\geqq 1$; the really significant case is $r = 2$, since the quantities we shall construct are trivial for $r = 1$, and those corresponding to $r > 2$ can all be expressed in terms of those belonging to $r = 2$ and $r = 1$. Let $a = (a_\rho)_{1 \leqq \rho \leqq r}$ be a set of r integers a_ρ modulo m, i.e. an element of the direct product G^r of r groups all identical with the additive group of integers modulo m; the characters on the group G^r are the functions on G^r of the form $\zeta^{\Sigma a_\rho u_\rho}$, where $u = (u_\rho)$ is also an element of G^r. Now write

$$\text{(I)} \qquad J_a(\mathfrak{p}) = (-1)^{r+1} \sum_{\substack{x_1 + \cdots + x_r \equiv -1 (\mathfrak{p}) \\ x_1, \cdots, x_r \bmod \mathfrak{p}}} \chi_{\mathfrak{p}}(x_1)^{a_1} \cdots \chi_{\mathfrak{p}}(x_r)^{a_r}$$

where the x_ρ run over complete sets of representatives of the congruence classes modulo $\mathfrak{p}$ in $\boldsymbol{Q}(\zeta)$ subject to the condition $\sum_{\rho=1}^{r} x_\rho \equiv -1 \pmod{\mathfrak{p}}$. For a given $\mathfrak{p}$, this is a function of $a \in G^r$. If, for any $u = (u_\rho)$, we denote by $N(u)$ the number of distinct sets of congruence classes (x_ρ) modulo $\mathfrak{p}$ satisfying $\sum_{\rho=1}^{r} x_\rho \equiv -1 \pmod{\mathfrak{p}}$ and $\chi_{\mathfrak{p}}(x_\rho) = \zeta^{u_\rho}$ for $1 \leqq \rho \leqq r$, then we have

$$\text{(1)} \qquad J_a(\mathfrak{p}) = (-1)^{r+1} \sum_u N(u) \zeta^{\Sigma a_\rho u_\rho}$$

which gives the expression of $J_a(\mathfrak{p})$ as a function on G^r in terms of the characters on G^r. By induction on r it is easily seen that we have

$$\text{(2)} \qquad J_0(\mathfrak{p}) = q^{-1}[1 - (1 - q)^r].$$

When some but not all of the a_ρ are 0, e.g. if $a_{s+1} = \cdots = a_r = 0$ and none of the $a_1, \cdots, a_s$ is 0, then it is easy to see that $J_a(\mathfrak{p})$ reduces to the sum $J_{a'}(\mathfrak{p})$ similarly built up from $a' = (a_1, \cdots, a_s)$; in particular, if all the a_ρ except a_1 are 0 and $a_1 \neq 0$, then $J_a(\mathfrak{p}) = \chi_{\mathfrak{p}}(-1)^{a_1}$. If we put $\alpha_\rho = a_\rho / m$ for $1 \leqq \rho \leqq r$, $J_a(\mathfrak{p})$, except for the sign, is no other than the Jacobi sum $j(\alpha_1, \cdots, \alpha_r, -\sum_{\rho=1}^{r} \alpha_\rho)$ as defined in NF.

For each $a \in G^r$, we extend the definition of $J_a(\mathfrak{p})$ to all ideals prime to m in $Q(\zeta)$ by the condition

$$\text{(II)} \qquad J_a(\mathfrak{a}\mathfrak{b}) = J_a(\mathfrak{a})J_b(\mathfrak{b})$$

which is to hold whenever $\mathfrak{a}$, $\mathfrak{b}$ are two such ideals. Our main purpose is to prove the following theorem:

THEOREM. *For each $a \neq (0)$, the function $J_a(\mathfrak{a})$ defined by* (I) *and* (II) *is a character on $Q(\zeta)$ in the sense of Hecke; and m^2 is a defining ideal for it.*

In order to prove this, we first observe that for each $\mathfrak{a}$ there is a function $A(u)$ with rational integral values on the group G^r such that

$$\text{(3)} \qquad J_a(\mathfrak{a}) = \sum_u A(u)\zeta^{\Sigma a_\rho u_\rho}$$

for all $a \in G^r$; in fact (1) shows that this is so if $\mathfrak{a}$ is prime; and if $J_a(\mathfrak{a})$, $J_a(\mathfrak{b})$ can be so expressed by means of integral-valued functions $A(u)$, $B(u)$, it follows immediately that $J_a(\mathfrak{a}\mathfrak{b})$ has a similar expression by means of the "convolution" of $A(u)$ and $B(u)$.

