ON THE REPRESENTATION OF A POLYNOMIAL IN A GALOIS FIELD AS THE SUM OF AN ODD NUMBER OF SQUARES

By Leonard Carlitz

1. **Introduction.** Let $GF(p^n)$ denote a Galois field of order p^n, where p is an *odd* prime, and n is an arbitrary positive integer; let $\mathfrak{D}(x, p^n)$ denote the totality of polynomials in an indeterminate x with coefficients in $GF(p^n)$. We consider the problem of determining the number of representations of a polynomial in $\mathfrak{D}$ as a sum of squares of polynomials in $\mathfrak{D}$ satisfying certain restrictions. The case of an even number of squares has been treated elsewhere;[1] in the present paper, we consider the case of an odd number of squares. Certain results derived in the paper on the even case will be required in the discussion of the odd case.

Our problem may be described more precisely thus. Let $\alpha_1, \alpha_2, \cdots, \alpha_{2s+1}$ be $2s + 1$ non-zero elements of $GF(p^n)$; let L be a *primary* polynomial, that is, one in which the coefficient of the highest power of x is 1. Then

(A) if L is of even degree $2k$, and

$$\epsilon = \alpha_1 + \alpha_2 + \cdots + \alpha_{2s+1} \neq 0,$$

we seek the number of solutions of

$$\epsilon L = \alpha_1 X_1^2 + \alpha_2 X_2^2 + \cdots + \alpha_{2s+1} X_{2s+1}^2$$

in primary X_i each of degree k.

(B) If L is of arbitrary degree l, $2k$ any even integer $> l$, α any non-zero element of the Galois field, and

$$\alpha_1 + \alpha_2 + \cdots + \alpha_{2s+1} = 0,$$

we seek the number of solutions of

$$\alpha L = \alpha_1 X_1^2 + \alpha_2 X_2^2 + \cdots + \alpha_{2s+1} X_{2s+1}^2$$

in primary X_i each of degree k.

The number of solutions of problems (A) and (B) is expressed in terms of the Artin numbers[2] σ_j now to be defined. If Δ and M are in $\mathfrak{D}$, M primary, the symbol (Δ/M) will denote the generalized quadratic character of Δ with respect to M:

Received June 4, 1935.

[1] L. Carlitz, Transactions of the American Mathematical Society, vol. 35 (1933), pp. 397–410; cited as Representations.

[2] E. Artin, Mathematische Zeitschrift, vol. 19 (1924), pp. 153–246.