Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 36 (1990)

Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: GAUSS SUMS AND THEIR PRIME FACTORIZATION

Autor: Brinkhuis, Jan

Kapitel: 6. Annihilators of the ideal class group of a cyclotomic field

DOI: https://doi.org/10.5169/seals-57901

On the other hand,

$$z = (\zeta_p - 1)^{\sigma_g - 1} = \sum_{i=0}^{g-1} \zeta_p^i$$

which is congruent to g mod $\mathfrak{P}$ and so $(0, z^k) = (0, \bar{g}^{k_i})$. Therefore the equality $l(\rho(\alpha)) = (0, z^k)$ amounts here to the following congruence

$$g^{\frac{p-1}{m}i} \equiv g^{k_i} \mod p$$

that is, by the choice of g,

$$k_i \equiv \frac{p-1}{m} i \mod p - 1 .$$

Thus k_i has been determined modulo $p - 1$. In fact one may replace in (5.4) the congruence sign by the equality sign as on the one hand clearly $0 < \frac{p-1}{m} i < p - 1$ and on the other hand by proposition (1.2) (iii) and (iv) one has $0 \leqslant k_i \leqslant v_{\mathfrak{P}}(p) = p - 1$. Therefore one gets

$$k_i = \frac{p-1}{m} i ,$$

This finishes the proof of the theorem.

6. Annihilators of the ideal class group of a cyclotomic field

In this section we give an account of the annihilation of the ideal class group of a cyclotomic field by the Stickelberger ideal. For each commutative ring R with unit element, each R-module M and each $\lambda \in R$, one says that λ annihilates M or that λ is an annihilator of M if $\lambda r = 0$ for all $r \in M$; the set $\mathrm{Ann}_R M$ of all annihilators of an R-module M clearly forms an ideal in the ring R.

Let $m > 1$. The structure of $Cl_{\mathbf{Q}(m)}$, the ideal class group of the cyclotomic field $\mathbf{Q}(m)$, and the action of the Galois group $\Gamma = \mathrm{Gal}\left(\mathbf{Q}(m)/\mathbf{Q}\right)$ on it, are of great interest. Information on this structure is contained in $\mathrm{Ann}_{\mathbf{Z}\Gamma} Cl_{\mathbf{Q}(m)}$.

It is difficult to analyse this ideal directly. However, what one can do is to relate this ideal to the annihilator of another $\mathbf{Z}\Gamma$-module, namely $\mu_m(\bar{\mathbf{Q}})$. Let $I = \mathrm{Ann}_{\mathbf{Z}\Gamma}\mu_m(\bar{\mathbf{Q}})$, $J = \mathrm{Ann}_{\mathbf{Z}\Gamma}Cl_{\mathbf{Q}(m)}$ and let $\theta \in \mathbf{Q}\Gamma$ be the Stickelberger element defined in (3.2). The main aim of this section is to derive from the prime factorization of the Gauss sums as given by theorem (3.3) the fact that multiplication in $\mathbf{Q}\Gamma$ by θ sends I into J, that is $\theta I \subseteq J$. The ideal θI in $\mathbf{Z}\Gamma$ is called the Stickelberger ideal. This result shows that a part of J can be obtained from I. Now I is the annihilator of a module with a rather transparent structure and so it can easily be determined completely in a direct way. Thus one achieves, all in all, the desired objective: one gets information on the $\mathbf{Z}\Gamma$-module $Cl_{\mathbf{Q}(m)}$. This section consists of two parts, which can be read independently, the determination of I and the proof of the inclusion $\theta I \subseteq J$.

