THE DEGREES OF THE FACTORS OF CERTAIN POLYNOMIALS OVER FINITE FIELDS

W. H. MILLS

ABSTRACT. Neal Zierler has discovered that the polynomial $x^{585}+x+1$ over GF(2) is the product of 13 irreducible factors of degree 45 and that the polynomial $x^{16513}+x+1$ over GF(2) is the product of 337 irreducible factors of degree 49. We prove a general theorem that includes these results, as well as some other well known results, as special cases.

Let K be a finite field containing exactly q elements. Let r be a power of q, say $r=q^n$. For any polynomial $f(x)=\sum a_ix^i$ over K we set

$$\hat{f}(x) = \sum a_i x^{(r^i-1)/(r-1)}$$

and

$$\hat{f}^\beta(x) = x\hat{f}(x^{r-1}) = \sum a_i x^{r^i}.$$

LEMMA 1 (ORE). *Let $A(x)$ and $B(x)$ be polynomials over K and set $C(x)=A(x)B(x)$. Then $C^\beta(x)=A^\beta(B^\beta(x))$.*

PROOF. Set $A(x)=\sum a_ix^i$ and $B(x)=\sum b_jx^j$. Then

$$\begin{aligned} A^\beta(B^\beta(x)) &= \sum_i a_i\Big(\sum_j b_j x^{r^j}\Big)^{r^i} \\ &= \sum_{i,j} a_i b_j x^{r^{i+j}} \\ &= C^\beta(x). \end{aligned}$$

THEOREM 1. *Let $f(x)$ and $g(x)$ be polynomials over K. Then $f(x)\mid g(x)$ if and only if $\hat{f}(x)\mid \hat{g}(x)$.*

PROOF. Suppose first that $f(x)\mid g(x)$ and set $g(x)=h(x)f(x)$. By Lemma 1 we have $g^\beta(x)=h^\beta(f^\beta(x))$. Since $x\mid h^\beta(x)$ this gives us $f^\beta(x)\mid g^\beta(x)$. Therefore we have $\hat{f}(x^{r-1})\mid \hat{g}(x^{r-1})$ which implies that $\hat{f}(x)\mid \hat{g}(x)$.

On the other hand suppose that $\hat{f}(x)\mid \hat{g}(x)$ and set $g(x)=A(x)+B(x)$, where $f(x)\mid A(x)$ and the degree of $B(x)$ is less than that of $f(x)$. By the first part of the proof we have $\hat{f}(x)\mid \hat{A}(x)$ so that

Received by the editors October 27, 1969.

AMS Subject Classifications. Primary 1225.

Key Words and Phrases. Factors of polynomials, polynomials over finite fields.

$$0 \equiv \hat{g}(x) = \hat{A}(x) + \hat{B}(x) \equiv \hat{B}(x) \pmod{\hat{f}(x)}.$$

Now the degree of $\hat{B}(x)$ is less than that of $\hat{f}(x)$, so that $\hat{B}(x)=0$ and $B(x)=0$. Therefore we have $f(x) \mid g(x)$.

THEOREM 2. *Suppose $f(x) \mid x^N-1$ and let d be a factor of $r-1$. Then the degree of every irreducible factor of $\hat{f}(x^d)$ over K divides nN.*

PROOF. By Theorem 1 we have $\hat{f}(x) \mid x^{(r^N-1)/(r-1)}-1$. This is equivalent to $\hat{f}(x^d) \mid x^{d(r^N-1)/(r-1)}-1$. Since $d \mid r-1$ this implies that $\hat{f}(x^d) \mid x^{r^N-1}-1$. Therefore every root of $\hat{f}(x^d)$ lies in GF(r^N). Since $r^N=q^{nN}$ this implies that the degree of every irreducible factor of $\hat{f}(x^d)$ over K divides nN.

COROLLARY. *If $r=q^n$, then the degree of every irreducible factor of $x^{1+r}+x+1$ over* GF(q) *divides $3n$.*

This corollary is the special case of Theorem 2 with $f(x)=x^2+x+1$, $N=3$, and $d=1$. It is well known and proofs have been given by a number of authors. See [1, p. 93].

Using Theorem 2 we can obtain many other results of the same nature. For example, since x^3+x+1 divides x^7-1 over GF(2) we see that if $r=2^n$, then the degree of every irreducible factor of $x^{1+r+r^2}+x+1$ over GF(2) divides $7n$.

Similarly if $r=2^n$, then the degree of every irreducible factor of $x^{1+r+r^2+r^3}+x+1$ over GF(2) divides $15n$.

When certain additional conditions are satisfied the degrees of the irreducible factors of $\hat{f}(x^d)$ are all equal to nN. To show this we need the following result.

LEMMA 2. *Let $f(x)$ be an irreducible polynomial over K, and let $g(x)$ be an arbitrary polynomial over K. Suppose for some positive integer d, $\hat{f}(x^d)$ and $\hat{g}(x^d)$ have a root in common. Then $f(x) \mid g(x)$.*

PROOF. Let $h(x)$ be the greatest common divisor of $\hat{f}(x^d)$ and $\hat{g}(x^d)$. Then $h(x)$ is not a constant. Let $\mathfrak{a}$ be the set of all polynomials $A(x)$ over K such that $h(x) \mid \hat{A}(x^d)$. Using Theorem 1 we see that $\mathfrak{a}$ is an ideal in the principal ideal ring $K[x]$. Since $f(x) \in \mathfrak{a}$, $1 \notin \mathfrak{a}$, and $f(x)$ is irreducible, it follows that $\mathfrak{a}$ consists of precisely the multiples of $f(x)$. Since $g(x) \in \mathfrak{a}$, we have $f(x) \mid g(x)$ and the proof is complete.

