COMPLEX MULTIPLICATION AND PRINCIPAL IDEAL THEOREM

FUMIYUKI TERADA

(Received February 15, 1954)

Introduction

The principal ideal theorem, which asserts that all ideals in a ground field become principal in the absolute class field, was translated by Artin into a group-theoretical one, and this was proved by Fürtwängler[1]. An arithmetical proof of this theorem is desired, and it is given only in the case of the cyclic absolute class field by the formula of the self-conjugate classes.

In the case of the quadratic imaginary ground field, Prof. H. Hasse gave a concrete respresentation of this theorem employing the complex multiplication[2]. But he restricted himself to the ideals $\mathfrak{m}$ with $N\mathfrak{m} \equiv 1 \bmod 12$, and as he mentioned recently[3], each absolute ideal class contains not always such an ideal, when the discriminant is not prime to 12.

In this note, we shall give a remark to the Hasse's proof and show that an analogous method is applicable to the ideals $\mathfrak{m}$ with $N\mathfrak{m} \equiv 5 \bmod. 12$.

1. Let $\Omega = R(\sqrt{d})$ be a quadratic imaginary extension of the rational field R with discriminant d, and K be the absolute class field of Ω. Let α_1, α_2 be numbers in Ω which constitute a basis of an ideal $\mathfrak{a}$ in Ω. Then it is shown that $K = \Omega(j(\alpha_1, \alpha_2))$, where $j(\alpha_1, \alpha_2)$ is a singular value of the modular function $j(\omega_1, \omega_2)$. Let $\mathfrak{m}$ be an ideal in Ω such that 1) $(\mathfrak{m}, 12d) = 1$, 2) $\mathfrak{m}$ is decomposable into the product of prime ideals in Ω with degree 1. Prof. H. Hasse proved the following theorem:

If $N\mathfrak{m} \equiv 1 \bmod 12$, then the number

$$\psi_M(\alpha_1, \alpha_2) = \frac{\Delta_{12}\left(\frac{1}{m} M(\alpha_1, \alpha_2)\right)}{\Delta_{12}(\alpha_1, \alpha_2)} = \frac{\Delta_{12}\left(\frac{\mathfrak{a}}{\mathfrak{m}}\right)}{\Delta_{12}(\mathfrak{a})} \tag{1}$$

is contained in $K = \Omega(j(\alpha_1, \alpha_2))$, and $\mathfrak{m} = (\psi_M(\alpha_1, \alpha_2))$, where M is a primitive transformation of degree $m = N\mathfrak{m}$ such that 1) $M \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 12$, 2) M

1) There are several simple proofs of this theorem. Moreover, a generalization of this theorem was proved by T. Tannaka and the author. cf. T. Tannaka, An alternative proof of the generalized principal ideal theorem, Proc. of the Japan Acad., vol. 25(1949): F. Terada, On a generalization of the principal ideal theorem, Tôhoku Math. Journ., 2nd Ser., vol. 1 (1949).

2) H. Hasse, Zum Hauptidealsatz der komplexen Multiplikation, Mont. f. Math. u. Phys., 38(1931).

3) H. Hasse, Zur Geschlechterie in quadratischen Zahlkörpern. Journ. of the Math. Soc. of Japan, vol. 3(1951), S. 449-456.

transforms α_1, α_2 to a basis of the ideal $m\cdot\frac{\mathfrak{a}}{\mathfrak{m}} = \overline{\mathfrak{m}}\,\mathfrak{a}$, and the function $\Delta_{12}(\omega_1, \omega_2)$ is given by the following

$$(2)\qquad \Delta_{12}(\omega_1, \omega_2) = \frac{2\pi}{\omega_2} q^{\frac{1}{12}} \prod_{k=1}^{\infty}(1-q^k)^2,\quad q^{\frac{1}{12}} = \exp\left(\frac{2\pi i}{12}\cdot\frac{\omega_1}{\omega_2}\right),\quad \mathfrak{F}\left(\frac{\omega_1}{\omega_2}\right) > 0.$$

