THE NONVANISHING OF CERTAIN CHARACTER SUMS

S. ULLOM

ABSTRACT. Let \( \chi \) be a Dirichlet character with conductor \( f \) and \( M(\chi) = \sum a \overline{\chi}(a) \), 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 \( \chi \) 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 \( \chi \) is either a faithful character or has order a power of 2.

1. Introduction. Let \( \chi \) be a Dirichlet character with conductor \( f \). If \( \chi \) is imaginary, that is \( \chi(-1) = -1 \), then the character sum \( M(\chi) \neq 0 \), where \( M(\chi) = \sum a \overline{\chi}(a) \), 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

\[
L(1, \chi) = f^{-2} \pi i r(\chi) M(\chi), \quad r(\chi) \text{ a Gauss sum,}
\]

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 \( \chi \) 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 \( a \phi \) which are essentially idempotents in the rational group ring. There is still no algebraic proof that \( M(\chi) \neq 0 \) for all imaginary \( \chi \).

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

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 \( f \)th root of 1 to its \( a \)th power. The semi-simple \( Q \)-algebra \( QG \) is isomorphic to a direct sum \( \sum F_\phi \) of cyclotomic fields \( F_\phi \), which correspond to the irreducible rational characters (in the sense of representation theory) of \( QG \). Each homomorphism \( \chi: G \to \mathbb{C}^\times \), \( C \) complex numbers, determines a rational character \( \phi \) as follows. Let \( Q(\chi) \) be the field of values of \( \chi \), then \( \phi(s) = \sum \gamma(\chi(s)), s \in G \), summation over \( \gamma \in G(\chi) / Q \); the field \( F_\phi = Q(\chi) \). Denote by \( e_\phi \) the primitive idempotent of \( QG \)

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

Then \( \chi \) extended to \( QG \) defines an isomorphism \( \chi: QGe_\phi \to F_\phi \). Define the subgroup \( G_\phi \) 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 \( G/G_\phi \) of order say \( g \); then \( \chi(s_\phi) \) is a primitive \( g \)th root of 1.

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

3. Group ring elements \( \alpha_\phi \). For each irreducible rational character \( \phi \) of \( G \) define the nonzero element \( \alpha_\phi \) of \( ZG \) by

\[
\alpha_\phi = \sigma(\phi) \prod_q (1 - s_\phi^g / q).
\]

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

(3.1) Lemma. Let \( \phi \) and \( \psi \) be irreducible rational characters of \( QG \). The product of \( \alpha_\phi \) with \( e_\psi \) is

\[
\alpha_\phi e_\psi = |G_\phi| \prod_q (e_\phi - (s_\phi e_\phi)^g / q) \quad \text{if} \quad \phi = \psi,
\]

\[
= 0 \quad \text{if} \quad \phi \neq \psi.
\]

Thus, if the complex character \( \chi \) determines \( \phi \), \( M(\chi) = 0 \) 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 \( G_\phi \) is a proper subgroup of \( G_\psi \), 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 $G_\phi$ is not contained in $G_\psi$. Then the order of $G_\phi/G_\psi \cap G_\psi$ is $h > 1$. Choose $t \in G_\phi$ generating $G_\phi/G_\psi \cap G_\psi$. Since $h > 1$, $\sum_{i=1}^h t^i e_\psi = 0$ 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 $\chi$ is a nontrivial faithful character (i.e. $G_\phi = 1$) of $(Z/fZ)^\chi$, then $M(\chi) \neq 0$.

Proof. Define a ring homomorphism $c: ZG \to Z/fZ$ by $c(\sum a_\phi s_\phi) = \sum a_\phi s_\phi \mod fZ$, $a_\phi \in Z$, $s_\phi \in G$. For any integer $a$ prime to $f$, one has $(s_\phi - a)\omega \in f \cdot ZG$. Therefore $\omega \alpha_\phi \equiv \omega(\alpha_\phi) \mod f \cdot ZG$. Now $c(\alpha_\phi) = \Pi_q (1 - b^g/q) \mod fZ$, 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 $\omega \alpha_\phi \equiv 0 \mod f \cdot ZG$, so $\omega \alpha_\phi \neq 0$; finally $M(\chi) \neq 0$ by (3.1).

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

Proof. Since the order $g$ of $\chi$ is a power of 2, $\alpha_\phi = 2e^{-\sigma(\phi)}$. Then

$$\alpha_\phi \omega = 0 \iff s_{-1} \sigma(\phi) \omega = \sigma(\phi) \omega.$$  \hspace{1cm} (3.4)

Let $\theta: ZG \to Z[G_\phi]$, be the canonical projection and suppose $\gamma$ is a generator of $G/G_\phi$. Set $\theta(\omega) = \sum_{i=1}^g n(i)\gamma^i$. 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 $n(i) + n(i^*) = |G_\phi|$,  

$$2n(i) = |G_\phi|, \quad i = 1, \ldots, g.$$  \hspace{1cm} (3.5)

If $p$ is odd, then $G_\phi$ has odd order (conductor of $\chi$ 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


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