THE SINGULAR SERIES FOR SUMS OF SQUARES OF POLYNOMIALS

By L. Carlitz

1. **Introduction.** In previous papers [2], [3] the writer has discussed the number of representations of a polynomial in $GF[p^n, x]$ as the sum of an arbitrary number of squares. The method and results for the case of an odd number of squares are quite different from those for an even number. In the present paper it is shown how the two cases can be considered simultaneously. We construct a certain series modeled after Hardy's singular series for sums of squares of integers [8].

Let $\epsilon(A, H)$ denote a certain p-th root of unity (see (2.3) below) and define the Gauss sum

$$S(A, H) = \sum_U \epsilon(AU^2, H), \tag{1.1}$$

the summation extending over a complete residue system (mod H); put

$$\mathfrak{A}(H) = \frac{1}{|H|^s} \sum_{(G,H)=1} \epsilon(-FG, H) \prod_{i=1}^{s} S(\alpha_i G, H), \tag{1.2}$$

the summation extending over a reduced residue system (mod H). Then we define the "singular series"

$$\mathfrak{S} = \mathfrak{S}(F; k, s) = p^{nk(s-2)} \sum_{\deg H \leq k} \mathfrak{A}(H), \tag{1.3}$$

the summation extending over all *primary* polynomials H of degree $\leq k$. Note that the series in (1.3) is finite.

Let F be a given polynomial of degree $\leq 2k$. Consider the number of solutions of

$$F = \alpha_1 U_1^2 + \cdots + \alpha_s U_s^2, \tag{1.4}$$

where, following Cohen [5], the first l (≥ 1) U's are primary of degree k, and the remaining U's are arbitrary of degree $< k$. Then we show that the number of solutions of (1.4) is given by $\mathfrak{S}(F; k, s)$ for all $s \geq 2$ and arbitrary F; indeed this is true for $s = 1$ also provided F is of degree $2k$, and the leading coefficient of F is a square in $GF(p^n)$. The method of proof is inductive; we first show that the stated result holds for $s = 1$ and then show that it holds for all larger s. Note that we assume $l \geq 1$; our theorem does not hold for $l = 0$ (compare, for s even, Cohen [6]). We remark that when deg $F < 2k$, the value $F = 0$ is allowed.

It remains to show that $\mathfrak{S}$ reduces to the formulas previously obtained [2], [3]. For s even this is rather simple. The odd case is more troublesome. One

Received August 16, 1947.