ON THE GAUSSIAN SUM AND THE JACOBI SUM WITH ITS APPLICATION.

AKIO YOKOYAMA

(Received January 20, 1964)

Let n be any rational integer > 2 and ζ_n a primitive n-th root of unity over the field P of rational numbers (e.g. $\zeta_n = e^{2\pi i/n}$) ; let $P_{(n)}$ denote the cyclotomic field generated by the primitive n-th root of unity ζ_n over the field of rational numbers. If t is any rational integer prime to n, $\zeta_n \to \zeta_n{}^t$ determines an automorphism σ_t of $P_{(n)}$ over P ; the Galois group of $P_{(n)}$ over P consists of all σ_t and therefore is isomorphic with the multiplicative group of the rational integers prime to n mod n.

Let $\mathfrak{p}$ be any prime ideal prime to n in $P_{(n)}$, and put $N\mathfrak{p} = q$; then $q \equiv 1$ (mod n). The n-th roots of unity ζ_n^a, for $0 \leqq a < n$, are all incongruent to each other mod $\mathfrak{p}$ and therefore are all the roots of the congruence $X^n \equiv 1$ (mod $\mathfrak{p}$) in $P_{(n)}$.‘For every integer x prime to $\mathfrak{p}$ in $P_{(n)}$, $x^{q-1} \equiv 1$ (mod $\mathfrak{p}$) and so there is one and only one n-th root of unity ζ_n^r $(0 \leqq r < n)$ satisfying the condition $x^{(q-1)/n} \equiv \zeta_n^r$ (mod $\mathfrak{p}$), since $x^{\frac{q-1}{n} \cdot n} \equiv 1$ (mod $\mathfrak{p}$).

Now, let $\chi_p(x)$ be an n-th root of unity satisfying

$$\chi_p(x) \equiv x^{(q-1)/n} \ (\text{mod } \mathfrak{p}),$$

and for $x \equiv 0$ (mod $\mathfrak{p}$) we put $\chi_p(x) = 0$. Then χ_p is a multiplicative character of order n of the field of q elements consisting of the congruence classes in $P_{(n)}$ mod $\mathfrak{p}$.

For such a character χ_p and any rational integers a and b such that a, b and $a + b \not\equiv 0$ mod n, Jacobi sum is defined as follows:

$$\omega(\chi^a_{.}, \chi^b_{.}) = -\sum_{x_1, x_2} \chi^a_{.}(x_1)\chi^b_{.}(x_2)$$

where x_1 and x_2 run over complete sets of representatives of the congruence classes modulo $\mathfrak{p}$ in $P_{(n)}$ subject to the condition $x_1 + x_2 \equiv 1$ mod $\mathfrak{p}$.

As Jacobi sums are closely related to the Gaussian sum we shall here deal with both Jacobi sums and the Gaussian sums. As can be seen in the above definition, Jacobi sums are certain sums of roots of unity in the residue class field modulo $\mathfrak{p}$. It will be shown that they are left invariant under all automorphisms of the residue class field modulo $\mathfrak{p}$. Jacobi sums may have some relation to the splitting field of $\mathfrak{p}$ with respect to $P_{(n)}/P$, and indeed they have. We shall prove that the splitting field of $\mathfrak{p}$ arises from the rational field by the adjunction of Jacobi sum. As for the Gaussian sum, S.Chowla [1]

[1] see [8]

shows that the Gaussian sum belonging to a character of the multiplicative group of rational integers modulo p, where p is an odd prime number, is equal to the product of a root of unity and$\sqrt{p}$ if and only if the order of the multiplicative character is two[1]. In case of the Gaussian sum belonging to the above multiplicative character $\chi^{a}_{\mathfrak{p}}$, it will be shown that it is equal to the product of a root of unity and $\sqrt{N\mathfrak{p}}$ or not, according as the splitting field of $\mathfrak{p}$ is real or imaginary.

D. Hilbert [6] shows a set of relations among the elements of the class group of the cyclotomic field generated by p-th roots of unity over the rational field, which R.E. MacKenzie [7] gives a generalization of. Here we shall prove that the above relations also hold in the class group of any Galois extension over P of finite degree containing $P_{(n)}$ and in a certain "Strahl" class group of any cyclotomic field $P_{(n)}$. The point of the proof which is founded on the ideas of MacKenzie consists in employing Jacobi sums.

1. Preliminaries. Let $\mathfrak{p}$ be any prime ideal prime to n in $P_{(n)}$ and $\psi(x)$ be any nontrivial character of the additive group of congruence classes modulo $\mathfrak{p}$ in $P_{(n)}$; consider the Gaussian sum

$$\tau(\chi^{a}_{\mathfrak{p}}) = -\sum_{x \bmod \mathfrak{p}} \chi^{a}_{\mathfrak{p}}(x)\,\psi(x)$$

for any integer a modulo n.
Then we get the relation between the Gaussian sum and Jacobi sum

$$\tau(\chi^{a}_{\mathfrak{p}})\tau(\chi^{b}_{\mathfrak{p}}) = \tau(\chi^{a+b}_{\mathfrak{p}})\omega(\chi^{a}_{\mathfrak{p}}, \chi^{b}_{\mathfrak{p}}) \tag{1}$$

when a, b and $a+b \not\equiv 0 \bmod n$.
And for any rational integer $C \not\equiv 0 \bmod n$

$$|\tau(\chi^{c}_{\mathfrak{p}})|^{2} = q. \tag{2}$$

From this and (1) we have for any rational integers a and b such that a, b and $a+b \not\equiv 0 \bmod n$

$$|\omega(\chi^{a}_{\mathfrak{p}}, \chi^{b}_{\mathfrak{p}})|^{2} = q\,. \tag{3}$$

