PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 45, Number 2, August 1974

THE NONVANISHING OF CERTAIN CHARACTER SUMS

S. ULLOM [1]

ABSTRACT. Let χ be a Dirichlet character with conductor f and $M(\chi) = \Sigma\, a\overline{\chi}(a)$, summation over integers a prime to f and $1 \leq a < f$. It is well known that the nonvanishing of the Dirichlet L-function $L(s, \chi)$ at $s = 1$ implies $M(\chi) \neq 0$ for χ imaginary, i.e. $\chi(-1) = -1$. This article provides a purely algebraic proof that $M(\chi) \neq 0$ when the conductor f is a prime power and the imaginary χ is either a faithful character or has order a power of 2.

1. **Introduction.** Let χ be a Dirichlet character with conductor f. If χ is imaginary, that is $\chi(-1) = -1$, then the character sum $M(\chi) \neq 0$, where $M(\chi) = \Sigma_a\, a\overline{\chi}(a)$, summation over integers a prime to f and $1 \leq a < f$. In fact one knows [1, §4] that the Dirichlet L-function $L(s, \chi)$ at $s = 1$ is

$$L(1, \chi) = f^{-2}\pi i \tau(\chi) M(\chi), \qquad \tau(\chi) \text{ a Gauss sum,}$$

and $L(1, \chi) \neq 0$.

The problem is to find an elementary proof that $M(\chi) \neq 0$. Hasse [1, §§31–32] obtained congruence properties of $M(\chi)$ which imply $M(\chi) \neq 0$ when the conductor f is a prime power and χ is either a faithful character or has order a power of 2. The purpose of this article is to give another algebraic proof of this result. The calculations of our method take place in a certain integral group ring and involve elements α_ϕ which are essentially idempotents in the rational group ring. There is still no algebraic proof that $M(\chi) \neq 0$ for all imaginary χ.

2. **Preliminaries.** In this article we fix f, $K = Q(\sqrt[f]{1})$, and the Galois group $G = G(K/Q)$. The group G is isomorphic to $(Z/fZ)^\times$ by $s_a \longrightarrow a \bmod f$,

Received by the editors September 7, 1973.

AMS (MOS) subject classifications (1970). Primary 10G05, 12A35; Secondary 16A26, 12A50.

Key words and phrases. Character sum, cyclotomic field, class number, integral group ring.

[1] This research was partially supported by a contract with the National Science Foundation.

$(a, f) = 1$; here $s_a \in G$ raises an fth root of 1 to its ath power. The semisimple Q-algebra QG is isomorphic to a direct sum ΣF_ϕ of cyclotomic fields F_ϕ, which correspond to the irreducible rational characters (in the sense of representation theory) of QG. Each homomorphism χ: $G \to C^\times$, C complex numbers, determines a rational character ϕ as follows. Let $Q(\chi)$ be the field of values of χ, then $\phi(s) = \Sigma_\gamma \gamma(\chi(s))$, $s \in G$, summation over $\gamma \in G(Q(\chi)/Q)$; the field $F_\phi = Q(\chi)$. Denote by e_ϕ the primitive idempotent of QG

$$e_\phi = \frac{1}{|G|} \sum_{s \in G} \phi(s^{-1})s.$$

Then χ extended to QG defines an isomorphism χ: $QGe_\phi \to F_\phi$. Define the subgroup G_ϕ of G by $G_\phi = \{s \in G: \chi(s) = 1\} = \{s \in G: \phi(s) = \phi(1)\}$. Choose $s_\phi \in G$ generating the group G/G_ϕ of order say g; then $\chi(s_\phi)$ is a primitive gth root of 1.

Let $\omega = \Sigma_a a s_a^{-1}$, $(a, f) = 1$, $1 \leq a < f$. Then $\chi(\omega) = M(\chi)$. Thus $M(\chi) \neq 0$ for all imaginary characters χ of G iff ωe^- $(e^- = \frac{1}{2}(1 - s_{-1}))$ is not a zero divisor of QGe^-.

3. **Group ring elements** α_ϕ. For each irreducible rational character ϕ of G define the nonzero element α_ϕ of ZG by

$$\alpha_\phi = \sigma(\phi) \prod_q (1 - s_\phi^{g/q}).$$

Here $\sigma(\phi)$ is the sum of the elements of G_ϕ and the product is taken over all primes q dividing g.

