GAUSS SUMS AND THEIR PRIME FACTORIZATION

Autor(en): **Brinkhuis, Jan**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **36 (1990)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **12.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-57901

L'Enseignement Mathématique, t. 36 (1990), p. 39-51

GAUSS SUMS AND THEIR PRIME FACTORIZATION

by Jan BRINKHUIS

INTRODUCTION

The prime factorization of Gauss sums associated to a finite field of p elements, with p a prime number, plays a fundamental role in the theory of cyclotomic fields. Therefore it is desirable to have a proof which is as simple as possible. The usual proof, as given for example by Weil in [W], proceeds by determining the leading term of the local expansion of such a Gauss sum in each completion above p of the appropriate cyclotomic field. This requires some relatively delicate manipulations with binomial coefficients. The new proof which is offered in the present paper avoids this completely: instead we proceed by deriving the prime factorization as a formal consequence of four basic properties of Gauss sums (they are listed in proposition (1.2)). The resulting proof is very easy to memorize, in fact it is probably the simplest possible one. The novel idea which gives rise to the simplification is a general, almost trivial observation on inertia groups, which sometimes leads to an effortless determination of discrete valuations modulo a specific positive integer (see lemma (4.3) and the discussion following it).

It seemed appropriate to include also an introduction to one of the main applications of the prime factorization of Gauss sums, the annihilation of ideal class groups by Stickelberger ideals. In our presentation of this application, we let the annihilator ideal of a group of roots of unity play a central role.

1. GAUSS SUMS AND SOME OF THEIR PROPERTIES

Let $\mathbf{Z}$ be the ring of rational integers, $\mathbf{Q}$ the field of rational numbers and $\bar{\mathbf{Q}}$ an algebraic closure of $\mathbf{Q}$ chosen once and for all. Subfields F of $\bar{\mathbf{Q}}$ of finite degree over $\mathbf{Q}$ are called algebraic number fields. For each

algebraic number field F the integral closure of $\mathbf{Z}$ in F is called the ring of algebraic integers in F. Let p be an odd prime number. We choose a primitive p-th root of unity ζ_p in $\bar{\mathbf{Q}}$. Let $\mathbf{F}_p$ be the finite field of p elements, that is, $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$. For each commutative ring R with unit element, let R^* be the group of invertible elements in R. Let χ be a non-trivial multiplicative character on $\mathbf{F}_p$, that is, a non-trivial homomorphism from $\mathbf{F}_p^*$, which is a cyclic group of order $p-1$, to $\bar{\mathbf{Q}}^*$. Let m be the order of χ, then $m > 1$ and $m|p-1$, that is, m divides $p-1$. We associate to χ the following number in $\bar{\mathbf{Q}}$, called the Gauss sum of χ,

$$G = \sum_x \chi(x^{-1})\zeta_p^x \tag{1.1}$$

where x runs over $\mathbf{F}_p^*$. Our aim is to determine the prime factorization of G. We start by recalling and verifying four properties of G; after that we can forget the explicit formula (1.1) as we will only use these four properties of G to obtain its prime factorization. Before stating them below in proposition (1.2) we first introduce some notation.

