AN APPLICATION OF THE POWER RESIDUE THEORY TO SOME ABELIAN FUNCTIONS

TOMIO KUBOTA

Dedicated to the memory of Professor TADASI NAKAYAMA

1°. The aim of this paper is to point out a number-theoretical property of a certain product of values taken by an abelian function at points of finite order of the abelian variety on which the abelian function is considered We use the theory of power residues and the theory of complex multiplication, and the result is somewhat similar to the so-called Stickelberger's relation in the theory of Gauss sums. A related investigation was previously made by the author in a special case of elliptic curves [2].

2°. To begin with, an elementary trick should be explained which we have to use in the proof of our main result.

Let F, F^* be two algebraic number fields of finite degree, both containing the m-th roots of unity. Let $\mathfrak{N}$ be a set of ideals of F, and λ be a mapping of $\mathfrak{N}$ into the set of non-zero elements of F^*. On the other hand, let $\mathfrak{M}$ be a set of ideals of F^*, and let g be a mapping of $\mathfrak{M}$ into the set of non-zero, algebraic numbers such that $g(\mathfrak{b})$ $(\mathfrak{b} \in \mathfrak{M})$ generates an abelian extension over F. Furthermore, we denote by $\sigma(\mathfrak{a})$ the Artin automorphism of an ideal $\mathfrak{a} \in \mathfrak{N}$, and assume

$$g(\mathfrak{b})^{\sigma(\mathfrak{a})} = \left(\frac{\lambda(\mathfrak{a})}{\mathfrak{b}}\right)_m g(\mathfrak{b})$$

whenever $\mathfrak{a}$ is prime to some ideal $\mathfrak{f}_{\mathfrak{b}}$ of F depending on $\mathfrak{b}$, where $\left(\frac{\lambda(\mathfrak{a})}{\mathfrak{b}}\right)_m$ is the m-th power residue symbol in F^*. Then, $g(\mathfrak{b})^m$ belongs to F, a mapping μ of $\mathfrak{M}$ into F is determined by $\mu(\mathfrak{b}) = g(\mathfrak{b})^m$, and we have the following reciprocity formula:

$$(1) \qquad \left(\frac{\mu(\mathfrak{b})}{\mathfrak{a}}\right)_m = \left(\frac{\lambda(\mathfrak{a})}{\mathfrak{b}}\right)_m, \quad (\mathfrak{a} \in \mathfrak{N},\ \mathfrak{b} \in \mathfrak{M},\ (\mathfrak{a}, \mathfrak{f}_{\mathfrak{b}}) = 1),$$

Received February 8, 1965.

where $\left(\frac{\mu(\mathfrak{b})}{\mathfrak{a}}\right)_m$ means the m-th power residue symbol in F.

3°. For the sake of simplicity, we restrict ourselves to the investigation of abelian functions on an abelian variety which belongs in the sense of [3] to a "primitive CM-type" $(F;\ \{\varphi_i\})$ with an abelian extension F over $\mathbf{Q}$ In this case, the dual of $(F;\ \{\varphi_i\})$ is given by $(F;\ \{\varphi_i^{-1}\})$. We shall also assume that the abelian variety, together with all of its endomorphisms, is defined on F in the sense of algebraic geometry, and that A is principal, i.e. the ring of endomorphisms of A is the ring of integers of F. Such an abelian variety actually exists; for example, the Jacobian variety defined over $\mathbf{Q}$ of the complete, non-singular model, defined over $\mathbf{Q}$, of the curve $y^2=1-x^l$, l being an odd prime number. (See [3], p. 129.)

4°. Our main result is the following:

THEOREM. *Let F be an abelian extension of finite degree over $\mathbf{Q}$, and let ζ be a primitive m-th root of unity contained in F. Suppose that A is an abelian varity belonging to a primitive CM-type $(F;\ \{\varphi_i\})$, and that A is principal. Assume A and every endomorphism of A are defined over F. Let now $f(z)$ be a function on A defined over F satisfying $f(\zeta z)=\zeta f(z)$, and β be an integer of F such that $\beta\equiv 1$ (mod m^2). Moreover, denote by B the set of (β)-section points of A different from 0. Then, there exists an element $\gamma\in F$ such that*

$$\prod_{b\in\mathfrak{B}} f(b)=\gamma^m\prod_i \beta^{\varphi_i c_i},$$

where $c_i\in\mathbf{Z}$, $\zeta^{\varphi_i c_i}=\zeta$.

5°. *Proof of the theorem.* As is shown in [3], there is a Grössencharacter λ of F which expresses the action of the Artin automorphism $\sigma(\mathfrak{a})$ of an ideal $\mathfrak{a}$ on section points of A. Namely, if $\mathfrak{a}$ is prime to a certain ideal of F depending on β and A, we have

$$f(b)^{\sigma(\mathfrak{a})}=f(\lambda(\mathfrak{a})b).$$

Furthermore, the number $\lambda(\mathfrak{a})\in F$ has the property

$$\lambda(\mathfrak{a})\cong\prod_i \mathfrak{a}^{\varphi_i^{-1}}.$$

On the other hand, if B is a subset of $\mathfrak{B}$ such that $\{B,\ \zeta B,\ \ldots,\ \zeta^{m-1}B\}=\mathfrak{B}$, then generalized Gauss' lemma (cf. e.g. [2]) yields

