Let $K$ be a field with a finite number $q$ of elements and let $\alpha$ be the mapping of $K[x]$ in itself that assigns

$$f^\alpha(x) = \sum_{i=0}^{n} f_i x^{q^i-1}$$

as image to

$$f(x) = \sum_{i=0}^{n} f_i x^i.$$

The order of a nonzero element $a$ of a finite field is the smallest of the positive integers $j$ for which $a^j = 1$. If $f(x)$ is irreducible over $K$, then all of its roots are of the same order, for given any two roots of $f$ lying in a finite extension $F$ of $K$ there is always an automorphism of $F$ mapping one on the other. We may therefore define the order of the irreducible polynomial $f$ to be the order of any one of its roots. The purpose of this note is to establish the following generalization of the theorem of Gleason and Marsh.3

**Theorem.** Let $f$ be an irreducible member of $K[x]$. Then the degree of every irreducible factor of $f^\alpha$ is equal to the order of $f$.

**Proof.** Let $\beta$ be the mapping of $K[x]$ in itself such that $g^\beta(x) = xg^\alpha(x) = \sum_{i=0}^{n} g_i x^{q^i}$. Clearly $\beta$ is linear over $K$; that is, if $g$ and $h$ are in $K[x]$ and $a$ and $b$ are in $K$ then $(ag + bh)^\beta = ag^\beta + bh^\beta$.

Let $g \in K[x]$. Then $(xg(x))^\beta = \sum g_i x^{q^i+1} = \left( \sum g_i x^{q^i} \right)^q = (g^\beta(x))^q$. That is,

$$1. \quad (xg)^\beta = g^{\beta q}.$$

Let $f$, $g$ and $a$ be in $K[x]$ and suppose $g = af$. Then $g^\beta(x) = (\sum a_i f^i(x))^\beta = \sum a_i (x^i f(x))^\beta = \sum a_i f^\beta(x)^q$ by (1). Thus, $f^\beta | g^\beta$ and so $f^\alpha | g^\alpha$. This proves

$$2. \quad f | g \text{ implies } f^\alpha | g^\alpha.$$
Now let $f$ be irreducible, let $g$ be arbitrary and let $h$ be a factor of $f^a$ of positive degree. We shall show that

$$h | g^a \implies f | g.$$  

Let $A = \{ b \in K[x] : h | b^a \}$. If $b \in A$ and $a \in K[x]$, $b^a | (ab)^a$ by (2) and so $ab \in A$. It follows easily that $A$ is an ideal containing $f$ but not 1 in $K[x]$. Hence, since $f$ is irreducible and $K[x]$ is a principal ideal domain, $A = (f)$ and (3) is established.

Now let $f$ be irreducible of order $r$ and let $d$ be the degree of an irreducible factor $h$ of $f^a$. Then $f | 1 - x^r$ and it follows from (2) that $h | 1 - x^{q^d - 1}$. Hence a splitting field of $h$, which has $q^d$ elements, may be regarded as a subfield of a splitting field of $1 - x^{q^d - 1}$, which has $q^r$ elements, and so $d | r$. On the other hand, $h | 1 - x^{q^d - 1}$ implies $f | 1 - x^d$ by (3) and hence $r | d$. It follows now that $d = r$ and the proof of the theorem is complete.

**Corollary (Gleason-Marsh).** Let $f$ be an irreducible polynomial of degree $n$ over $K$. The order of $f$ is $q^n - 1$ if and only if $f^a$ is irreducible.

*Massachusetts Institute of Technology*