Each action of a group Γ on a field F will be denoted by the exponential notation: r^γ is the image of r under the action of γ for each $\gamma \in \Gamma$ and each $r \in F$. Whenever such an action is given we will extend the action of Γ on the multiplicative group F^* by $\mathbf{Z}$-linearity to an action of the group ring $\mathbf{Z}\Gamma$ on F^*; we will denote this action also by the exponential notation. Thus for each element $\lambda = \sum_\gamma n_\gamma \gamma$ of $\mathbf{Z}\Gamma$ where γ runs over Γ and where $n_\gamma \in \mathbf{Z}$ for all $\gamma \in \Gamma$, and for each $r \in F^*$, the element r^λ is the element $\prod_\gamma (r^\gamma)^{n_\gamma}$ in F^* where γ runs over Γ. For each $n \in \mathbf{N}$ let $\mathbf{Q}(n)$ be the n-th cyclotomic field, which is defined to be the algebraic number field generated over $\mathbf{Q}$ by the n-th roots of unity. For each Galois extension of fields F/E let $\mathrm{Gal}(F/E)$ be its Galois group. As $m \mid p-1$, the integers p and m are relatively prime and so $\mathrm{Gal}(\mathbf{Q}(pm)/\mathbf{Q}) = \mathrm{Gal}(\mathbf{Q}(p)/\mathbf{Q}) \times \mathrm{Gal}(\mathbf{Q}(m)/\mathbf{Q})$. We view the two factors of this product as subgroups of $\mathrm{Gal}(\mathbf{Q}(pm)/\mathbf{Q})$. In other words, we identify $\mathrm{Gal}(\mathbf{Q}(p)/\mathbf{Q})$ with $\mathrm{Gal}(\mathbf{Q}(pm)/\mathbf{Q}(m))$ by letting each $\sigma \in \mathrm{Gal}(\mathbf{Q}(p)/\mathbf{Q})$ act trivially on the m-th roots of unity and, similarly, we identify $\mathrm{Gal}(\mathbf{Q}(m)/\mathbf{Q})$ with $\mathrm{Gal}(\mathbf{Q}(pm)/\mathbf{Q}(p))$ by letting each $\tau \in \mathrm{Gal}(\mathbf{Q}(m)/\mathbf{Q})$ act trivially on the p-th roots of unity. For each $n \in \mathbf{N}$ one defines an isomorphism from $(\mathbf{Z}/n\mathbf{Z})^*$ to $\mathrm{Gal}(\mathbf{Q}(n)/\mathbf{Q})$ by sending each $i \in (\mathbf{Z}/n\mathbf{Z})^*$ to the automorphism of the field $\mathbf{Q}(n)$ which acts on the n-th roots of unity by raising each of them to the power i. For each $x \in (\mathbf{Z}/p\mathbf{Z})^*$ we denote the corresponding

element of $\mathrm{Gal}(\mathbf{Q}(p)/\mathbf{Q})$ by σ_x and for each $y \in (\mathbf{Z}/m\mathbf{Z})^*$ we denote the corresponding element of $\mathrm{Gal}(\mathbf{Q}(m)/\mathbf{Q})$ by τ_y. If $x \in (\mathbf{Z}/p\mathbf{Z})^*$ and if $k \in \mathbf{Z}$ is a representative of x, we will sometimes write σ_k instead of σ_x; we make a similar convention for the elements of $\mathrm{Gal}(\mathbf{Q}(m)/\mathbf{Q})$. Now we state and verify those properties of the number G which we will use to determine its prime factorization.

(1.2) PROPOSITION. *The Gauss sum G as defined by (1.1) has the following properties*

(i) $G \in \mathbf{Q}(pm)$

(ii) $G^{\sigma_x - 1} = \chi(x)$ *for all* $x \in \mathbf{F}_p^*$

(iii) G *is an algebraic integer*

(iv) $G \mid p$, *that is,* G *divides* p.

Proof. (i) and (iii). These properties follow immediately from the definition of G as a sum of roots of unity of order dividing pm.

(ii) Let $x \in \mathbf{F}_p^*$. Then $G^{\sigma_x} = \sum_y \chi(y^{-1})\zeta_p^{xy}$, where y runs over $\mathbf{F}_p^*$, replacing y by $x^{-1}y$ one gets $\chi(x)\sum_y \chi(y^{-1})\zeta_p^{y}$, that is, $\chi(x)G$. Therefore $G^{\sigma_x - 1} = \chi(x)$, as required.

(iv) We take the product of $G = \sum_x \chi(x^{-1})\zeta_p^{x}$ and its complex conjugate $H = \sum_y \chi(y)\zeta_p^{-y}$ where x and y run over $\mathbf{F}_p^*$. This product equals $\sum_{x,y} \chi(x^{-1}y)\zeta_p^{x-y}$, replacing y by xy one gets

$$\sum_{x,y} \chi(y)\zeta_p^{x-xy} = \sum_y [\chi(y)\sum_x \zeta_p^{(1-y)x}]$$

where x and y run over $\mathbf{F}_p^*$. Now we let, in the inner sum of this expression, x run over the whole of $\mathbf{F}_p$ instead of over $\mathbf{F}_p^*$. Then the value of the expression does not change, as $\sum_y \chi(y) = 0$ where y runs over $\mathbf{F}_p^*$-here we use that χ is non-trivial. If we now use the following formulas

$$\begin{aligned} \sum_v \zeta_p^{uv} &= p \quad \text{if } u = 0 \\ &= 0 \quad \text{if } u \in \mathbf{F}_p^* \end{aligned}$$

where v runs over $\mathbf{F}_p$, then we get that the product of G and H is equal to p and so, as H is an algebraic integer, we conclude that G divides p, as required. □