Furthermore we have, for all $\mathfrak{a}$:

$$\text{(4)} \qquad J_0(\mathfrak{a})N\mathfrak{a} \equiv 1 \pmod{m^r},$$

where $N\mathfrak{a}$ is the norm of $\mathfrak{a}$. In fact, since m divides $q-1$, (2) shows that this is so when $\mathfrak{a}$ is prime; the general case follows from this at once.

If all the a_ρ except one are 0, and e.g. $a_1 \neq 0$, then, as we have seen, $J_a(\mathfrak{a}) = J_1(\mathfrak{a})^{a_1}$ where $J_1(\mathfrak{a})$ is defined by (II) and by $J_1(\mathfrak{p}) = \chi_\mathfrak{p}(-1)$. If m is odd, we have $J_1(\mathfrak{a}) = 1$ for all $\mathfrak{a}$; if m is even, it is well known that $J_1(\mathfrak{a})$ is a character of conductor 4 on $Q(\zeta)$ belonging to the quadratic extension $Q(\zeta^{1/2})$ of $Q(\zeta)$. This implies that in all cases $J_1((\alpha)) = 1$ whenever α is an integer in $Q(\zeta)$ such that $\alpha \equiv 1 \pmod{m^2}$.

Now we need the prime ideal decomposition of $J_a(\mathfrak{a})$; for a prime $\mathfrak{a}$ this has been obtained by Stickelberger [7] and is as follows. Let $\psi(x)$ be any nontrivial character of the additive group of congruence classes modulo $\mathfrak{p}$ in $Q(\zeta)$; consider the Gaussian sum

$$g(a) = \sum_{x \bmod \mathfrak{p}} \chi_\mathfrak{p}(x)^a \psi(x)$$

for any integer a modulo m; then $g(a)^m$ is an integer in $Q(\zeta)$ whose prime ideal decomposition is given by $(g(a)^m) = \mathfrak{p}^{m\theta(a)}$ and by

$$\text{(5)} \qquad \theta(a) = \sum_{\substack{(t,m)=1 \\ t \bmod m}} \left\langle \frac{ta}{m} \right\rangle \sigma_{-t}^{-1}.$$

Here $\langle\lambda\rangle$ denotes the "fractional part" of the real number λ, defined by putting $\langle\lambda\rangle=\lambda-[\lambda]$ where $[\lambda]$ is the "integral part" of λ, i.e. the greatest integer $\leqq\lambda$; the summation is over all integers t prime to m modulo m. Thus $m\theta(a)$ is an element of the group-ring (with integral coefficients) of the Galois group of $Q(\zeta)$ over Q; symbolic powers of elements and of ideals of $Q(\zeta)$ are to be understood as usual by putting e.g. $\mathfrak{a}^\nu=\prod_t(\mathfrak{a}^{\sigma_t})^{n_t}$ if ν is the element $\nu=\sum_t n_t\sigma_t$ of the group-ring. It is clear that we have

$$\theta(a)\sigma_t=\theta(ta),\qquad \theta(a)(\sigma_0+\sigma_{-1})=\theta(a)+\theta(-a)=\sum_t\sigma_t \tag{6}$$

where t is again prime to m.

We now borrow from NF (p. 501) the classical and easily proved relation

$$J_a(\mathfrak{p})=N\mathfrak{p}^{-1}g(a_1)\cdots g(a_r)g\left(-\sum_{\rho=1}^{r}a_\rho\right), \tag{7}$$

which holds whenever the α_ρ are not all 0 and shows incidentally that $J_a(\mathfrak{a})$ depends symmetrically upon the $r+1$ integers $a_1,\cdots,a_r,-\sum a_\rho$ (a fact which we do not need here). This gives at once, at first for a prime ideal $\mathfrak{p}$ and then for an arbitrary $\mathfrak{a}$, the prime ideal decomposition of $J_a(\mathfrak{a})$:

$$(J_a(\mathfrak{a}))=\mathfrak{a}^{\omega(a)}\qquad (a\not\equiv(0)) \tag{8}$$

where $\omega(a)$ is the element of the group-ring defined by

$$\begin{aligned}\omega(a)&=\sum_{\rho=1}^{r}\theta(a_\rho)+\theta\left(-\sum_{\rho=1}^{r}a_\rho\right)-\sum_t\sigma_t\\&=\sum_{\rho=1}^{r}\theta(a_\rho)-\theta\left(\sum_{\rho=1}^{r}a_\rho\right)\\&=\sum_{\substack{(t,m)=1\\ t \bmod m}}\left[\sum_{\rho=1}^{r}\left\langle\frac{ta_\rho}{m}\right\rangle\right]\sigma_{-t}^{-1}.\end{aligned} \tag{9}$$

The last expression, where [ ] denotes the integral part, shows that the coefficients of the σ_t in $\omega(a)$ are integers $\geqq 0$ and $\leqq r-1$.

At the same time we have $g(0)=-1$ and, for $a\neq 0$, $|g(a)|^2=q$; this last relation (cf. NF p. 501) may be considered as the special case $r=1$ of (7) if one takes into account the value $J_a(\mathfrak{p})=\chi_{\mathfrak{p}}(-1)^a$ of $J_a(\mathfrak{p})$ for $r=1$ and the obvious relation $\overline{g(a)}=\chi_{\mathfrak{p}}(-1)^a g(-a)$. This gives, again at first for a prime ideal and then in general:

$$|J_a(\mathfrak{a})|^2=N\mathfrak{a}^{s-2} \tag{10}$$

if exactly s of the $r+1$ integers a_ρ, $\sum_\rho a_\rho$ are $\not\equiv 0 \pmod m$ and $s\geqq 1$; moreover, when that is so, all the conjugates of $J_a(\mathfrak{a})$ have that same absolute value since they are given by

$$J_a(\mathfrak{a})^{\sigma_t} = J_{ta}(\mathfrak{a}) \tag{11}$$

which is an obvious consequence of (3).

All this applies to the case where $\mathfrak{a}$ is a principal ideal (α). In that case we put, whenever the a_ρ are not all 0:

$$\epsilon(a) = J_a((\alpha))\alpha^{-\omega(a)}. \tag{12}$$

Then, by (8), $\epsilon(a)$ is a unit in $\boldsymbol{Q}(\zeta)$. The conjugate imaginary to any element β of $\boldsymbol{Q}(\zeta)$ is $\beta^{\sigma_{-1}}$, and more generally the conjugate imaginary to β^{σ_t} is $\beta^{\sigma_{-t}}$, so that $|\beta^{\sigma_t}|^2 = \beta^{\sigma_t+\sigma_{-t}}$; using (6) and (9), one finds at once that all conjugates of $\alpha^{\omega(a)}$ have the absolute value $N(\alpha)^{(s-2)/2}$, where s is as above. As the field $\boldsymbol{Q}(\zeta)$ is purely imaginary, there is no distinction to be made between the norms of the number α and of the principal ideal (α). Therefore, by (10), $\epsilon(a)$ and all its conjugates have the absolute value 1. By a classical theorem of Kronecker, this implies that $\epsilon(a)$ is a root of unity and hence of the form $\pm\zeta^h$; but we shall not need this. If all but one of the a_ρ are 0, and e.g. $a_1 \neq 0$, then, by (9), $\omega(a) = 0$ and $\epsilon(a) = J_{a_1}((\alpha))$.

Now take $\alpha \equiv 1 \pmod{m^r}$. By (4) and (12) this implies that

$$J_a((\alpha)) \equiv \epsilon(a) \pmod{m^r}$$

if we put $\epsilon(0) = 1$. For any $u \in G^r$, put

$$E(u) = m^{-r} \sum_a \epsilon(a)\zeta^{-\Sigma a_\rho u_\rho}.$$

If we use (6), (9), (11), and (12), we see at once that $\epsilon(a)^{\sigma_t} = \epsilon(ta)$ for any t prime to m; this implies that the $E(u)$ are invariant by all automorphisms σ_t and are therefore in $\boldsymbol{Q}$. At the same time, using (3), we get

$$E(u) = A(u) + m^{-r} \sum_a \bigl(\epsilon(a) - J_a((\alpha))\bigr)\zeta^{-\Sigma a_\rho u_\rho},$$