In the proof of this theorem, he asserted that each class of the m-th primitive transformation can be represented by a transformation M_ν such that

$$(3)\qquad M_\nu = \begin{pmatrix} a_\nu & b_\nu \\ 0 & d_\nu \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 12, \quad \text{where } a_\nu d_\nu = m \equiv 1 \bmod 12.$$

But, for example if $m = 25$, the class which contains a transformation of the form $\begin{pmatrix} a_\nu & b_\nu \\ 0 & d_\nu \end{pmatrix} \equiv \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix} \bmod 12$, will not be represented by a transformation of the form (3). If we treat only prime ideals, the above assertion is correct by the restriction $m \equiv 1 \bmod. 12$. Nevertheless, to avoid the use of the theorem of the arithmetical progression, it will be desirable to treat also the case of a non-prime m. Therefore, it needs to add a certain consideration to the Hasse's proof, and it will be shown in the following 3, especially the formula (7).

2. In general, let $\mathfrak{m}$ be an ideal in Ω which is prime to $12d$. Then $\mathfrak{m}$ is decomposable into a product of prime ideals with degree 1 and prime ideals with degree 2. Since each prime ideal with degree 2 is principal, we may assume that $\mathfrak{m}$ is a product of prime ideals with degree 1, when we concern the principal ideal theorem. Let us now select a complete system of representations of the $\psi(m)$ classes of the m-th primitive transformation M_ν by the following manner. Since $(m, 12d) = 1$, we may select so as

$$M_\nu = \begin{pmatrix} a_\nu & b_\nu \\ 0 & d_\nu \end{pmatrix},\quad \text{where}\begin{cases} b_\nu \equiv 0 \bmod 12,\ a_\nu d_\nu = m,\ a_\nu > 0,\ d_\nu > 0 \\ b_\nu \text{ constitute representations mod } d_\nu. \end{cases}$$

Moreover, let us divide the problem into four cases according to the value of $m = N\mathfrak{m}$, and in each case, we shall select suitable normalized representations. That is:

Case 1. $m \equiv 1 \bmod 12$. If $a_\nu \equiv d_\nu \equiv 7$ or $a_\nu \equiv d_\nu \equiv 11 \bmod 12$, multiplying a modular transformation $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, we may construct a system of representations so as

$$(4)\qquad M_\nu = \begin{pmatrix} a_\nu & b_\nu \\ 0 & d_\nu \end{pmatrix},\quad \text{where}\begin{cases} b_\nu \equiv 0 \bmod 12,\ a_\nu d_\nu = m \\ b_\nu \text{ constitute representations mod } |d_\nu|, \end{cases}$$

and

$$(5)\qquad M_\nu \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{or} \equiv \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix} \bmod 12.$$

Case II. $m \equiv 5 \bmod 12$. By the same way as it was described in Case I, we may construct a system of representations of the same form as (4), where the additional condition (5) is replaced by the following

$$(5')\qquad M_\nu \equiv \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix} \text{ or } \equiv \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix} \bmod 12.$$

Case III. $m \equiv 7 \bmod 12$. Instead of (5)

$$M_\nu \equiv \begin{pmatrix} 7 & 0 \\ 0 & 1 \end{pmatrix} \text{ or } \equiv \begin{pmatrix} 1 & 0 \\ 0 & 7 \end{pmatrix} \bmod 12. \tag{5''}$$

Case IV. $m \equiv 11 \bmod 12$. Instead of (5)

$$M_\nu \equiv \begin{pmatrix} 11 & 0 \\ 0 & 1 \end{pmatrix} \text{ or } \equiv \begin{pmatrix} 1 & 0 \\ 0 & 11 \end{pmatrix} \bmod 12. \tag{5'''}$$

