PACIFIC JOURNAL OF MATHEMATICS
Vol. 32, No. 3, 1970

FACTORIZATION OF A SPECIAL POLYNOMIAL OVER A FINITE FIELD

L. CARLITZ

Let $q = p^z$, where p is a prime and $z \geqq 1$, and put $r = q^n$, $n \geqq 1$. Consider the polynomial

$$F(x) = x^{2r+1} + x^{r-1} + 1 .$$

Mills and Zierler proved that, for $q = 2$, the degree of every irreducible factor of $F(x)$ over $GF(2)$ divides either $2n$ or $3n$. We shall show that, for arbitrary q, the degree of every irreducible factor of $F(x)$ over $GF(q)$ divides either $2n$ or $3n$.

We shall follow the notation of Mills and Zierler [1]. Put

$$K = GF(r) , \qquad L = GF(r^2) , \qquad M = GF(r^3) . \tag{1.1}$$

The identity

$$\begin{aligned}(x^{(2r+1)r} + x^{(r-1)r} + 1) - x^{r^2-r}(x^{2r+1} + x^{r-1} + 1) \\ = (x^{r^2-1} - 1)(x^{r^2+r+1} - 1)\end{aligned}$$

is easily verified. Since

$$(x^{2r+1} + x^{r-1} + 1)^r = x^{(2r+1)r} + x^{(r-1)r} + 1 ,$$

it is clear that

$$F^r(x) - x^{r^2-r}F(x) = (x^{r^2-1} - 1)(x^{r^2+r+1} - 1) . \tag{1.2}$$

Let $F(\alpha) = 0$, where α lies in some finite extension of $GF(q)$. Then by (1.2)

$$(\alpha^{r^2-1} - 1)(\alpha^{r^2+r+1} - 1) ,$$

so that either

$$\alpha^{r^2-1} - 1 = 0 \tag{1.3}$$

or

$$\alpha^{r^2+r+1} - 1 = 0 . \tag{1.4}$$

Clearly (1.4) implies

$$\alpha^{r^3-1} - 1 = 0 .$$

Hence α lies in either L or M.

Assume $\alpha \in K$. Then $\alpha^r = \alpha$, so that $F(\alpha) = 0$ reduces to