which, by the above congruences, shows that the $E(u)$ are integers and therefore rational integers. Finally we have

$$\sum_u | E(u) |^2 = m^{-r} \sum_a | \epsilon(a) |^2$$

(the "Parseval relation" for the group G^r). As all $\epsilon(a)$ have the absolute value 1, the right-hand side is 1; as the $E(u)$ are integers, they are all 0 except one of them which is ± 1; if that one is $E(v)$, we have therefore $\epsilon(a) = E(v)\zeta^{\Sigma a_\rho v_\rho}$ for all a. Taking $a = (0)$, we get $E(v) = 1$. Taking one a_ρ equal to 1 and all others equal to 0, we get $\zeta^{v_\rho} = J_1((\alpha))$ for all ρ. But we have seen that $\alpha \equiv 1 \pmod{m^2}$ implies $J_1((\alpha)) = 1$; so we have proved that if $r \geqq 2$ and $\alpha \equiv 1 \pmod{m^r}$ the units $\epsilon(a)$ are all equal to 1, or in other words

$$J_a((\alpha)) = \alpha^{\omega(a)}$$

whenever the a_ρ are not all 0. This shows that $J_a(\mathfrak{a})$ is a "Grössencharakter" with the defining ideal m^r.

But, as we have mentioned, the characters $J_a(\mathfrak{a})$ for $r>2$ can be expressed in terms of those for $r=1$ and 2; in fact, using (7), once easily gets the relations

$$J_{a_1,\cdots,a_r}(\mathfrak{a}) = J_{a_2}(\mathfrak{a})J_{a_3,\cdots,a_r}(\mathfrak{a})N\mathfrak{a}$$

if $a_1+a_2\equiv 0 \pmod{m}$, and

$$J_{a_1,\cdots,a_r}(\mathfrak{a}) = J_{a_1+a_2}(\mathfrak{a})J_{a_1,a_2}(\mathfrak{a})J_{a_1+a_2,a_3,\cdots,a_r}(\mathfrak{a})$$

if $a_1+a_2 \not\equiv 0 \pmod{m}$. As m^2 is a defining ideal for $r=1$ and for $r=2$ it follows by induction on r that it is also a defining ideal for all r.

It seems doubtful whether m^2 is ever the true conductor of the characters $J_a(\mathfrak{a})$. For $m=4$, one finds that the conductor is 4; when m is an odd prime one finds that the conductor is either $(1-\zeta)$ or $(1-\zeta)^2$; actually it is the latter in the numerical examples which I have examined. A general investigation of this question might lead to results of some interest.

2. **Hasse's conjecture.** Consider the plane algebraic curve

$$\text{(III)} \qquad Y^e = \gamma X^f + \delta$$

where e, f are integers such that $2\leqq e\leqq f$ and γ, δ are nonzero elements of a field k of characteristic prime to ef. Let m be the L.C.M. of e and f, and let ζ be a primitive m-th root of unity in the algebraic closure of k. Then the Galois group of $k(\zeta)$ over k consists of the automorphisms $\zeta\rightarrow\zeta^t$ where t runs over a subgroup H of the multiplicative group of integers prime to m modulo m. If (x, y) is a generic point of the curve (III) over k, the normal field generated by $k(x, y)$ and its conjugates over $K_0=k(x^f, y^e)$ is $K=k(\zeta, x, y)$, and its Galois group Γ consists of the automorphisms

$$(\zeta, x, y) \rightarrow (\zeta^t, \zeta^u x, \zeta^v y)$$

with $t\in H$, $u\equiv 0 \pmod{m/f}$, $v\equiv 0 \pmod{m/e}$, u and v as well as t being taken modulo m; these automorphisms will be denoted respectively by (t, u, v). The subfield $k(x, y)$ of K corresponds to the subgroup G of Γ consisting of the automorphisms $(1, u, v)$ in Γ; this is isomorphic to a subgroup of the group denoted by G^2 in §1. It is an elementary exercise to determine all the irreducible representations of the group Γ and in particular to determine the decomposition into irreducible representations of the permutation group Γ/G (i.e. of the group Γ acting on the cosets of G in Γ). One finds that the latter is the sum of irreducible representations $D_{a,b}$, each taken with coefficient 1; here a is an integer modulo f, b an integer modulo e, and one must take one representative for each set of pairs $(ta, tb)_{t\in H}$. Furthermore one finds that the monomial representation of Γ induced by the character $e^{2\pi i(au+bv)/m}$ of G contains the representation $D_{a,b}$ with the coefficient 1 and does not contain any representation $D_{a',b'}$ not equivalent to $D_{a,b}$.

