FACTORIZATION OF IRREDUCIBLE POLYNOMIALS OVER A FINITE FIELD WITH THE SUBSTITUTION $x^{p^r} - x$ FOR x

ANDREW F. LONG, JR.

1. Introduction. Let $GF(q)$ denote the finite field of order $q = p^n$, where p is an arbitrary prime and $n \geq 1$. Let $Q(x)$ denote an irreducible polynomial of degree s over $GF(q)$. For convenience $Q(x)$ is assumed monic throughout the paper.

It is well known [3; 34] that if $Q(x)$ is irreducible of degree s over $GF(q)$, then $Q(x^p - x)$ is also irreducible over $GF(q)$ if the coefficient β of x^{s-1} in $Q(x)$ satisfies

$$\sum_{j=0}^{n-1} \beta^{p^j} \neq 0. \tag{1.1}$$

However, if the sum in (1.1) is equal to zero, $Q(x^p - x)$ is the product of p irreducible factors each of degree s over $GF(q)$. The purpose of the present paper is to describe the irreducible factors of $Q(x^{p^r} - x)$ over $GF(q)$ for an arbitrary positive integer r. Results are known when $n|r$ [4], [5], and we show that [5; Theorems 5.3 and 5.4] are special cases of the results we obtain here.

The principal results of this present paper are contained in the following two theorems from Section 5.

Let

$$N(k, q) = \sum_{ij=k} \mu(i) q^j,$$

where μ is the Möbius function, and let

$$\rho_{\delta,d}(x) = \sum_{j=0}^{\delta-1} x^{p^{dj}}.$$

THEOREM I. *Let $Q(x)$ be irreducible of degree s over $GF(q)$. Let $(r, ns) = d$, and let $ns = d\delta$ and $r = dr'$. If $Q(x) \mid \rho_{\delta,d}(x)$, then $Q(x^{p^r} - x)$ is the product over $GF(q)$ of irreducibles of degree st where t divides r'. For each t dividing r' the number of irreducibles of degree st is*

$$\sum_{\substack{v|d \\ (t,d/v)=1}} N(vt, p)/t.$$

THEOREM II. *Let $Q(x)$ be irreducible of degree s over $GF(q)$. Let $(r, ns) = d$, and let $ns = d\delta$ and $r = dr'$. Let $r' = p^k l$, $(p, l) = 1$ and $k \geq 0$. Let $D = p^k d$. If $Q(x) \nmid \rho_{\delta,d}(x)$, then $Q(x^{p^r} - x)$ is the product over $GF(q)$ of irreducibles of*

Received September 5, 1972.