4. A USEFUL LEMMA

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

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