2. The prime factorization of p in $\mathbf{Q}(pm)$

The next thing to do is to recall the prime factorization of the prime number p in the field $\mathbf{Q}(pm)$ and to introduce a notation for the primes of $\mathbf{Q}(pm)$ above p which is convenient for bookkeeping purposes. The prime number p ramifies completely in $\mathbf{Q}(p)$, in fact $p \sim (\zeta_p - 1)^{p-1}$ where $\sim$ denotes equality up to a factor which is an algebraic unit. The prime number p splits completely in $\mathbf{Q}(m)$, as $p \equiv 1 \bmod m$. These two facts determine by ramification theory the prime factorization of p in $\mathbf{Q}(pm)$: the prime number p splits completely in the extension $\mathbf{Q}(m)/\mathbf{Q}$ and each prime in $\mathbf{Q}(m)$ above p ramifies completely in the extension $\mathbf{Q}(pm)/\mathbf{Q}(m)$. This implies moreover that for each prime $\mathfrak{Q}$ in $\mathbf{Q}(pm)$ above p its residue field is $\simeq \mathbf{F}_p$ and that the group $\mathrm{Gal}(\mathbf{Q}(pm)/\mathbf{Q}(m))$, which we have identified with $\mathrm{Gal}(\mathbf{Q}(p)/\mathbf{Q})$, is the inertia group of $\mathfrak{Q}$ in the extension $\mathbf{Q}(pm)/\mathbf{Q}$, that is, it consists of the automorphisms of the field $\mathbf{Q}(pm)$ which leave $\mathfrak{Q}$ fixed and which moreover induce the trivial automorphism on the residue class field of $\mathfrak{Q}$ (this last property is automatically satisfied as the residue class field is $\simeq \mathbf{F}_p$ and so it has no non-trivial automorphisms).

Now we are going to give a more precise description of the primes in $\mathbf{Q}(pm)$ above p. Let ϕ be the Euler phi function defined on the natural numbers in one of the following, equivalent, ways:

(i) $\phi(n)$ is the number of positive integers $\leqslant n$ which are relatively prime to n.

(ii) $\phi(n) = \#(\mathbf{Z}/n\mathbf{Z})^*$.

(iii) $\phi(n) = [\mathbf{Q}(n) : \mathbf{Q}]$.

(iv) $\phi(n)$ is the number of isomorphisms between two cyclic groups of order n.

For each field F and each $n \in \mathbf{N}$ let $\mu_n(F)$ be the group of n-th roots of unity in F; this is in general a cyclic group of order dividing n. As $m \mid p-1$ the order of $\mu_m(\mathbf{F}_p)$ is precisely m. The set of primes $\mathfrak{q}$ in $\mathbf{Q}(m)$ above p and the set of isomorphisms ψ from $\mu_m(\bar{\mathbf{Q}})$ to $\mu_m(\mathbf{F}_p)$ have both $\phi(m)$ elements. In fact there is a canonical bijection between these two sets: let $\mathfrak{q}$ correspond to ψ iff $\zeta \equiv \psi(\zeta) \bmod \mathfrak{q}$ for all $\zeta \in \mu_m(\bar{\mathbf{Q}})$. Among those isomorphisms ψ we will now single one out. Let z be a generator of $\mathbf{F}_p^*$, then $\chi(z)$ is a generator of $\mu_m(\bar{\mathbf{Q}})$ and $z^{(p-1)/m}$ is a generator of $\mu_m(\mathbf{F}_p)$. Therefore there is a unique isomorphism from $\mu_m(\bar{\mathbf{Q}})$ to $\mu_m(\mathbf{F}_p)$ which sends $\chi(z)$ to $z^{(p-1)/m}$. It clearly sends $\chi(x)$ to $x^{(p-1)/m}$ for all $x \in \mathbf{F}_p^*$. This is the isomorphism which we single out. Let $\mathfrak{p}$ be the prime in $\mathbf{Q}(m)$ above p