Moreover, it follows that for any rational integer $a \not\equiv 0 \bmod n$

$$\prod_{\mu=1}^{n-1} \omega(\chi^{a\mu}_{\mathfrak{p}}, \chi^{a}_{\mathfrak{p}})\ (N\mathfrak{p})^{d} = \tau(\chi^{a}_{\mathfrak{p}})^{n} \tag{4}$$

where d denotes the positive greatest common divisor of a and n.[2]
On the other hand, n-th power of the Gaussian sum $\tau(\chi^{a}_{\mathfrak{p}})$ is an integer in $P_{(n)}$ whose prime ideal decomposition in $P_{(n)}$ is given by Stickelberger and Hasse [5], [9], [10] as follows; for $a \not\equiv 0 \bmod n$

$$(\tau(\chi^{a}_{\mathfrak{p}})^{n}) = \mathfrak{p}^{\theta(a)} \tag{5}$$

[2] In the case $\mu = \frac{n}{d} - 1$, $\omega(\chi^{a\mu}_{\mathfrak{p}}, \chi^{a}_{\mathfrak{p}})$ is equal to $\chi^{a}_{\mathfrak{p}}(-1)$.

where $\theta(a)$ denotes the sum $\sum_t r(-ta)\sigma_t^{-1}$; $r(x)$ denotes the least positive rest of x mod n and the summation is over all rational integers t prime to n modulo n. Thus $\theta(a)$ is an element of the group-ring (with integral coefficients) of the Galois group of $P_{(n)}$ over P; symbolic powers of ideals of $P_{(n)}$ 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

$$\theta(a)\sigma_t = \theta(ta) \tag{6. 1}$$

$$\theta(a)(\sigma_1 + \sigma_{-1}) = \theta(a) + \theta(-a) = n \sum_t \sigma_t \tag{6. 2}$$

where t is again prime to n.

Now, Jacobi sum $\omega(\chi_{\mathfrak{p}}^a, \chi_{\mathfrak{p}}^b)$ is an integer in $P_{(n)}$. From (1) and (4), the prime ideal decomposition of Jacobi sum in $P_{(n)}$ is obtained as follows: when a, b and $a + b \not\equiv 0 \bmod n$

$$(\omega(\chi_{\mathfrak{p}}^a, \chi_{\mathfrak{p}}^b)) = \mathfrak{p}^{\eta(a,b)}. \tag{7}$$

Here $\eta(a,b)$ denotes the sum $\sum_t d(-ta, -tb)\sigma_t^{-1}$, where generally

$$d(x_1, x_2) = \frac{r(x_1) + r(x_2) - r(x_1 + x_2)}{n} = \begin{cases} 0 \text{ for } r(x_1) + r(x_2) < n \\ 1 \text{ for } r(x_1) + r(x_2) \geqq n \end{cases}$$

and the sum is taken over all integers t prime to n modulo n.
Since the expression $d(x_1, x_2)$ is equal to 0 or 1 according as $r(x_1) + r(x_2) < n$ or $r(x_1) + r(x_2) \geqq n$, $\eta(a,b)$ is an element of the group-ring (with integral coefficients) of the Galois group of $P_{(n)}$ over P. And we see at once that $n\eta(a,b) = \theta(a) + \theta(b) - \theta(a+b)$ as elements of the group-ring, so we have

$$\eta(a,b)\sigma_t = \eta(ta, tb) \tag{8. 1}$$

$$\eta(a,b)(\sigma_1 + \sigma_{-1}) = \sum_t \sigma_t. \tag{8. 2}$$

Let p be the prime number which is divisible by $\mathfrak{p}$. Then the Gaussian sums $\tau(\chi_{\mathfrak{p}}^a)$ are integers in $P_{(np)}$, so any element of the Galois group of $P_{(n)}$ over P acts on them; for an automorphism ρ_s of $P_{(np)}/P_{(n)}$ which corresponds to the automorphism $\zeta_p \rightarrow \zeta_p^s$ of $P_{(np)}/P_{(n)}$ we have $\tau(\chi_{\mathfrak{p}}^a)^{\rho_s} = \chi_{\mathfrak{p}}^{-a}(s)\tau(\chi_{\mathfrak{p}}^a)$ and for an automorphism $\bar{\sigma}_t$ of $P_{(np)}/P_{(p)}$ which corresponds to the automorphism σ_t of $P_{(n)}/P$, we have also $\tau(\chi_{\mathfrak{p}}^a)^{\bar{\sigma}_t} = \tau(\chi_{\mathfrak{p}}^{at})$. On the other hand, any element of the Galois group of $P_{(n)}$ over P acts on n-th power of Gaussian sum and Jacobi sum $\omega(\chi_{\mathfrak{p}}^a, \chi_{\mathfrak{p}}^b)$, which are integers in $P_{(n)}$. Therefore we have the following;

$$\tau(\chi_{\mathfrak{p}}^a)^{n\sigma_t} = \tau(\chi_{\mathfrak{p}}^{at})^n \qquad \omega(\chi_{\mathfrak{p}}^a, \chi_{\mathfrak{p}}^b)^{\sigma_t} = \omega({}_{\mathfrak{p}}^{at}, \chi_{\mathfrak{p}}^{bt}) \tag{9}$$

for all elements σ_t of the Galois group of $P_{(n)}$ over P.