$$\prod_{b \in B} f(\nu b) = \left(\frac{\nu}{\beta}\right)_m \prod_{b \in B} f(b)$$

for any integer ν of F prime to β. Therefore, in particular, $g(\beta)^{\sigma(\mathfrak{a})} = \left(\frac{\lambda(\mathfrak{a})}{\beta}\right)_m$ $g(\beta)$ for

$$g(\beta) = \prod_{b \in B} f(b).$$

From now on, we treat only those β for which $g(\beta) \neq 0$, because the theorem is trivial if $g(\beta) = 0$. Applying (1) for the case where $F = F^*$, $\mu(\beta) = g(\beta)^m$, $\mathfrak{N} = \{$the set of ideals $\mathfrak{a}$ for which λ is defined$\}$, and $\mathfrak{M} = \{$the set of all principal ideals (β) with $\beta \equiv 1 \pmod{m^2}$, $g(\beta) \neq 0\}$, we have

$$\left(\frac{\mu(\beta)}{\mathfrak{a}}\right)_m = \left(\frac{\lambda(\mathfrak{a})}{\beta}\right)_m.$$

When β is fixed, this formula is valid for all ideals of F which are prime to one certain ideal of F.

By the theory of power residue symbol including the reciprocity law

$$\left(\frac{\lambda(\mathfrak{a})}{\beta}\right)_m = \left(\frac{\beta}{\lambda(\mathfrak{a})}\right)_m = \prod_i \left(\frac{\beta^{\varphi_i}}{\mathfrak{a}}\right)_m^{\varphi_i^{-1}} = \prod_i \left(\frac{\beta^{\varphi_i c_i}}{\mathfrak{a}}\right)_m,$$

so that

$$\left(\frac{\mu(\beta)}{\mathfrak{a}}\right)_m = \left(\frac{\beta^*}{\mathfrak{a}}\right)_m$$

for $\beta^* = \prod_i \beta^{\varphi_i c_i}$. This shows that $\mu(\beta)/\beta^*$ is the m-th power of an element $\gamma \in F$. Since $\frac{1}{m}(N\beta - 1) \equiv 0 \pmod{m}$ entails

$$\mu(\beta) = \prod_{b \in B} f(b) f(\zeta b) \cdot\cdot\cdot f(\zeta^{m-1} b) = \prod_{b \in B} f(b),$$

the theorem is proved.

6°. Let ζ be a primitive m-th root of unity, and set $F = F^* = \mathbf{Q}(\zeta)$. Let $\mathfrak{N}$ be the set of all ideals of F, and let $\mathfrak{M}$ be the set of all principal prime ideals (π) with $\pi \equiv 1 \pmod{m^2}$. Furthermore, denote by $\lambda(\mathfrak{a})$ the norm of $\mathfrak{a}$, and set

$$g(\pi) = -\sum_{u \bmod \pi} \left(\frac{u}{\pi}\right)_m^{-1} e\left(\frac{1}{p} S_\pi u\right)$$

for $\pi \in M$, where p is the prime number divisible by π, S_π means the local trace, and e is a character of the additive group of $\mathbf{Q}_p$ mod 1 satisfying $e\left(\frac{1}{p}\right) \neq 1$. Then we have

https://doi.org/10.1017/S0027763000011843 Published online by Cambridge University Press

$$g(\pi)^{\rho(\mathfrak{a})} = \left(\frac{\lambda(\mathfrak{a})}{\pi}\right)_m g(\pi)$$

whenever $\mathfrak{a}$ is prime to pm. Therefore, if we set $\mu(\pi) = g(\pi)^m$, it follows from (1) that

$$\left(\frac{\mu(\pi)}{\mathfrak{a}}\right)_m = \left(\frac{\lambda(\mathfrak{a})}{\pi}\right)_m.$$

By the same argument as in 5°, we can deduce from this

$$\mu(\pi) = \gamma^m \prod_\sigma \pi^{\sigma c_\sigma}, \ \gamma \in F, \tag{2}$$

where σ runs through the Galois group of $F/\mathbf{Q}$, and $c_\sigma \in \mathbf{Z}$, $\zeta^{\sigma c_\sigma} = 1$. The formula (2) has a similar form to the explicit decomposition $\mu(\pi) = \prod_\sigma \pi^{\sigma c_\sigma}$ of $\mu(\pi)$ obtained by Stickelberger's relation (see [1], [4]), although the latter is a far stronger assertion than the former. Since the formula in our main theorem also has the same form as (2), it may be regarded as a first approach to a deeper result, like Stickelberger's relation, about abelian functions.

References

[1] H. Hasse, Zetafunktion und L-Funktion zu einem arithmetischen Funktionenkörper vom Fermatschen Typus, Abh. Deutsch. Akad. der Wiss. zu Berlin, Klasse für Math. und allg. Naturw., Jahrg. 1954, Heft 4.

[2] T. Kubota, Reciprocities in Gauss' and Eisenstein's number fields, J. reine angew. Math. **208** (1961), 35-50.

[3] G. Shimura and Y. Taniyama, Complex multiplication of abelian varieties and its application to number theory, Publ. of the Math. Soc. of Japan **6** (1961).

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

Mathematical Institute
Nagoya University