corresponding to this isomorphism and let $\mathfrak{P}$ be the prime in $\mathbf{Q}(pm)$ above $\mathfrak{p}$, so $\mathfrak{P}^{p-1} = \mathfrak{p}$, if we identify the prime ideal $\mathfrak{p}$ of $\mathbf{Q}(m)$ with its extension to a fractional ideal of $\mathbf{Q}(pm)$. Thus we have the following congruence

$$\chi(x) \equiv x^{(p-1)/m} \bmod \mathfrak{P} \quad \text{for all } x \in \mathbf{F}_p^* \,. \tag{2.1}$$

Let $v_{\mathfrak{P}}$ be the valuation on $\mathbf{Q}(pm)$ corresponding to $\mathfrak{P}$. The number $\zeta_p - 1$ is a uniformizing element of $v_{\mathfrak{P}}$ in the sense that $v_{\mathfrak{P}}(\zeta_p - 1) = 1$. Moreover one has $v_{\mathfrak{P}}(p) = p - 1$. From the prime $\mathfrak{P}$ we get the other primes in $\mathbf{Q}(pm)$ above p by Galois action: each prime in $\mathbf{Q}(pm)$ above p is equal to $\mathfrak{P}^\tau$, the image of $\mathfrak{P}$ under the Galois action of τ, for a unique $\tau \in \mathrm{Gal}\,(\mathbf{Q}(m)/\mathbf{Q})$.

(2.2) In the same way we get from the prime $\mathfrak{p}$ all the primes in $\mathbf{Q}(m)$ above p. However, in the last section of this paper, it will be more convenient to use a slightly different description of the primes in $\mathbf{Q}(m)$ above p. There we will not fix χ, as we do in the rest of the paper, but we will let it run over the $\phi(m)$ multiplicative characters on $\mathbf{F}_p$ of order m. For each such χ we let $\mathfrak{p} = \mathfrak{p}(\chi)$ be the prime in $\mathbf{Q}(m)$ above p associated to χ in the way described above. Then $\mathfrak{p} = \mathfrak{p}(\chi)$ runs over the $\phi(m)$ primes in $\mathbf{Q}(m)$ above p.

3. The prime factorization of the Gauss sum: statement of the result

Before we state the outcome of the prime factorization of G we introduce some more notation. For each $i \in \mathbf{Z}$ with $0 < i < m$ and $(i, m) = 1$ we define the integer k_i to be the exponent of the prime $\mathfrak{P}^{\tau_i^{-1}}$ in the prime factorization of G in $\mathbf{Q}(pm)$ (it turns out that an inverse has to appear somewhere and this is a convenient place). Equivalently, k_i is the exponent of the prime $\mathfrak{P}$ in the prime factorization of G^{τ_i}, that is,

$$k_i = v_{\mathfrak{P}}(G^{\tau_i}) \,. \tag{3.1}$$

Any given action of a group Γ on an algebraic number field F induces an action of the group Γ on $I(F)$, the group of fractional ideals in F. Now we proceed with it just as we did above with the action of Γ on the multiplicative group F^*: we denote the action of Γ on $I(F)$ by the

exponential notation, we extend it by $\mathbf{Z}$-linearity to an action of the group ring $\mathbf{Z}\Gamma$ on $I(F)$ and we denote this action also by the exponential notation. If moreover E is a subfield of F then we can view $I(E)$ as a subgroup of $I(F)$ by extension of fractional ideals; moreover if $\mathfrak{a} \in I(E)$ with $\mathfrak{a} = \mathfrak{b}^r$ for some $\mathfrak{b} \in I(F)$ and some $r \in \mathbf{N}$ and if $\lambda \in \mathbf{Q}\Gamma$ with $r\lambda \in \mathbf{Z}\Gamma$, then we make as usual the convention that the formal expression $\mathfrak{a}^\lambda$ means the fractional ideal $\mathfrak{b}^{(r\lambda)}$ in F. We define the Stickelberger element θ in the group ring $\mathbf{Q}[\mathrm{Gal}(\mathbf{Q}(m)/\mathbf{Q})]$ by

$$\theta = \sum_i \frac{i}{m} \tau_i^{-1} \tag{3.2}$$

where i runs over the positive integers $< m$ which are relatively prime to m. The formal expression $\mathfrak{p}^\theta$ denotes the ideal $\mathfrak{P}^{(p-1)\theta}$, by the convention made above for fractional exponents and by the relation $\mathfrak{p} = \mathfrak{P}^{p-1}$ between $\mathfrak{p}$ and $\mathfrak{P}$.