Now, let k be any finite algebraic number field over P containing $P_{(n)}$ and p be any prime number which does not divide the discriminant of k; let $\mathfrak{p}$ denote a prime divisor of p in $P_{(n)}$, and $\mathfrak{P}$ a prime divisor of $\mathfrak{p}$ in k.

For the character $\chi_{\mathfrak{p}}$ of the multiplicative group of congruence classes modulo $\mathfrak{p}$, the character $\chi_{\mathfrak{P}}$ of the multiplicative group of congruence classes modulo $\mathfrak{P}$ is defined by

$$(10) \qquad \chi_{\mathfrak{P}}(\bar{x}) = \chi_{.}(\overline{N x})$$

where $\bar{x}$ is any integer prime to $\mathfrak{P}$ in k and $\bar{N}$ denotes the norm mapping from the multiplicative group of congruence classes modulo $\mathfrak{P}$ to the multiplicative group of congruence classes modulo $\mathfrak{p}$.
Furthermore, let f be the relative degree of $\mathfrak{P}$ with respect to $k/P_{(n)}$, namely $N\mathfrak{P} = \mathfrak{p}^f$ then $\bar{N}\bar{x} = \bar{x}^{1+q+\dots+q^{f-1}} \equiv \bar{x}^{(q^f-1)/(q-1)}$ mod $\mathfrak{p}$. Therefore, by the definition, for any rational integer $a \not\equiv 0$ mod n $\chi_{\mathfrak{P}}^{a}(x) \equiv x^{(q^f-1)a/n}$ mod $\mathfrak{p}$ and so mod $\mathfrak{P}$. Hence we see that $\chi_{\mathfrak{P}}^{a}(\bar{x}) = \chi_{\mathfrak{p}}^{a}(\overline{N x})$ for any rational integer $a \not\equiv 0$ mod n.
For such characters $\chi_{\mathfrak{P}}^{a}$ and $\chi_{\mathfrak{P}}^{b}$ Jacobi sum $\omega(\chi_{\mathfrak{P}}^{a}, \chi_{\mathfrak{P}}^{b})$ and the Gaussian sum $\tau(\chi_{\mathfrak{P}}^{a})$ may be defined in the same way, then Hasse [2], [5] proved the following relation;

$$(11) \qquad \omega(\chi^{a}, \chi_{\mathfrak{P}}^{b}) = \omega(\chi_{\mathfrak{p}}^{a}, \chi_{\mathfrak{p}}^{b})^{f}.$$

2. Gaussian sums and Jacobi sums. Let $\mathfrak{p}$ be any prime ideal prime to n in $P_{(n)}$ and put $N\mathfrak{p} = p^{f'}$, where p is a rational prime number.

In the following, a prime ideal $\mathfrak{p}$ and rational prime number p mean what is mentioned above unless otherwise stated. We also omit the subscript $\mathfrak{p}$ in characters $\chi_{\mathfrak{p}}^{a}$, the Gaussian sums $\tau(\chi_{\mathfrak{p}}^{a})$ and Jacobi sums $\omega(\chi_{\mathfrak{p}}^{a}, \chi^{b})$.

We shall first deal with Jacobi sums. Using (7) and that the prime ideal $\mathfrak{p}$ is left invariant under the Frobenius substitution of p with respect to $P_{(n)}/P$, we see at once that the Frobenius substitution of p leaves fixed the principal ideal generated by Jacobi sum. However, we shall now show that Jacobi sum itself is left invariant under the Frobenius substitution of p. This follows from these consideration: using (9), for the Frobenius substitution φ of p with respect to $P_{(n)}/P$, characterized by $\zeta_n^{\varphi} = \zeta_n^{p}$, we have the following;

$$\begin{aligned}
\omega(\chi^{a}, \chi^{b})^{\varphi} &= \omega(\chi^{ap}, \chi^{bp}) = -\sum_{x_1+x_2\equiv 1 \bmod \mathfrak{p}} \chi^{ap}(x_1)\chi^{bp}(x_2) \\
&= -\sum_{x_1 \not\equiv 0, 1 \bmod \mathfrak{p}} \chi^{ap}(x_1)\chi^{bp}(1-x_1) = -\sum_{x_1 \not\equiv 0, 1} \chi^{a}(x_1{}^{p})\chi((1-x_1)^{p}) \\
&= -\sum_{x_1 \not\equiv 0, 1} \chi^{a}(x_1{}^{p})\chi^{b}(1-x_1{}^{p}).
\end{aligned}$$

Here, paying attention to the quality of the Frobenius substitution of p we have further

$$= -\sum_{x_1{}^p \neq 0, 1 \bmod \mathfrak{p}} \chi^a(x_1{}^p)\chi^b(1 - x_1{}^p) = -\sum_{x_1^p + x_2^p \equiv 1 \bmod \mathfrak{p}} \chi^a(x_1{}^p)\chi^b(x_2{}^p)$$

$$= \omega(\chi^a, \chi^b).$$

Hence Jacobi sum $\omega(\chi^a, \chi^b)$ is left invariant under any element of the splitting group of p with respect to $P_{(n)}/P$.