Assume first that k is a finite field with q elements; for that case the zeta-function of the curve (III) has been determined in NF; it can be written as

$$Z(U) = \prod_{a,b} L_{a,b}(U)$$

where the pair (a, b) runs over a complete set of representatives for the sets of pairs $(ta, tb)_{t\in H}$, a being an integer modulo f and b an integer modulo e, and where the $L_{a,b}(U)$ are as follows. If one and only one of the numbers af^{-1}, be^{-1}, and $af^{-1}+be^{-1}$ is $\equiv 0 \pmod 1$, we have $L_{a,b}(U)=1$; for $a=b=0$, we have

$$L_{0,0}(U) = \frac{1}{(1-U)(1-qU)}\cdot$$

Finally, when af^{-1}, be^{-1}, and $af^{-1}+be^{-1}$ are all $\not\equiv 0 \pmod 1$, let m_0 be the smallest integer such that $a_0=m_0af^{-1}$ and $b_0=m_0be^{-1}$ are integers; m_0 is a divisor of m. Let d be the degree over k of the field $k'=k(\zeta^{m/m_0})$. Let w be a generator of the multiplicative group of nonzero elements in k' such that

$$\zeta^{m/m_0} = w^{(q^d-1)/m_0};$$

let χ be the character of that multiplicative group determined by $\chi(w)=e^{2\pi i m/m_0}$. Then we have

$$L_{a,b}(U) = 1 + \chi[(\gamma^{-1}\delta)^{a_0}(-\delta)^{b_0}]jU^d,$$

where j is the Jacobi sum in k' defined by

$$j = \sum_{\substack{x+y+1=0\\ x,y \text{ in } k'}} \chi(x)^{a_0}\chi(y)^{b_0}.$$

This suggests that the $L_{a,b}(U)$ are no other than the Artin L-functions belonging to the representations $D_{a,b}$, which is indeed the case. In order to verify it, one need only remark that those L-functions, in view of the results stated above, must respectively be the G.C.D.'s of $Z(U)$ and of the L-functions of the field $k(\zeta, x, y)$ over $k(\zeta, x^f, y^e)$; the latter, being abelian L-functions, are easily determined (the case $\gamma=-1$, $\delta=1$ has been treated by Davenport and Hasse in [5], and the general case is quite similar).

Now we take for k an algebraic number-field. If $\mathfrak{p}$ is a prime ideal in k, prime to $ef\gamma\delta$, the equation (III), reduced modulo $\mathfrak{p}$, defines a curve over the finite field with $q=N\mathfrak{p}$ elements; if we call $Z_{\mathfrak{p}}(U)$ the zeta-function of that curve, Hasse defines the zeta-function of the curve (III) over k as

$$\mathcal{Z}(s) = \prod_{\mathfrak{p}} Z_{\mathfrak{p}}(N\mathfrak{p}^{-s}),$$

and he conjectured that this is a meromorphic function satisfying a functional equation of the usual type. Now consider the group Γ and its representations.

When we reduce everything modulo $\mathfrak{p}$, the group H is replaced by the subgroup H_0 of H generated by q; Γ is replaced by the subgroup Γ_0 consisting of the elements of Γ of the form (t, u, v) with $t \in H_0$; and $D_{a,b}$ splits up as follows on Γ_0. If m_0 is again the smallest integer such that $a_0 = m_0 af^{-1}$ and $b_0 = m_0 be^{-1}$ are integers, and if H_0' is the subgroup of H consisting of the elements of H which are $\equiv 1 \pmod{m_0}$, $D_{a,b}$ splits up on Γ_0 into the sum of the representations $D_{ta,tb}$ of Γ_0 where t runs over a set of representatives for the cosets of H_0H_0' in H. Now, to $D_{a,b}$ and $\mathfrak{p}$, we attach the product $P_{a,b,\mathfrak{p}}(U)$ of the L-functions $L_{ta,tb}(U)$ of the curve (III) reduced modulo $\mathfrak{p}$ when t runs over a set of representatives for the cosets of H_0H_0'; and we introduce the function

$$\mathcal{L}_{a,b}(s) = \prod_{\mathfrak{p}} P_{a,b,\mathfrak{p}}(N\mathfrak{p}^{-s}).$$

