

SUMS OF SQUARES OF POLYNOMIALS

BY LEONARD CARLITZ

1. **Introduction.** In this note we determine the number of representations of 0 as the sum of an arbitrary number of squares of polynomials in a single indeterminate with coefficients in a fixed Galois field $GF(p^n)$, $p > 2$. More accurately, if $\alpha_1, \dots, \alpha_t$ are t non-zero elements of $GF(p^n)$, $\alpha_1 + \dots + \alpha_t = 0$, we determine the number of solutions of

$$(1.1) \quad 0 = \alpha_1 Y_1^2 + \dots + \alpha_t Y_t^2$$

in primary¹ polynomials Y_i each of degree k , an assigned positive integer. We denote the number of solutions of (1.1) by

$$N_t(0) = N_t^k(0).$$

The more general equation

$$(1.2) \quad \alpha G = \alpha_1 Y_1^2 + \dots + \alpha_t Y_t^2,$$

where $\alpha G \neq 0$, G of degree $\leq 2k$, has been treated in two papers, one on the case t even, the other on the case t odd.² In the latter paper a formula for $N_{2s}(0)$ appeared incidentally. We shall derive this formula anew by the simpler and direct method used in the paper on t even.

To evaluate $N_{2s+1}(0)$, we make use of a known formula for $N_{2s}(G)$, the number of solutions of (1.2) for $t = 2s$. Applying this formula, we first evaluate the sums

$$\sum_G \frac{N_{2s}(G)}{|G|^w}, \quad \sum_G \frac{N_{2s}(G^2)}{|G|^w},$$

extended over all primary G ; the latter sum leads at once to the determination of $N_{2s+1}(0)$.

2. **Determination of $N_{2s}(0)$.** In equation (1.2), let $t = 2s$, $\alpha = \alpha_1 + \dots + \alpha_{2s} \neq 0$, so that G is of degree $2k$. Assume further

$$(2.1) \quad \gamma_i = \alpha_{2i-1} + \alpha_{2i} \neq 0 \quad (i = 1, \dots, s).$$

Received October 27, 1936.

¹ A polynomial is *primary* if the coefficient of the highest power of the indeterminate is the unit element of the Galois field. The capitals A, B, E, G, M, U, V, Y will denote primary polynomials.

² The even case in Transactions of the American Mathematical Society, vol. 35 (1933), pp. 397-410; the odd case in this Journal, vol. 1 (1935), pp. 298-315. These papers will be cited as I and II, respectively.