

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

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **23.09.2024**

#### **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.

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

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

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  $\tau$ , for a unique  $\tau \in \text{Gal}(\mathbf{Q}(m)/\mathbf{Q})$ .

(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  $\chi$ , 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  $\chi$  we let  $\mathfrak{p} = \mathfrak{p}(\chi)$  be the prime in  $\mathbf{Q}(m)$  above  $p$  associated to  $\chi$  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  $G^{\tau_i}$ , that is,

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

Any given action of a group  $\Gamma$  on an algebraic number field  $F$  induces an action of the group  $\Gamma$  on  $I(F)$ , the group of fractional ideals in  $F$ . Now we proceed with it just as we did above with the action of  $\Gamma$  on the multiplicative group  $F^*$ : we denote the action of  $\Gamma$  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  $\alpha \in I(E)$  with  $\alpha = \mathfrak{b}^r$  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  $\alpha^\lambda$  means the fractional ideal  $\mathfrak{b}^{(r\lambda)}$  in  $F$ . We define the Stickelberger element  $\theta$  in the group ring  $\mathbf{Q}[\text{Gal}(\mathbf{Q}(m)/\mathbf{Q})]$  by

$$(3.2) \quad \theta = \sum_i \frac{i}{m} \tau_i^{-1}$$

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

#### 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  $\pi$  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  $\alpha/\pi^k$ . We call  $l(\alpha)$