It is clear that $\mathcal{L}_{a,b}(s) = 1$ when one and only one of the numbers af^{-1}, be^{-1}, $af^{-1}+be^{-1}$ is an integer, and that

$$\mathcal{L}_{0,0}(s) = \zeta_k(s)\zeta_k(s-1)Q_{0,0}(s)^{-1}$$

where $\zeta_k(s)$ is the Dedekind zeta-function of the field k and $Q_{0,0}(s)$ is the product of those factors in the infinite product for $\zeta_k(s)\zeta_k(s-1)$ which pertain to the prime ideals dividing $ef\gamma\delta$. Let now a, b be such that af^{-1}, be^{-1}, $af^{-1}+be^{-1}$ are all $\not\equiv 0 \pmod 1$; define m_0, a_0, b_0 as above; put $\zeta_0 = e^{2\pi i/m_0}$ and $\xi = (\gamma^{-1}\delta)^{a_0}(-\delta)^{b_0}$. For each prime ideal $\mathfrak{P}$ prime to $ef\gamma\delta$ in the field $k(\zeta_0)$, let $\chi_{\mathfrak{P}}(x)$ be the character modulo $\mathfrak{P}$ in $k(\zeta_0)$ defined by taking

$$\chi_{\mathfrak{P}}(x) \equiv x^{(N\mathfrak{P}-1)/m_0} (\mathfrak{P})$$

for all integers x in $k(\zeta_0)$. Then, after some calculations which we will omit, one finds for $\mathcal{L}_{a,b}(s)$ the expression

$$\mathcal{L}_{a,b}(s) = \prod_{\mathfrak{P}} \left(1 - \chi_{\mathfrak{P}}(\xi)J_{a_0,b_0}[N_{k(\zeta_0)/Q(\zeta_0)}\mathfrak{P}]N\mathfrak{P}^{-s}\right)$$

where the product is taken over all prime ideals $\mathfrak{P}$ prime to $ef\gamma\delta$ in $k(\zeta_0)$; N denotes the absolute norm, and $N_{k(\zeta_0)/Q(\zeta_0)}$ the relative norm over $\boldsymbol{Q}(\zeta_0)$ of ideals in $k(\zeta_0)$; as to $J_{a_0,b_0}(\mathfrak{a})$, it is the character we have introduced and studied in §1.

Classfield theory shows that $\chi_{\mathfrak{P}}(\xi)$ is a character in $k(\zeta_0)$ belonging to the cyclic extension $k(\zeta_0, \xi^{1/m_0})$ of $k(\zeta_0)$. The infinite product for $\mathcal{L}_{a,b}(s)$ is therefore no other, except possibly for a finite number of factors, than that for the reciprocal of the Hecke L-function defined on the field $k(\zeta_0)$ by the "Grössencharakter"

$$\chi(\mathfrak{P}) = \chi_{\mathfrak{P}}(\xi)J_{a_0,b_0}[N_{k(\zeta_0)/Q(\zeta_0)}\mathfrak{P}].$$

The missing factors, whose product we shall denote by $Q_{a,b}(s)$, are those pertaining to the prime ideals dividing $ef\gamma\delta$ which do not divide the conductor of that character. As the above character is of absolute value $N\mathfrak{P}^{1/2}$, we write our result as follows:

$$\mathcal{L}_{a,b}(s) = H_{a,b}\left(s - \frac{1}{2}\right)^{-1} Q_{a,b}(s)^{-1},$$

where $H_{a,b}(s)$ is the Hecke L-function defined by means of the character $\chi(\mathfrak{P})N\mathfrak{P}^{-1/2}$.

These results imply that $Z(s)$ is a meromorphic function and that $Z(2-s)Z(s)^{-1}$ can be expressed as a product of a finite number of "elementary" factors (including of course gamma functions) which could easily be written explicitly. Thus we have verified Hasse's conjecture in the case of the curve (III). For $e=2$ and $f=3$ or 4, (III) defines an elliptic curve with a complex multiplication; it would be of considerable interest to investigate more general elliptic curves with a complex multiplication from the same point of view.

University of Chicago,
Chicago, Ill.