3. Let us now operate a modular transformation S to the arguments of function $\psi_{M_\nu}(\omega_1, \omega_2)$. Then, if $M_\nu S = S_\nu M_\mu$,

$$\psi_{M_\nu}(S(\omega_1, \omega_2)) = \frac{\Delta_{12}\left(\frac{1}{m} M_\nu S(\omega_1, \omega_2)\right)}{\Delta_{12}(S(\omega_1, \omega_2))} = \frac{\chi_{12}(S_\nu)\Delta_{12}\left(\frac{1}{m} M_\mu(\omega_1, \omega_2)\right)}{\chi_{12}(S)\Delta_{12}(\omega_1, \omega_2)}$$
$$= \frac{\chi_{12}(S_\nu)}{\chi_{12}(S)} \psi_{M_\mu}(\omega_1, \omega_2),$$

where $\chi_{12}(S)$ is given by the following formula[4], i.e. if $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$,

$$\chi_{12}(S) = \chi_3(S)\chi_4(S)^{-1}$$
$$\chi_3(S) = \exp\left(\frac{2\pi i}{3} (a^2 + c^2)(ab + cd)\right)$$
$$\chi_4(S) = \exp\left(\frac{2\pi i}{4} [a^2(ab - ac - a + 1) + (1 - a^2)(ac + cd + d)]\right)$$

Now, if $S_\nu = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$, then the relation $M_\nu S = S_\nu M_\mu$ means

$$e \equiv a'_\mu a_\nu a, \quad f \equiv d'_\mu a_\nu b, \quad g \equiv a'_\mu d_\nu c, \quad h \equiv d'_\mu d_\nu d \bmod 12,$$

where a'_μ and d'_μ are such that $a'_\mu\, a_\mu \equiv 1 \equiv d'_\mu\, d_\mu \bmod 12$. From these relations we have a relation between $\chi_{12}(S)$ and $\chi_{12}(S_\nu)$, which is the following lemmas.

LEMMA 1. *In the case I, we get for an arbitrary modular transformation S and an arbitrary M_ν,*

$$\chi_{12}(S_\nu) = \chi_{12}(S).$$

PROOF. Since $a_\nu^2 \equiv d_\nu^2 \equiv a'^2_\mu \equiv d'^2_\mu \equiv 1 \bmod 12$,

$$\chi_3(S_\nu) = \exp\left(\frac{2\pi i}{3} (e^2 + g^2)(ef + gh)\right) \tag{6}$$
$$= \exp\left(\frac{2\pi i}{3} (a^2 + c^2) \cdot (ab + cd)m\right)$$

where m' is such that $mm' \equiv 1 \bmod 12$, and therefore $m' \equiv 1 \bmod 12$ in our case. Then it follows that $\chi_3(S_\nu) = \chi_3(S)$. On the other hand, we have from (5), $a_\nu \equiv d_\nu \equiv a'_\mu \equiv d'_\mu = 1 \bmod 4$, and it follows that $e \equiv a, f \equiv b, g \equiv c, h \equiv d \bmod 4$, and this shows that $\chi_4(S_\nu) = \chi_4(S)$.

LEMMA 2. *In the case II, we get for arbitrary S and M_ν,*

$$\chi_{12}(S_\nu) = \chi_{12}(S)\chi_3(S).$$

PROOF. Since $m' \equiv 5 \bmod 12$ in (6), we have $\chi_3(S_\nu) = \chi_3(S)^2$. On the other hand, as it was mentioned in the proof of Lemma 1,

4) R. Fricke, Die elliptischen Funktionen und ihre Anwendungen, Berlin.

$\chi_4(S_\nu) = \chi_4(S)$, and our lemma follows immediately.