We start by determining the ideal $I = \mathrm{Ann}_{\mathbf{Z}\Gamma}\mu_m(\bar{\mathbf{Q}})$. For each $x \in (\mathbf{Z}/m\mathbf{Z})^*$ we write $<x>$ for the smallest non-negative representative of x in $\mathbf{Z}$. We define the set of elements $\{\beta_x\}_x$ in $\mathbf{Z}\Gamma$ where x runs over $(\mathbf{Z}/m\mathbf{Z})^*$ by

(6.1)
$$\begin{aligned} \beta_x &= 1 && \text{if } x = 1 \\ &= \sigma_x - <x> && \text{otherwise}. \end{aligned}$$

This set is clearly a $\mathbf{Z}$-basis of $\mathbf{Z}\Gamma$, that is, every element $\lambda \in \mathbf{Z}\Gamma$ can be written uniquely as

(6.2)
$$\lambda = \textstyle\sum_x a_x\beta_x$$

where x runs over $(\mathbf{Z}/m\mathbf{Z})^*$ and with $a_x \in \mathbf{Z}$ for all $x \in (\mathbf{Z}/m\mathbf{Z})^*$.

(6.3) PROPOSITION. *Let* $\lambda \in \mathbf{Z}\Gamma$; *write* λ *as in (6.2). The following conditions on* λ *are equivalent:*

(i) λ annihilates $\mu_m(\bar{\mathbf{Q}})$.

(ii) $a_1 \equiv 0 \bmod m$.

(iii) $\lambda\theta \in \mathbf{Z}\Gamma$.

Proof. (i) $\Leftrightarrow$ (ii). Let ζ be a generator of the group $\mu_m(\bar{\mathbf{Q}})$. For each $x \in (\mathbf{Z}/m\mathbf{Z})^*$ one has clearly

$$\begin{aligned} \zeta^{\beta_x} &= \zeta && \text{if } x = 1 \\ &= 1 && \text{otherwise}. \end{aligned}$$

Therefore $\zeta^\lambda = \zeta^{a_1}$. As ζ has order m, it follows that (i) and (ii) are equivalent.

(ii) $\Leftrightarrow$ (iii). We are going to compute the product in $\mathbf{Q}\Gamma$ of β_x and θ for all $x \in (\mathbf{Z}/m\mathbf{Z})^*$, in order to verify the following facts

$$(6.4) \qquad \begin{aligned} \beta_x\theta &= \theta && \text{if } x = 1 \\ &\in \mathbf{Z}\Gamma && \text{otherwise}. \end{aligned}$$

Proof of (6.4). Let $x \in (\mathbf{Z}/m\mathbf{Z})^*$; if $x = 1$ the statement in (6.4) is obvious, so assume $x \neq 1$.

$$\beta_x\theta = (\sigma_x - <x>) \sum_i \frac{<i>}{m} \sigma_i^{-1}$$

where i runs over $(\mathbf{Z}/m\mathbf{Z})^*$. This is

$$\sum_i \frac{<i>}{m} \sigma_{x^{-1}i}^{-1} - \sum_i \frac{<x> \ <i>}{m} \sigma_i^{-1},$$

replacing in the first sum i by ix we get

$$\sum_i \frac{<ix>}{m} \sigma_i^{-1} - \sum_i \frac{<x> \ <i>}{m} \sigma_i^{-1} = \sum_i \frac{<ix> \ - \ <i> \ <x>}{m} \sigma_i^{-1};$$

in particular $\beta_x\theta \in \mathbf{Z}\Gamma$. This finishes the verification of (6.4) □.

It follows from (6.4), using moreover (6.2) and the definition (3.2) of θ that for each $i \in (\mathbf{Z}/m\mathbf{Z})^*$ the coefficient of σ_i in $\lambda\theta$ is a rational number which has the same class in the quotient group $\mathbf{Q}/\mathbf{Z}$ as $\dfrac{a_i <i>}{m}$. We conclude that $\lambda\theta \in \mathbf{Z}\Gamma$ iff $a_1 \equiv 0 \bmod m$, that is, (i) is equivalent to (iii). This finishes the proof of proposition (6.3). □

Having thus determined $\mathrm{Ann}_{\mathbf{Z}\Gamma}\mu_m(\bar{\mathbf{Q}})$ we now come to the main aim of this section, which is to relate the annihilator ideal I of the $\mathbf{Z}\Gamma$-module $\mu_m(\bar{\mathbf{Q}})$ to the annihilator ideal J of the $\mathbf{Z}\Gamma$-module $Cl_{\mathbf{Q}(m)}$. This relation is given by the following result, to be derived from theorem (3.3) and proposition (1.2) (i), (ii); we will not need proposition (6.3) for the proof.