Theorem 1 and Lemma 2 are closely related to results of Zierler [3].

THEOREM 3. *Let $f(x)$ be an irreducible polynomial over K with period N. Let d be a factor of $r-1$ and set $r-1=de$. Suppose that $(e, dN)=1$ and that every prime factor of n is also a factor of N. Then every irreducible factor of $\hat{f}(x^d)$ over K has degree nN.*

PROOF. Since $f(x) \mid x^N - 1$ it follows from Theorem 1 that

$$\hat{f}(x) \mid x^{(r^N-1)/(r-1)} - 1.$$

Replacing x by x^d we obtain $\hat{f}(x^d) \mid x^{(r^N-1)/e} - 1$. Let α be a root of $\hat{f}(x^d)$. Then we have $\alpha^{(r^N-1)/e} = 1$ and $\alpha \in \mathrm{GF}(r^N)$. Now $r \equiv 1 \pmod{e}$ and therefore

$$\begin{aligned}(r^N - 1)/e &= d(r^N - 1)/(r - 1) \\ &= d(r^{N-1} + r^{N-2} + \cdots + r + 1) \\ &\equiv dN \pmod{e}.\end{aligned}$$

Since $(e, dN) = 1$ it follows that e is relatively prime to the order of α. Let m be the degree of α over $\mathrm{GF}(r)$. Then $m \mid N$ and $\alpha^{r^m-1} = 1$. Since e is relatively prime to the order of α we have

$$1 = \alpha^{(r^m-1)/e} = \alpha^{d(r^m-1)/(r-1)}.$$

This gives us $\hat{B}(\alpha^d) = 0$ where $B(x) = x^m - 1$. Thus $\hat{f}(x^d)$ and $\hat{B}(x^d)$ have a root in common. By Lemma 2 we have $f(x) \mid B(x)$. Since N is the period of $f(x)$ this gives us $N \mid m$, and therefore $m = N$.

Now let M be the degree of α over K. Then $M \mid nN$. Suppose $M < nN$. Then for some prime λ we have $\lambda M \mid nN$. Since every prime factor of n is also a factor of N we have $\lambda \mid N$. Thus α is contained in a field of degree $n(N/\lambda)$ over K. This field has degree N/λ over $\mathrm{GF}(r)$, which implies that $m < N$, a contradiction. Therefore we have $M = nN$. Since α was an arbitrary root of $\hat{f}(x^d)$ it follows that every irreducible factor of $\hat{f}(x^d)$ over K has degree nN, and the proof is complete.

Setting $d = r - 1$ and $e = n = 1$ in Theorem 3 we obtain the following result:

COROLLARY 1. (*Zierler's generalization of the theorem of Ore, Gleason, and Marsh.*) *Let $f(x)$ be an irreducible polynomial over* $\mathrm{GF}(q)$, *say $f(x) = \sum a_i x^i$. Let N be the period of $f(x)$. Then every irreducible factor of $\sum a_i x^{q^i-1}$ over* $\mathrm{GF}(q)$ *has degree N.*

We observe that $x^2 + x + 1$ is irreducible over $\mathrm{GF}(q)$ if and only if $q \equiv 2 \pmod 3$. Thus setting $d = 1$, $n = 3^s$, $f(x) = x^2 + x + 1$, and $N = 3$ we obtain the following special case of Theorem 3:

COROLLARY 2. *If $q \equiv 2$* (mod 3), *$n = 3^s \geqq 1$, $r = q^n$, and $d = 1$, then every irreducible factor of $x^{1+r} + x + 1$ over* $\mathrm{GF}(q)$ *has degree $3n$.*

Setting $q = 2$, $n = 7^s$, $d = 1$, $f(x) = x^3 + x + 1$, and $N = 7$ in Theorem 3 we obtain the following result:

COROLLARY 3. *If* $n=7^s\geqq 1$ *and* $r=2^n$, *then the degree of every irreducible factor of* $x^{1+r+r^2}+x+1$ *over* GF(2) *is* $7n$.

For example, $x^{16513}+x+1$ is the product of 337 irreducible factors over GF(2), each of which has degree 49.

Similarly, setting $q=2$, $n=3^s5^t$, $d=1$, $f(x)=x^4+x+1$, and $N=15$ we obtain this result:

COROLLARY 4. *If* $n=3^s5^t\geqq 1$ *and* $r=2^n$, *then every irreducible factor of* $x^{1+r+r^2+r^3}+x+1$ *over* GF(2) *has degree* $15n$.

For example, $x^{585}+x+1$ is the product of 13 irreducible factors of degree 45 over GF(2).

REFERENCES

1. Solomon W. Golomb, *Shift register sequences*, Holden-Day, San Francisco, Calif., 1967.

2. Oystein Ore, *Contributions to the theory of finite fields*, Trans. Amer. Math. Soc. **36** (1934), 243–274.

3. Neal Zierler, *On the theorem of Gleason and Marsh*, Proc. Amer. Math. Soc. **9** (1958), 236–237.

INSTITUTE FOR DEFENSE ANALYSES, PRINCETON, NEW JERSEY 08540