(3.1) **Lemma.** *Let ϕ and ψ be irreducible rational characters of QG. The product of α_ϕ with e_ψ is*

$$\alpha_\phi e_\psi = |G_\phi| \prod_q (e_\phi - (s_\phi e_\phi)^{g/q}) \quad \text{if } \phi = \psi,$$
$$= 0 \qquad \text{if } \phi \neq \psi.$$

Thus, if the complex character χ determines ϕ, $M(\chi) = 0$ iff $\omega e_\phi = 0$ iff $\omega \alpha_\phi = 0$.

Proof. Suppose $G_\phi \subset G_\psi$. Since $t \in G_\psi$ implies $te_\psi = e_\psi$, we have

$$\alpha_\phi e_\psi = |G_\phi| \prod_q (e_\psi - (s_\phi e_\psi)^{g/q}).$$

If $G_\phi = G_\psi$ (so $\phi = \psi$), we obtain the desired result. If G_ϕ is a proper subgroup of G_ψ, there exists a prime q dividing g such that $s_\phi^{g/q} \in G_\psi$. For such q, the factor $e_\psi - (s_\phi e_\psi)^{g/q} = 0$.

On the other hand, suppose G_ϕ is not contained in G_ψ. Then the order of $G_\phi/G_\phi \cap G_\psi$ is $h > 1$. Choose $t \in G_\phi$ generating $G_\phi/G_\phi \cap G_\psi$. Since $h > 1$, $\Sigma_{i=1}^{h} t^i e_\psi = 0$ and then $\sigma(\phi)e_\psi = 0$. Thus $\alpha_\phi e_\psi = 0$ if $\phi \neq \psi$. The last assertion of (3.1) is now clear.

(3.2) **Proposition.** *Suppose $f = p^r$, p prime. If χ is a nontrivial faithful character (i.e. $G_\phi = 1$) of $(Z/fZ)^\times$, then $M(\chi) \neq 0$.*

Proof. Define a ring homomorphism c: $ZG \longrightarrow Z/fZ$ by $c(\Sigma\, n_a s_a) = \Sigma\, n_a a \bmod fZ$, $n_a \in Z$, $s_a \in G$. For any integer a prime to f, one has $(s_a - a)\omega \in f \cdot ZG$. Therefore $\omega\alpha_\phi \equiv \omega c(\alpha_\phi) \bmod f \cdot ZG$. Now $c(\alpha_\phi) \equiv \Pi_q\, (1 - b^{g/q}) \bmod fZ$, where $s_b = s_\phi$ and $g = (p-1)p^{r-1}$. The factor $1 - b^{g/q}$ is prime to p for $q \neq p$, and p^{r-1} is the exact power of p dividing $1 - b^{g/q}$ when $q = p$. Thus $\omega\alpha_\phi \not\equiv 0 \bmod f \cdot ZG$, so $\omega\alpha_\phi \neq 0$; finally $M(\chi) \neq 0$ by (3.1).

(3.3) **Proposition.** *If $f = p^r$ and χ is an imaginary character with conductor f and order a power of 2, then $M(\chi) \neq 0$.*

Proof. Since the order g of χ is a power of 2, $\alpha_\phi = 2e^-\sigma(\phi)$. Then $\alpha_\phi\omega = 0$ iff

(3.4) $$s_{-1}\sigma(\phi)\omega = \sigma(\phi)\omega.$$

Let θ: $ZG \longrightarrow Z[G/G_\phi]$ be the canonical projection and suppose γ is a generator of G/G_ϕ. Set $\theta(\omega) = \Sigma_{i=1}^{g}\, n(i)\gamma^i$. If (3.4) holds, then $n(i) = n(i^*)$ where i^* is defined by $\gamma^{i^*} = s_{-1}\gamma^i$. Note $i^* \neq i$. Since $n(i) + n(i^*) = f|G_\phi|$,

(3.5) $$2n(i) = f|G_\phi|, \qquad i = 1, \cdots, g.$$

If p is odd, then G_ϕ has odd order (conductor of χ is f) and (3.5) is impossible. Suppose $f = 2^r$. We take $r \geq 3$; if $f = 4$, (3.5) clearly is false. Now $G_\phi = \{s_1, s_{-1}s_5^{2^{r-3}}\}$. Thus $n(g) = 1 + (-1)5^{2^{r-3}}$ which is not 2^r as required by (3.5). Hence $\alpha_\phi\omega \neq 0$.

REFERENCE

1. H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Akademie-Verlag, Berlin, 1952. MR 14, 141.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS, URBANA, ILLINOIS 61801