From these lemmas, we have the following formulas; that is, if $m \equiv 1$ mod 12

(7) $$\psi_{M_\nu}(S(\omega_1, \omega_2)) = \psi_{M_\mu}(\omega_1, \omega_2), \text{ where } M_\mu \sim M_\nu S,$$

and if $m \equiv 5$ mod 12,

(8) $$\psi_{M_\nu}(S(\omega_1, \omega_2)) = \chi_3(S)\psi_{M_\mu}(\omega_1, \omega_2), \text{ where } M_\mu \sim M_\nu S.$$

In the case III and IV, we may conclude analogous formulas. But in these cases $\chi_{12}(S_\nu)/\chi_{12}(S)$ are the quadratic and 6-*th* root of 1, respectively. And especially they are dependent not only on S but on the suffix ν.

4. As it was treated by Hasse, we can find a function $l_{M_\nu}(\omega_1, \omega_2)$ such that 1) $l_{M_\nu}(\alpha_1, \alpha_2)$ is contained in the absolute class field $\Omega(j(\alpha_1, \alpha_2))$ of Ω, 2) $l_{M_\nu}(\alpha_1, \alpha_2) \neq l_M(\alpha_1, \alpha_2)$ if $M_\nu \not\sim M$, 3) $l_{M_\nu}(S(\omega_1, \omega_2)) = l_{M_\mu}(\omega_1, \omega_2)$ where $M_\mu \sim M_\nu S$. Then the polynomial

$$L(t, \omega_1, \omega_2) = \prod_{\nu=1}^{\psi(m)} (t - l_\nu(\omega_1, \omega_2)).$$

is a polynomial of t and the function $j(\omega_1, \omega_2)$ with integral coefficient.

Now, as it was mentioned by Hasse

(9) $$\mathfrak{m} = (\psi_M(\alpha_1, \alpha_2)),$$

and, especially in the case I, $\psi_M(\alpha_1, \alpha_2)$ is contained in $\Omega(j(\alpha_1, \alpha_2))$. That is, from (7), the coefficient of the polynomial

(10) $$G(t\,; \omega_1, \omega_2) = L(t, j(\omega_1, \omega_2)) \cdot \sum_{\nu=1}^{\psi(m)} \frac{\psi_{M_\nu}(\omega_1, \omega_2)}{t - l_{M_\nu}(\omega_1, \omega_2)}$$

are invariant under each modular transformation, and this polynomial is a polynomial of t and $j(\omega_1, \omega_2)$ with integral coefficient, and finally,

(11) $$\psi_M(\alpha_1, \alpha_2) = \frac{G(l_M(\alpha_1, \alpha_2), j(\alpha_1, \alpha_2))}{L'(l_M(\alpha_1, \alpha_2), j(\alpha_1, \alpha_2))}$$

is contained in the absolute class field $\Omega(j(\alpha_1, \alpha_2))$ of Ω.

On the contrary, in the case II, the coefficients of $G(t\,; \omega_1, \omega_2)$ are not invariant under modular transformations; that is from (8),

$$G(t\,; S(\omega_1, \omega_2)) = \chi_3(S)G(t;\, \omega_1, \omega_2)$$

The coefficients of t are cubic algebraic functions of $j(\omega_1, \omega_2)$. Nevertheless, the coefficients of a polynomial

(12) $$G_3(t\,; \omega_1, \omega_2) = L(t\,; j(\omega_1, \omega_2)) \sum_{\nu=1}^{\psi(m)} \frac{\psi^3_{M_\nu}(\omega_1, \omega_2)}{t - l_{M_\nu}(\omega_1, \omega_2)}$$

are invariant under each modular transformation. Moreover, $\psi^3_{M_\nu}(\omega_1, \omega_2)$ has the following q-expansion:

$$\psi^3_{M_\nu}(\omega_1, \omega_2) = \frac{\left(\dfrac{m}{d_\nu}\right)^3 q^{\frac{a_\nu}{4d_\nu}} \zeta_\nu^{\frac{|b_\nu|}{4}} \prod_{k=1}^{\infty} (1 - \zeta_\nu^{k|b_\nu|} q^{k\frac{a_\nu}{d_\nu}})^6}{q^{\frac{1}{4}} \prod_{k=1}^{\infty} (1 - q^k)^6}$$