Conversely, assume $\omega(\chi^a, \chi^b) = \omega(\chi^a, \chi^b)^{\sigma_k}$ for some element σ_k of the Galois group of $P_{(n)}$ over P, then we have $(\omega(\chi^a. \chi^b)) = (\omega(\chi^a, \chi^b))^{\sigma_k}$. By (7) and (8. 1) we obtain the prime ideal decomposition of $(\omega(\chi^a, \chi^b))^{\sigma_k}$ in $P_{(n)}$ as follows:

$$(\omega(\chi^a, \chi^b))^{\sigma_k} = \mathfrak{p}^{\eta(ka, kb)}.$$

Here, let $\mathfrak{p}^{\sigma_{t_1}^{-1}}, \mathfrak{p}^{\sigma_{t_2}^{-1}}, \cdots \mathfrak{p}^{\sigma_{t_s}^{-1}}$, $(s = \varphi(n)/f')$[3] be different prime divisors of p. Then (7) may be written in the form

$$(12) \qquad (\omega(\chi_{\mathfrak{p}}^a, \chi_{\mathfrak{p}}^b)) = \mathfrak{p}^{\sum_{i=1}^{s} D(at_i, bt_i)\sigma_{t_i}^{-1}}$$

where $D(x_1, x_2)$ denotes the sum $\sum_{\mu=0}^{f'-1} d(-x_1 p^\mu, -x_2 p^\mu)$.

By (12) and the assumption, we get

$$(\omega(\chi^a, \chi^b))^{\sigma_k} = \mathfrak{p}^{\sum_{i=1}^{s} D(kat_i, kbt_i)\sigma_{t_i}^{-1}} = \mathfrak{p}^{\sum_{i=1}^{s} D(at_i, bt_i)\sigma_{t_i}^{-1}} = (\omega(\chi^a, \chi^b)).$$

This implies that each prime ideal $\mathfrak{p}^{\sigma_{t_i}^{-1}}$ in both sides of the above equation has the same exponent, that is, $D(kat_i, kbt_i) = D(at_i, bt_i)$ holds for each $i, i = 1, 2, \cdots, s$.

If there exists at least one $D(at_j, bt_j)$ different from the others, then we see immediately that the above equation holds only when k is the power of p ; namely σ_k is contained in the splitting group of p.

Thus we have the following

LEMMA 1. *Assume that there exists at least one $D(at_j, bt_j)$ different from the others. Then in order that some elements of the Galois group of $P_{(n)}$ over P leave Jacobi sum $\omega(\chi_{\mathfrak{p}}^a, \chi_{\mathfrak{p}}^b)$ fixed, it is necessary and sufficient that they are contained in the splitting group of p with respectct to $P_{(n)}/P$.*

According to Lemma 1, it may be possible that some of Jacobi sums are real numbers, and indeed they are. Then we have the following

[3] $\varphi(n)$ denotes Euler's function.

LEMMA 2. *If the splitting field of p with respect to $P_{(n)}/P$ is a real subfield of $P_{(n)}$, then Jacobi sum $\omega(\chi_{\mathfrak{p}}^{a}, \chi_{\mathfrak{p}}^{b})$ is equal to $\pm\sqrt{N\mathfrak{p}}$ which is a rational integer and conversely, if there exists at least one $D(at_j, bt_j)$ different from the rest.*

PROOF. In order that the splitting field of p is a subfield of the maximal real subfield of $P_{(n)}$, it is necessary and sufficient that the complex conjugation σ_{-1} of the imaginary field $P_{(n)}$ is contained in the splitting group of p.
Suppose that the splitting field of p is real, then we see at once that $\omega(\chi^a, \chi^b)^{\sigma_{-1}} = \omega(\chi^a, \chi^b)$ for the complex conjugation σ_{-1} from the first part of Lemma 1 and what is mentioned above. And we see further from (3) that $N\mathfrak{p} = \omega(\chi^a, \chi^b)\cdot\omega(\chi^a, \chi^b)^{\sigma_{-1}} = \omega(\chi^a, \chi^b)^2$. When we put $N\mathfrak{p} = p^{f'}$, by the assumption f' is an even integer. Therefore Jacobi sum is equal to $\pm\sqrt{N\mathfrak{p}}$ and a rational integer.
Conversely, suppose that there exists at least one $D(at_j, bt_j)$ different from the rest and Jacobi sum is equal to $\pm\sqrt{N\mathfrak{p}}$ which is not necessarily a rational integer, then it holds that $\omega(\chi^a, \chi^b)^{\sigma_{-1}} = \omega(\chi^a, \chi^b)$. This fact shows that the complex conjugation σ_{-1} is contained in the splitting group of p by the latter part of Lemma 1. Thus we obtain the assertion to be proved.

Now, paying attention to Lemma 2 we can express Lemma 1 in another way, that is the following

THEOREM 1. *Assume that the splitting field P_z of p with respect to $P_{(n)}/P$ is an imaginary subfield of $P_{(n)}$ and there exists at least one $D(at_j, bt_j)$ different from the others. Then we have $P_z = P(\omega(\chi_{\mathfrak{p}}^{a}, \chi_{\mathfrak{p}}^{b}))$.*

PROOF. We see immediately that $\omega(\chi^a, \chi^b)$ is not contained in P, but contained in P_z. Furthermore, Lemma 1 shows that the number of the different conjugates of the element $\omega(\chi^a, \chi^b)$ in P_z is equal to the degree of P_z over P and $P(\omega(\chi^a, \chi^b))$ is a normal extension over P. Hence our assertion is true.

