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

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **12.07.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

"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 $g\,(\mathrm{mod}\, p)$ 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 $\mathrm{Ann}_{\mathbf{Z}\Gamma} Cl_{\mathbf{Q}(m)}$.