Now we are ready to formulate the following result of Stickelberger on the Gauss sum G as defined in (1.1):

(3.3) THEOREM. *The prime factorization of the Gauss sum G is $\mathfrak{p}^\theta$.*

(3.3) The statement of the theorem is clearly equivalent to the following one: only the primes in $\mathbf{Q}(pm)$ above p occur in the prime factorization of G, and their exponents in this factorization are as follows: for each positive integer $i < m$ which is relatively prime to m, the exponent of the prime $\mathfrak{P}^{\tau_i^{-1}}$ is $k_i = \dfrac{p-1}{m} i$.

4. A USEFUL LEMMA

In the proof of theorem (3.3) we will use a simple general lemma to determine the exponents in the prime factorization of the Gauss sum G. The aim of this section is to state and to prove this lemma. Let F be a field, v a discrete valuation on F, $F(v)$ the residue class field of v and π a uniformizing element of v, that is, $\pi \in F^*$ with $v(\pi) = 1$. An element $u \in F^*$ with $v(u) = 0$ will be called a v-unit. We define a homomorphism l from F^* to $\mathbf{Z} \times F(v)^*$ by sending each $\alpha \in F^*$ to the pair (k, r) consisting of the integer $k = v(\alpha)$ and the residue class r in $F(v)$ of the v-unit α/π^k. We call $l(\alpha)$

the "leading term" of $\alpha \in F^*$ with respect to the valuation v and the uniformizing element π. We define the inertia group I of F at v to be the group of those automorphisms of the field F which fix the valuation v and which induce the trivial automorphism on the residue class field $F(v)$. Now let an element γ of I be given. We consider the homomorphism ρ from the multiplicative group F^* to itself which sends α to $\alpha^{\gamma-1}$ for each $\alpha \in F^*$. From our assumptions on the automorphism γ the following facts follow immediately:

(4.1) The leading term of $\rho(u)$ is $(0, 1)$ for each v-unit u.

(4.2) The leading term of $\rho(\pi)$ is $(0, z)$ where z is the residue class in $F(v)$ of the v-unit $\pi^{\gamma-1}$.

The following crucial lemma gives the effect of ρ on the leading term of an arbitrary element of F^*.

(4.3) LEMMA. *Let* $\alpha \in F^*$. *If* $l(\alpha) = (k, r)$, *then* $l(\rho(\alpha)) = (0, z^k)$.

Proof. Let $\alpha \in F^*$; write $\alpha = \pi^k u$ with $k = v(\alpha)$ and u a v-unit. Then $\rho(\alpha) = \rho(\pi)^k \rho(u)$. So, as l is a homomorphism and by (4.1) and (4.2), we get that the leading term of $\rho(\alpha)$ is $(0, z^k)$ as required. □

(4.4) Discussion. This lemma is intended for the following type of application. Suppose we are given a field F, a discrete valuation v on F and a non-zero element α of F and we are asked to determine the integer $v(\alpha)$. Then lemma (4.3) suggests the following approach. Find a non-trivial element γ of I, the inertia group of F at v and pick a uniformizing element π of the valuation ring in F of v. Let $\mathfrak{m}$ be the maximal ideal of this valuation ring. Let $e_0 \in \mathbf{N} \cup \{\infty\}$ be the order of the residue class $\pi^{\gamma-1}$ mod $\mathfrak{m}$ in the multiplicative group $F(v)^*$. Having done that, determine a rational integer k such that the following congruence holds

$$\alpha^{\gamma-1} \equiv (\pi^{\gamma-1})^k \bmod \mathfrak{m}\,. \tag{4.5}$$

It then follows that $v(\alpha) \equiv k \pmod{e_0}$ (if $e_0 = \infty$ we just mean by this that $v(\alpha) = k$). The crux of the matter is that it is much easier to determine $v(\alpha)$ mod e_0 via the congruence (4.5) than it is to compute $v(\alpha)$ itself by the following "brute force" method, which is the usual approach: one embeds F in its completion at v, one expands α there as a power series in π with coefficients in a suitable set of representatives of the residue class field $F(v)$, and one determines the leading term of the resulting expansion. Moreover,