Next, we shall deal with the Gaussian sums. As mentioned above, Jacobi sum is left invariant under any element of the splitting group of p with respect to $P_{(n)}/P$. From this and (4) it follows that any element of the splitting group of p leaves n-th power of the Gaussian sum fixed.
As before, let $\mathfrak{p}^{\sigma_{t_1}^{-1}}, \mathfrak{p}^{\sigma_{t_2}^{-1}}, \cdots, \mathfrak{p}^{\sigma_{t_s}^{-1}}$, $(s = \varphi(n)/f')$ be different prime divisors of p. Then (5) may be written in the form

$$(\tau(\chi_{\mathfrak{p}}^{a})^n) = \mathfrak{p}^{\sum_{i=1}^{s} R(t_i a)\sigma_{t_i}^{-1}} \tag{13}$$

where $R(x)$ denotes the sum $\sum_{\mu=0}^{f'-1} r(-xp^{\mu})$.

Now, assume $\tau(\chi^a)^n = \tau(\chi^a)^{n\sigma_k}$ for some element σ_k of the Galois group of $P_{(n)}$ over P. Then by (13) we get

$$(\tau(\chi^a)^n)^{\sigma_k} = \mathfrak{p}^{\sum_{i=1}^{s} R(t_i ka)\sigma_{t_i}^{-1}} = \mathfrak{p}^{\sum_{i=1}^{s} R(t_i a)\sigma_{t_i}^{-1}} = (\tau(\chi^a)^n).$$

This implies that $R(t_i a)$ is equal to $R(t_i ka)$ for each i, $i = 1, 2, \cdots s$. If there exists at least one $R(t_j a)$ different from the others, then we see immediately that the above equation holds only when σ_k is contained in the splitting group of p.

Thus we have the following

LEMMA 3. *If there exists at least one $R(t_j a)$ different from the rest, then n-th power of the Gaussian sum $\tau(\chi_{\mathfrak{p}}^a)$ is left invariant under some elements of the Galois group of $P_{(n)}$ over P only when they are contained in the splitting group of p.*

When $\chi_{\mathfrak{p}}^a$ is a multiplicative character of order 2 of the multiplicative group of congruence classes modulo $\mathfrak{p}$ in particular, it is a famous fact that the Gaussian sum $\tau(\chi_{\mathfrak{p}}^a)$ is equal to $\pm\sqrt{\chi_{\mathfrak{p}}^a(-1)\cdot N\mathfrak{p}}$. As to the Gaussian sum of multiplicative characters of oder n of the multiplicative group of congruence classes modulo $\mathfrak{p}$, we have the following

THEOREM 2. *We put the Gaussian sum $\tau(\chi^a) = \varepsilon(\chi^a)\cdot\sqrt{N\mathfrak{p}}$. If the splitting field of p with respect to $P_{(n)}/P$ is real, then in the case p is odd, $\varepsilon(\chi^a)$ is an n-th root or a 2n-th root of unity according as n is even or odd, and in the case p is 2, $\varepsilon(\chi^a)$ is an n-th root of unity and conversely if there is at least one $R(t_j a)$ different from the others. Then we have $\varepsilon(\chi^a)\varepsilon(\chi^b) = \pm\varepsilon$ (χ^{a+b}).*

This theorem is proved by the same methods as in the proof of Lemma 2.

Now, assume that the splitting field of p is imaginary and there is at least one $R(t_j a)$ different from the rest. Obviously $\varepsilon(\chi^a)$ is not a root of unity. Since $\tau(\chi^a)$ is equal to $\varepsilon(\chi^a)\sqrt{N\mathfrak{p}}$, $\varepsilon(\chi^a)^{2n}$ is contained in $P_{(n)}$; more explicitly, in the case n and f' is odd, where f' denotes the degree of $\mathfrak{p}$ relative to P, $\varepsilon(\chi^a)^{2n}$ is contained in $P_{(n)}$ and in other cases $\varepsilon(\chi^a)^n$ is contained in $P_{(n)}$. And its prime ideal decomposition in $P_{(n)}$ follows from (5) and (6.2);

$(\varepsilon(\chi^a)^{2n}) = \mathfrak{p}^{\sum_t (2r(-at)-n)\sigma_t^{-1}} = \mathfrak{p}^{\sum_{i=1}^{s=1} (2R(t_i a)-nf')\sigma_{t_i}^{-1}}$. As for the exponents of $\mathfrak{p}^{\sigma_{t_i}^{-1}}$, we have the relation $R(t_i a) + R((n - t_i)a) = nf'$ for each i, where i is an integer satisfying $1 \leqq i \leqq \frac{s}{2}$ or $\frac{s-1}{2}$ according as s is even or odd, respectively, because we may take $\{\sigma_{t_1}^{-1}, \sigma_{t_2}^{-1}, \cdots, \sigma_{n-t_2}^{-1}, \sigma_{n-t_1}^{-1}\}$ as a representative system of the right coset of the splitting group of p in the Galois group of $P_{(n)}$ over P and $r(-x) + r(x) = n$ holds. Therefore the sign of the rational integer $2R(t_ja) - nf'$ does not coincide with the sign of the rational integer $2R((n - t_j)a) - nf'$ by the assumption; this implies that $\mathcal{E}(\chi^a)^{2n}$ is not an integer but we have $|\mathcal{E}(\chi^a)| = 1$ easily. As the field $P_{(n)}$ is purely imaginary, there is no distinction to be made between the norms of the number $\mathcal{E}(\chi^a)^{2n}$ and of the principal ideal $(\mathcal{E}(\chi^a)^{2n})$. Therefore, by the above prime ideal decompostion we have $N_{P(n)/P}\,\mathcal{E}(\chi^a)^{2n}$.

