1. Gauss sums and some of their properties

L'Enseignement Mathématique, t. 36 (1990), p. 39-51

GAUSS SUMS AND THEIR PRIME FACTORIZATION

by Jan BRINKHUIS

INTRODUCTION

The prime factorization of Gauss sums associated to a finite field of p elements, with p a prime number, plays a fundamental role in the theory of cyclotomic fields. Therefore it is desirable to have a proof which is as simple as possible. The usual proof, as given for example by Weil in [W], proceeds by determining the leading term of the local expansion of such a Gauss sum in each completion above p of the appropriate cyclotomic field. This requires some relatively delicate manipulations with binomial coefficients. The new proof which is offered in the present paper avoids this completely: instead we proceed by deriving the prime factorization as a formal consequence of four basic properties of Gauss sums (they are listed in proposition (1.2)). The resulting proof is very easy to memorize, in fact it is probably the simplest possible one. The novel idea which gives rise to the simplification is a general, almost trivial observation on inertia groups, which sometimes leads to an effortless determination of discrete valuations modulo a specific positive integer (see lemma (4.3) and the discussion following it).

It seemed appropriate to include also an introduction to one of the main applications of the prime factorization of Gauss sums, the annihilation of ideal class groups by Stickelberger ideals. In our presentation of this application, we let the annihilator ideal of a group of roots of unity play a central role.

1. GAUSS SUMS AND SOME OF THEIR PROPERTIES

Let $\mathbf{Z}$ be the ring of rational integers, $\mathbf{Q}$ the field of rational numbers and $\bar{\mathbf{Q}}$ an algebraic closure of $\mathbf{Q}$ chosen once and for all. Subfields F of $\bar{\mathbf{Q}}$ of finite degree over $\mathbf{Q}$ are called algebraic number fields. For each

algebraic number field F the integral closure of $\mathbf{Z}$ in F is called the ring of algebraic integers in F. Let p be an odd prime number. We choose a primitive p-th root of unity ζ_p in $\bar{\mathbf{Q}}$. Let $\mathbf{F}_p$ be the finite field of p elements, that is, $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$. For each commutative ring R with unit element, let R^* be the group of invertible elements in R. Let χ be a non-trivial multiplicative character on $\mathbf{F}_p$, that is, a non-trivial homomorphism from $\mathbf{F}_p^*$, which is a cyclic group of order $p-1$, to $\bar{\mathbf{Q}}^*$. Let m be the order of χ, then $m > 1$ and $m|p-1$, that is, m divides $p-1$. We associate to χ the following number in $\bar{\mathbf{Q}}$, called the Gauss sum of χ,

$$G = \sum_x \chi(x^{-1})\zeta_p^x \tag{1.1}$$

where x runs over $\mathbf{F}_p^*$. Our aim is to determine the prime factorization of G. We start by recalling and verifying four properties of G; after that we can forget the explicit formula (1.1) as we will only use these four properties of G to obtain its prime factorization. Before stating them below in proposition (1.2) we first introduce some notation.