(6.5) THEOREM. $\theta I \subseteq J$.

However there will be a problem. We will see that theorem (3.3) only implies the following result (6.6). Let the absolute degree of a prime ideal in an algebraic number field be the degree of its residue class field over its prime field.

(6.6) Let $\lambda \in \mathbf{Z}\Gamma$. If λ is an annihilator of $\mu_m(\bar{\mathbf{Q}})$ then $\lambda\theta$ is an annihilator of the subgroup of $Cl_{\mathbf{Q}(m)}$ generated by the classes of the primes in $\mathbf{Q}(m)$ of absolute degree one.

In order to get the full result (6.5) one can proceed in either one of the following two ways.

(i) One can extend theorem (3.3) and proposition (1.2) (ii) to Gauss sums associated to *arbitrary* finite fields. Then the extended results imply the desired theorem. However, the easy method of obtaining the prime factorization of Gauss sums which is given in this paper does not seem to extend to the case of arbitrary finite fields. Therefore we would fall back on the usual proof of this prime factorization, which, though it is elementary, requires rather delicate arguments.

(ii) One can instead allow oneself to use the following fact:

(6.7) The subgroup of $Cl_{\mathbf{Q}(m)}$ generated by the primes in $\mathbf{Q}(m)$ of absolute degree one is the whole of $Cl_{\mathbf{Q}(m)}$.

This follows immediately from the following standard density results. Let F be an algebraic number field, then

(a) The set of primes in F of absolute degree > 1 has zero Dirichlet density.

(b) The primes in F are distributed over the elements of Cl_F, the ideal class group of F, with equal Dirichlet density.

We choose the second alternative. Now we are ready to prove theorem (6.5).

Proof of Theorem (6.5). Let λ be an innihilator of the $\mathbf{Z}\Gamma$-module $\mu_m(\bar{\mathbf{Q}})$. By proposition (1.2) (ii) the number G^λ in $\mathbf{Q}(pm)^*$ is fixed by $\text{Gal}\left(\mathbf{Q}(pm)/\mathbf{Q}(m)\right)$ and so, by Galois theory, $G^\lambda \in \mathbf{Q}(m)^*$. By theorem (3.3) we get the following result

(6.8) The fractional ideal $\mathfrak{p}^{\lambda\theta}$ in $\mathbf{Q}(m)$ is principal.

Namely it has generator G^λ.

Recall that the primes in $\mathbf{Q}(m)$ of absolute degree one are precisely the primes which lie over prime numbers which are $\equiv 1 \bmod m$ and recall the description of such primes given in (2.2). Now we can, while keeping m fixed, vary (p, χ) over all pairs consisting of a prime number $p \equiv 1 \bmod m$ and a multiplicative character χ on $\mathbf{F}_p$ of order m. Then $\mathfrak{p}$ runs over all primes in $\mathbf{Q}(m)$ of absolute degree one. Therefore (6.8) amounts to the fact that $\lambda\theta$ kills the class in $Cl_{\mathbf{Q}(m)}$ of each prime in $\mathbf{Q}(m)$ of absolute degree one. Therefore we have proved (6.6) and so, by (6.7), the statement of theorem (6.5) follows. □

REFERENCE

[W] WEIL, A. La cyclotomie jadis et naguère. *Enseign. Math. 20* (1974), 247-263.

(Reçu le 14 septembre 1989)

Jan Brinkhuis
Econometric Institute
Erasmus University
P.O. Box 1738
3000 DR Rotterdam
(The Netherlands)

ADDED IN PROOF. Essentially the same simplification occurs in the following paper: L. C. WASHINGTON, "Stickelberger's theorem for cyclotomic fields, in the spirit of Kummer and Thaine", in *Number Theory,* ed. J.-M. de Koninck and C. Levesque, Proceedings of the International Number Theory Conference at Laval 1987, Walter de Gruyter, Berlin-New York, 1989, pp. 990-993.