Thus we have the following

COROLLARY 1. *Let notation $\mathcal{E}(\chi^a)$ be as in Theorem 2. Assume that the splitting field of p with respect to $P_{(n)}/P$ is imaginary and there exists at least one $R(t_ja)$ different from the others. Then $\mathcal{E}(\chi^a)$ is not an integer in $P_{(n)}$ but it is characterized by $|\mathcal{E}(\chi^a)| = 1$ and $N_{P(n)/P}\mathcal{E}(\chi^a)^{2n} = 1$*

Moreover we have

THEOREM 3. *Assume that the splitting field P_z of p with respect to $P_{(n)}/P$ is imaginary and there exists at least one $R(t_ja)$ different from the rest. Then we have $P_z = P(\tau(\chi_{\mathfrak{p}}^a)^n)$.*

This theorem can be proved in the same way as in the proof of Theorem 1.

3. An application of Jacobi sums. Let k be any finite algebraic number field over P containing $P_{(n)}$ and p be any rational prime number which does not divide the discriminant of k.
Let $\mathfrak{p}^{\sigma_{t_i}^{-1}}$ $(i = 1, 2, \cdots, s)$ denote the distinct prime divisors of p in $P_{(n)}$ as before and moreover, let $\mathfrak{p}^{\sigma_{t_i}^{-1}} = \mathfrak{P}_{i,1}\cdot\mathfrak{P}_{i,2}\cdots\mathfrak{P}_{i,r_i}$ be the prime ideal decomposition of $\mathfrak{p}^{\sigma_{t_i}^{-1}}$ in k, then for any rational integer a and b such that a, b and $a + b \not\equiv 0 \bmod n$, the prime ideal decomposition of Jacobi sum $\omega(\chi_{\mathfrak{p}}^a, \chi_{\mathfrak{p}}^b)$ in k is given by

$$(\omega(\chi_{\mathfrak{p}}^a, \chi_{\mathfrak{p}}^b)) = \prod_{i=1}^{s}\prod_{j=1}^{r_i} \mathfrak{P}_{i,j}^{D(t_ia, t_ib)} \tag{14}$$

Let $\mathfrak{K}_{i,j}$ denote the ideal class of k containing the prime ideal $\mathfrak{P}_{i,j}$ for each i, j $(i = 1, 2, \cdots, s, j = 1, 2, \cdots, r_i)$. Then it follows from (14) *that for any rational integer a and b such* that a,b *and* $a + b \not\equiv 0 \bmod n$

$$\prod_{i=1}^{s}\prod_{j=1}^{r_i} \mathfrak{K}_{i,j}^{D(t_ia, t_ib)} = 1$$

where $D(t_ia, t_ib)$ denotes the same notation as in (12).

Especially, assume that k is a Galois extension over P containing $P_{(n)}$. Let the Galois groups of $P_{(n)}/P$ and $k/P_{(n)}$ be denoted by $\mathfrak{G}$ and $\mathfrak{H}$, respectively. Then we denote by σ_t a representative in the Galois group of k/P of the coset corresponding to an element σ_t of $\mathfrak{G}$.

We now prove the following

THEOREM 4. *Assume that k is a Galois extension over P of finite degree containing $P_{(n)}$. Let $\mathfrak{K}$ be any ideal class of k. Then for any rational integers a and b except when $a \not\equiv 0$, $b \not\equiv 0$ and $a+b\equiv 0 \mod n$*

$$\prod_{\bar{\sigma}_t^{-1}} \prod_{\tau \in H} (\mathfrak{K}^{\bar{\sigma}_t^{-1}\tau})^{d(-ia,-ib)} = 1$$

where the product is over all automorphisms of k.

PROOF. The generalized theorem on arithmetic progressions assures us that every ideal class of k contains prime ideals of degree 1 relative to P. Let $\mathfrak{K}$ be any ideal class of k and $\mathfrak{P}$ be a prime ideal in k of degree 1 relative to P which is contained in $\mathfrak{K}$. Then for this ideal class we may state from (14) that $\prod_{\bar{\sigma}_t^{-1}} \prod_{\tau} (\mathfrak{K}^{(\bar{\sigma}_t^{-1}\tau})^{d'-ia,-ib)}$ is the principal class, provided that neither a nor b is divisible by n. On the other hand, in case that a or b or both are divisible by n, the value of Jacobi sums $\omega(\chi^a, \chi^b)$ are as follows:

$$\omega(\chi^a, \chi^b) = \begin{cases} -(N\mathfrak{p}-2) & \text{when } a\equiv 0 \mod n \text{ and } b\equiv 0 \mod n \\ 1 & \text{when } a\equiv 0 \mod n \text{ or } b\equiv 0 \mod n \\ \chi^a(-1) & \text{when } a+b\equiv 0 \;\; a\not\equiv 0 \text{ and } b\not\equiv 0 \mod n. \end{cases}$$

So, in these cases the exponents $d(-ia, -ib)$ of $\mathfrak{p}^{\sigma_t^{-1}}$ in the prime ideal decomposition of Jacobi sum in $P_{(n)}$ is all equal to zero except when $a+b\equiv 0$, $a\not\equiv 0$ and $b\not\equiv 0 \mod n$. Moreover, from what is mentioned above, the above statement regarding $\mathfrak{K}$ is true even if either a or b is divisible by n. Hence Theorem 4 is true.

