Zeitschrift: L'Enseignement Mathématique
Band: 36 (1990)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: GAUSS SUMS AND THEIR PRIME FACTORIZATION
Kapitel: Introduction
Autor: Brinkhuis, Jan
DOI: https://doi.org/10.5169/seals-57901

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