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 $q\equiv 1 \pmod{n}$. 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 $X^n\equiv 1 \pmod{\mathfrak{p}}$ in $P_{(n)}$.'For every integer x prime to $\mathfrak{p}$ in $P_{(n)}$, $x^{q-1}\equiv 1 \pmod{\mathfrak{p}}$ and so there is one and only one n-th root of unity ζ_n^r $(0\leqq r<n)$ satisfying the condition $x^{(q-1)/n}\equiv \zeta_n^r \pmod{\mathfrak{p}}$, since $x^{\frac{q-1}{n}\cdot n}\equiv 1 \pmod{\mathfrak{p}}$.

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

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

and for $x\equiv 0 \pmod{\mathfrak{p}}$ 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 $a+b \not\equiv 0 \bmod n$, 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 $x_1+x_2\equiv 1 \bmod \mathfrak{p}$.

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]