REMARK: Put $k = P_{(n)}$ in this theorem, then we have Theorem 4 of MacKenzie [7].

Particularly, as to the cyclotomic fields we see that Theorem 4 is true even if $\mathfrak{K}$ is any absolute ideal class of a cyclotomic field (an absolute ideal class means an ideal class in the narrow sense). And what is more, we prove the following

THEOREM 5. *Let n be any rational integer* > 2, $\mathfrak{p}$ *be any prime ideal prime to n in* $P_{(n)}$ *and* $\mathfrak{m}$ *be an ideal of* $P_{(n)}$ *such that* $\omega(\chi_{\mathfrak{p}}^{a}, \chi_{\mathfrak{p}}^{b})-1$ *or* $\omega(\chi_{\mathfrak{p}}^{a}, \chi_{\mathfrak{p}}^{b})+1$ *is divisible by* $\mathfrak{m}$. *Let* $\mathfrak{K}$ *be the "Strahl" class* mod $\mathfrak{m}$ *of* $P_{(n)}$ *containing* $\mathfrak{p}$. *Then we have for any rational integer a and b such that* $a + b \not\equiv 0$ mod n

$$\prod_{i=1}^{s} (\mathfrak{K}^{\sigma_{t_i}^{-1}})^{D(at_i, bt_i)} = 1$$

where $D(at_i, bt_i)$ *denotes the same notation as in* (12).

PROOF. By the assumption we see at once that "Strahl" class mod $\mathfrak{m}$ containing the principal ideal generated by Jacobi sum $\omega(\chi^a, \chi^b)$ is the "Strahl" mod $\mathfrak{m}$. So it follows from (14) that our assertion is true.

Furthermore, we have the following

THEOREM 6. *Assume that* $n = \prod_{i=1}^{\nu} l_i^{\nu_i}$ *is the factorization of n into powers of distinct primes and* $\mathfrak{l}_i$ *is a prime divisor of* l_i *in* $P_{(n)}$. *Let* $\mathfrak{K}$ *be any "Strahl" class* mod $\mathfrak{l}_i^{2c}(1 \leqq c \leqq l_i^{\nu_i-\mu}$ *and* $1 \leqq \mu \leqq \nu_i$ *or* $2 \leqq \mu \leqq \nu_i$ *according as* l_i *is odd prime or even).*

Then for any rational integer a and b except when $a \not\equiv 0$, $b \not\equiv 0$ *and* $a+b \equiv 0$ mod n *we have*

$$\prod_{\sigma_t^{-1} \in \mathfrak{G}} (\mathfrak{K}^{\sigma_t^{-1}})^{d(-s_\mu a, -s_\mu tb)} = 1$$

where s_μ *denotes the rational integer such that* $n = l_i^{\mu} s_\mu$ *and* $d(-s_\mu ta, -s_\mu tb)$ *denotes the same notation as in* (7).

PROOF, Since $\sum_{x \not\equiv 0, 1 \bmod \mathfrak{p}} \chi^{as_\mu}(x) = -1$ holds trivially Jacobi sum can be also written as follows: for any rational integer a,b and $a + b \not\equiv 0$ mod n

$$\omega(\chi^{as_\mu}, \chi^{bs_\mu}) = -\sum_{x_1+x_2 \equiv 1 \bmod \mathfrak{p}} \chi^{as_\mu}(x_1)\chi^{bs_\mu}(x_2) = -\sum_{x \not\equiv 0, 1 \bmod \mathfrak{p}} \chi^{as_\mu}(x_1)\chi^{bs_\mu}(1 - x_1)$$

$$= 1 - \sum_{x \not\equiv 0,1} \chi^{as_\mu}(x_1)(\chi^{bs_\mu}(1-x_1)-1).$$

Let $\overline{\mathfrak{l}}_{i,\mu}$ be the prime divisor of l_i in $P_{(l_i^\mu)}$. Then we have $\overline{\mathfrak{l}}_{i,\mu} = (\mathfrak{l}_i \cdots)^{l_i^{\nu_i - \mu}}$. By the assumption multiplicative characters $\chi^{as_\mu}{}_{(x_1)}$ and $\chi^{bs_\mu}\ (1-x_1)$ are at most l_i^μ-th roots of unity, hence $\chi^{as_\mu}(x_1)$ and $\chi^{bs_\mu}(1-x_1) \equiv 1 \bmod \overline{\mathfrak{l}}_{i,\mu}$ and so mod $\mathfrak{l}_i^c$. From this the congruence follows

$$\chi^{as_\mu}(x_1)\ (\chi^{bs_\mu}(1-x_1)-1) \equiv \chi^{bs_\mu}(1-x_1) - 1 \bmod \mathfrak{l}_i^{2c}, \text{ when } x_1 \not\equiv 0,\ 1 \bmod \mathfrak{p}$$

and consequently

$$\omega(\chi^{as_\mu}, \chi^{bs_\mu}) \equiv 1 - \sum_{x_1 \not\equiv 0,1} (\chi^{bs_\mu}(1-x_1) - 1) \equiv N\mathfrak{p} \equiv 1 \bmod n \text{ and so mod } \mathfrak{l}_i^{2c}.$$

In other cases, the last congruence trivially holds. Therefore we see that the "Strahl"class mod $\mathfrak{l}_i^{2c}$ containing the principal ideal generated by Jacobi sum is the "Strahl" mod $\mathfrak{l}_i^{2c}$. The generalized theorem on arithmetic progressions assures us that every "Strahl" class mod $\mathfrak{l}_i^{2c}$ of $P_{(n)}$ contains prime ideals of degree 1 relative to P. So, putting the "Strahl" class mod $\mathfrak{l}_i^{2c}$ in the place of the ideal class in Theorem 4 the remaining part can be proved in the same way as in the proof of Theorem 4.