$$= a_\nu^3 q^{\frac{1}{4}\left(\frac{a_\nu}{d_\nu}-1\right)} \zeta_\nu^{\frac{|b_\nu|}{4}} \frac{\prod_{k=1}^{\infty}(1-\zeta_\nu^{k|b_\nu|} q^{k\frac{a_\nu}{d_\nu}})^6}{\prod_{k=1}^{\infty}(1-q^k)^6},$$

where $\zeta_\nu = \exp\left(\frac{2\pi i}{|d_\nu|}\right)$. This expansion does not depend on the 4-th root of 1, because $a_\nu - d_\nu \equiv 0,\ b_\nu \equiv 0 \bmod 4$. Then it follows that the coefficients of the polynomial $G_3(t;\ \omega_1, \omega_2)$ are polynomials of the function $j(\omega_1, \omega_2)$ with rational integral coefficient. Therefore,

$$\psi_M^3(\alpha_1, \alpha_2) = \frac{G_3(l_M(\alpha_1, \alpha_2), j(\alpha_1, \alpha_2))}{L'(l_M(\alpha_1, \alpha_2), j(\alpha_1, \alpha_2))}$$

is contained in $\Omega(j(\alpha_1, \alpha_2))$, and from (9) $\mathfrak{m}^3 = (\psi_M^3(\alpha_1, \alpha_2))$.

On the other hand, the ideal $\mathfrak{m}^2$ is an ideal treated in the case I, and the number

$$\psi_N(\alpha_1, \alpha_2) = \frac{G(l_N(\alpha_1, \alpha_2), j(\alpha_1, \alpha_2))}{L'(l_N(\alpha_1, \alpha_2), j(\alpha_1, \alpha_2))}$$

is contained in $\Omega(j(\alpha_1, \alpha_2))$ and $\mathfrak{m}^2 = (\psi_N(\alpha_1, \alpha_2))$, where N is a m^2-th primitive transformation which transforms $\alpha_1 . \alpha_2$ to a basis $m^2 \frac{\mathfrak{a}}{\mathfrak{m}^2} = \overline{\mathfrak{m}}^2\mathfrak{a}$. Then, we have a number

$$\frac{G_3(l_M(\alpha_1, \alpha_2), j(\alpha_1, \alpha_2))}{L'(l_M(\alpha_1, \alpha_2), j(\alpha_1, \alpha_2))} \frac{L'(l_N(\alpha_1, \alpha_2), j(\alpha_1, \alpha_2))}{G(l_N(\alpha_1, \alpha_2), j(\alpha_1, \alpha_2)} \tag{12}$$

which is contained in the absolute class field $\Omega(j(\alpha_1, \alpha_2))$ and generate the ideal $\mathfrak{m}$ in this field.

From the above consideration, we have a concrete representation of the principal ideal theorem concerning a ideal $\mathfrak{m}$ which is prime to $12\,d$ and $N\mathfrak{m} \equiv 1 \bmod 4$.

THEOREM. *If* $N\mathfrak{m} \equiv 1$ *mod* 12, *a number* (11) *generate the ideal* $\mathfrak{m}$ *in* $\Omega(j\ (\alpha_1, \alpha_2))$, *and if* $N\mathfrak{m} \equiv 5$ *mod* 12, *the number* (12) *generate the ideal* $\mathfrak{m}$ *in* $\Omega(j\ (\alpha_1, \alpha_2))$.

In the case of III or IV, we may also construct a polynomial $G_2(t;\omega_1, \omega_2)$ or $G_6(t;\omega_1, \omega_2)$ as before. But, in these cases, we have only a generator of the ideal $\mathfrak{m}^2$ or $\mathfrak{m}^5$, and an analogous method is not applicable in these cases.

MATHEMATICAL INSTITUTE, TÔHOKU UNIVERSITY.