"sometimes" there is, once one has determined $v(\alpha)$ mod e_0, a relatively easy method to determine moreover $v(\alpha)$ itself. It would take us too far to give a formal account of this method, so in this matter we will restrict ourselves to the special case of Gauss sums.

(4.6) For general insight it is of interest to know how e_0 depends on γ. We will give the answer under the assumptions that the residual characteristic of v is a prime number, say l, and that γ has finite order, say e. For each $n \in \mathbf{N}$ we can write $n = l^r n'$ with $r \in \mathbf{N} \cup \{0\}$, $n' \in \mathbf{N}$ and $l \nmid n'$; then we call n' the l-free part of n. Now we give the desired result.

(4.7) The number e_0 is the l-free part of e.

We omit the proof of this fact, as we will not make use of it: in our application it will be obvious what e_0 is, once we have computed the class of $\pi^{\gamma-1}$ in $F(v)$ which is something that we have to do anyway.

5. The prime factorization of the Gauss sum: proof of the result

Now we are ready to prove theorem (3.3). We will do this by proving the statements in (3.4).

Proof of (3.4). By proposition (1.2) (i), (iii) and (iv) only primes of $\mathbf{Q}(pm)$ above p can occur in the prime factorization of G. Let $i \in \mathbf{Z}$ with $0 < i < m$ and $(i, m) = 1$. We have to determine the integer k_i defined by (3.1). We are first going to determine k_i modulo $p - 1$ by using lemma (4.3). We apply this lemma to $F = \mathbf{Q}(pm)$, $v = v_{\mathfrak{P}}$, $\alpha = G^{\tau_i}$, $\pi = \zeta_p - 1$ and $\gamma = \sigma_g$ where $g \in \mathbf{Z}$ with $0 < g < p$ is such that $g \pmod p$ generates $(\mathbf{Z}/p\mathbf{Z})^* = \mathbf{F}_p^*$; then $k = k_i$ and the residue class field $F(v)$ it $\mathbf{F}_p$. This choice satisfies the requirements of the lemma as σ_g lies in $\mathrm{Gal}(\mathbf{Q}(p)/\mathbf{Q})$ which is the inertia group of $\mathfrak{P}$ in the extension $\mathbf{Q}(pm)/\mathbf{Q}$. Now let us calculate the left and right hand side of the equality $l(\rho(\alpha)) = (0, z^k)$ which holds by lemma (4.3). On the one hand $\rho(\alpha) = G^{\tau_i(\sigma_g - 1)}$ which is by proposition (1.2) (ii) equal to

$$\chi(\bar{g})^{\tau_i} = \chi(\bar{g})^i \quad \text{where} \quad \bar{g} = g \bmod p$$

and this is by (2.1) congruent to $g^{\frac{p-1}{m} i} \bmod \mathfrak{P}$. Therefore

$$l(\rho(\alpha)) = (0, \bar{g}^{\frac{p-1}{m} i}) .$$

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 $\Gamma = \mathrm{Gal}(\mathbf{Q}(m)/\mathbf{Q})$ 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

$$\beta_x = 1 \qquad \text{if } x = 1 \tag{6.1}$$
$$= \sigma_x - <x> \qquad \text{otherwise}.$$

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

$$\lambda = \sum_x a_x \beta_x \tag{6.2}$$

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

$$\zeta^{\beta_x} = \zeta \qquad \text{if } x = 1$$
$$= 1 \qquad \text{otherwise}.$$

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

$$\beta_x\theta = \theta \quad \text{if } x = 1$$
$$\in \mathbf{Z}\Gamma \quad \text{otherwise}. \tag{6.4}$$

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 $\frac{a_i <i>}{m}$. 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 $\mathrm{Gal}(\mathbf{Q}(pm)/\mathbf{Q}(m))$ 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.