This theorem can be expressed in another way as follows:

THEOREM 6'. *The assumptions being the same as in Theorem* 6, *let* $\mathfrak{K}$ *be any "Stahl" class* mod $\mathfrak{l}_i^{2c}$ *of* $P_{(n)}$ *and* $\mathfrak{H}$ *denotes the Galois group of* $P_{(n)}$ *over the cyclotomic field* $P_{(l_i^\mu)}$ *generated by the primitive* l_i^μ*-th root of unity over the rational field. Then for any rational integer* a *and* b *except when* $a, b \not\equiv 0$ *and* $a + b \equiv 0$ mod n *we have*

$$\prod_{\sigma_t^{-1}} \prod_{\tau \in H} (\mathfrak{K}^{\sigma_t^{-1}\tau})^{d^{(l_i^\mu)}(-ta,-tb)} = 1$$

where $d^{(l_i^\mu)}(-ta, -tb) = \dfrac{r(-ta + r(-tb) - r(-ta, -tb)}{l_i^\mu}$ *and* σ_t^{-1} *ranges over all elements of a representative system of the factor group of the Galois group of* $P_{(n)}/P$ *by the Galois group of* $P_{(n)}/P_{(l_i^\mu)}$.

PROOF. Assume that $\mathfrak{p}$ is a prime ideal in $P_{(n)}$ of degree 1 relative to P and $\mathfrak{q}$ is the prime ideal in $P_{(l_i^\mu)}$ which is divisible by $\mathfrak{p}$, then the prime ideal decomposition of Jacobi sum $\omega(\chi_p^b, \chi_q^b)$ in $P_{(n)}$ is as follows:

$$(\omega(\chi_q^a, \chi_q^b)) = \mathfrak{p}^{\sum_{\sigma_t^{-1}} \sum_{\tau} d^{(l_i^\mu)}(-ta,-tb)\sigma_t^{-1}\tau} \cdot$$

Here, σ_t^{-1} ranges over all elements of a representative system of the factor group of the Galois group of $P_{(n)}/P$ by the Galois group of $P_{(n)}/P^{(l_i^\mu)}$ and τ ranges over all elements of the Galois group $\mathfrak{H}$ of $P_{(n)}/P^{(l_i^\mu)}$. On the other hand, we have seen that $\omega(\chi_{\mathfrak{q}}^a, \chi_{\mathfrak{q}}^b) \equiv 1 \bmod \mathfrak{l}_i^{2c}$, except when $a \not\equiv 0$, $b \not\equiv 0$ and $a + b \equiv 0 \bmod n$. Therefore let $\mathfrak{K}$ be the "Strahl" class mod $\mathfrak{l}_i^{2c}$ containing $\mathfrak{p}$, we see at once that

$$\prod_{\sigma_t^{-1}} \prod_{\tau} (\mathfrak{K}^{\sigma_t^{-1}\tau})^{d^{(l_i^\mu)}(-ta,\,-tb)} = 1.$$

Hence Theorem 6′ is true for the case when $\mathfrak{K}$ is the "Strahl" class mod $\mathfrak{l}_i^{2c}$ containing $\mathfrak{p}$. As any "Strahl" class mod $\mathfrak{l}_i^{2c}$ surely contains the prime ideal of degree 1 relative to P, the above statement regarding $\mathfrak{K}$ is true for any "Strahl" class mod $\mathfrak{l}_i^{2c}$. Hence our assertion is true.

REFERENCES

[1] S. CHOWLA, On Gaussian sums, Proc. of National Academy of Science, 48(1962), 1127-1128.

[2] H. DAVENPORT-H. HASSE, Die Nullstellen der Kongruenzzetafunktion in gewissen zyklischen Fällen. Journ. r. a. Math., 172(1934), 151-182.

[3] H. HASSE, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, I, Ia, II, Jahresber. der Deutsch. Math. Ver., 35(1926).

[4] H. HASSE, Vorlesungen über Zahlentheorie, Berlin, 1950.

[5] H. HASSE, Zetafunktionen und L-Funktionen zu einem arithmetischen Funktionenenkörper vom Fermatschen Typus, Abh. Deutsch. Akad. Wiss. Berlin, Kl. Math. Nat., 1954 Heft 4(1955).

[6] D. HILBERT, Die Theorie der algebraischen Zahlkörper, Jahresber. der Deutsch. Math. Ver., 4(1897), 175-546.

[7] R. E. MACKENZIE, Class group relations in cyclotomic fields, Amer. Journ. of Math., 74(1952), 759-763.

[8] L. T. MORDELL, On a cyclotomic resolvent, Arch. der Math., 13(1962).

[9] L. STICKELBERGER, Über eine Verallgemeinerung des Kreisteilungs, Math. Ann., 37 (1890), 321-367.

[10] A. WEIL, On Jacobi sums as "Grössencharaktere", Trans. Amer. Math. Soc., 73 (1952), 487-495.

DEPARTMENT OF MATHEMATICS
SHIZUOKA UNIVERSITY.