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: **26.09.2024**

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

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 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,

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

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 $l(\alpha)$