Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 36 (1990)

Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: GAUSS SUMS AND THEIR PRIME FACTORIZATION

Autor: Brinkhuis, Jan

Kapitel: 2. The prime factorization of p in Q(pm)

DOI: https://doi.org/10.5169/seals-57901

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

(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 $\tau \in \mathrm{Gal}\left(\mathbf{Q}(m)/\mathbf{Q}\right)$.

(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