Each action of a group Γ on a field F will be denoted by the exponential notation: r^γ is the image of r under the action of γ for each $\gamma \in \Gamma$ and each $r \in F$. Whenever such an action is given we will extend the action of Γ on the multiplicative group F^* by $\mathbf{Z}$-linearity to an action of the group ring $\mathbf{Z}\Gamma$ on F^*; we will denote this action also by the exponential notation. Thus for each element $\lambda = \sum_\gamma n_\gamma \gamma$ of $\mathbf{Z}\Gamma$ where γ runs over Γ and where $n_\gamma \in \mathbf{Z}$ for all $\gamma \in \Gamma$, and for each $r \in F^*$, the element r^λ is the element $\prod_\gamma (r^\gamma)^{n_\gamma}$ in F^* where γ runs over Γ. For each $n \in \mathbf{N}$ let $\mathbf{Q}(n)$ be the n-th cyclotomic field, which is defined to be the algebraic number field generated over $\mathbf{Q}$ by the n-th roots of unity. For each Galois extension of fields F/E let $\mathrm{Gal}(F/E)$ be its Galois group. As $m \mid p-1$, the integers p and m are relatively prime and so $\mathrm{Gal}(\mathbf{Q}(pm)/\mathbf{Q}) = \mathrm{Gal}(\mathbf{Q}(p)/\mathbf{Q}) \times \mathrm{Gal}(\mathbf{Q}(m)/\mathbf{Q})$. We view the two factors of this product as subgroups of $\mathrm{Gal}(\mathbf{Q}(pm)/\mathbf{Q})$. In other words, we identify $\mathrm{Gal}(\mathbf{Q}(p)/\mathbf{Q})$ with $\mathrm{Gal}(\mathbf{Q}(pm)/\mathbf{Q}(m))$ by letting each $\sigma \in \mathrm{Gal}(\mathbf{Q}(p)/\mathbf{Q})$ act trivially on the m-th roots of unity and, similarly, we identify $\mathrm{Gal}(\mathbf{Q}(m)/\mathbf{Q})$ with $\mathrm{Gal}(\mathbf{Q}(pm)/\mathbf{Q}(p))$ by letting each $\tau \in \mathrm{Gal}(\mathbf{Q}(m)/\mathbf{Q})$ act trivially on the p-th roots of unity. For each $n \in \mathbf{N}$ one defines an isomorphism from $(\mathbf{Z}/n\mathbf{Z})^*$ to $\mathrm{Gal}(\mathbf{Q}(n)/\mathbf{Q})$ by sending each $i \in (\mathbf{Z}/n\mathbf{Z})^*$ to the automorphism of the field $\mathbf{Q}(n)$ which acts on the n-th roots of unity by raising each of them to the power i. For each $x \in (\mathbf{Z}/p\mathbf{Z})^*$ we denote the corresponding

element of $\mathrm{Gal}(\mathbf{Q}(p)/\mathbf{Q})$ by σ_x and for each $y \in (\mathbf{Z}/m\mathbf{Z})^*$ we denote the corresponding element of $\mathrm{Gal}(\mathbf{Q}(m)/\mathbf{Q})$ by τ_y. If $x \in (\mathbf{Z}/p\mathbf{Z})^*$ and if $k \in \mathbf{Z}$ is a representative of x, we will sometimes write σ_k instead of σ_x; we make a similar convention for the elements of $\mathrm{Gal}(\mathbf{Q}(m)/\mathbf{Q})$. Now we state and verify those properties of the number G which we will use to determine its prime factorization.

(1.2) PROPOSITION. *The Gauss sum G as defined by (1.1) has the following properties*

(i) $G \in \mathbf{Q}(pm)$

(ii) $G^{\sigma_x - 1} = \chi(x)$ *for all* $x \in \mathbf{F}_p^*$

(iii) G *is an algebraic integer*

(iv) $G \mid p$, *that is,* G *divides* p.

Proof. (i) and (iii). These properties follow immediately from the definition of G as a sum of roots of unity of order dividing pm.

(ii) Let $x \in \mathbf{F}_p^*$. Then $G^{\sigma_x} = \sum_y \chi(y^{-1})\zeta_p^{xy}$, where y runs over $\mathbf{F}_p^*$, replacing y by $x^{-1}y$ one gets $\chi(x)\sum_y \chi(y^{-1})\zeta_p^{y}$, that is, $\chi(x)G$. Therefore $G^{\sigma_x - 1} = \chi(x)$, as required.

(iv) We take the product of $G = \sum_x \chi(x^{-1})\zeta_p^{x}$ and its complex conjugate $H = \sum_y \chi(y)\zeta_p^{-y}$ where x and y run over $\mathbf{F}_p^*$. This product equals $\sum_{x,y} \chi(x^{-1}y)\zeta_p^{x-y}$, replacing y by xy one gets

$$\sum_{x,y} \chi(y)\zeta_p^{x-xy} = \sum_y [\chi(y)\sum_x \zeta_p^{(1-y)x}]$$

where x and y run over $\mathbf{F}_p^*$. Now we let, in the inner sum of this expression, x run over the whole of $\mathbf{F}_p$ instead of over $\mathbf{F}_p^*$. Then the value of the expression does not change, as $\sum_y \chi(y) = 0$ where y runs over $\mathbf{F}_p^*$-here we use that χ is non-trivial. If we now use the following formulas

$$\begin{aligned} \sum_v \zeta_p^{uv} &= p \quad \text{if } u = 0 \\ &= 0 \quad \text{if } u \in \mathbf{F}_p^* \end{aligned}$$

where v runs over $\mathbf{F}_p$, then we get that the product of G and H is equal to p and so, as H is an algebraic integer, we conclude that G divides p, as required. □