ON THE THEOREM OF GLEASON AND MARSH[1]

NEAL ZIERLER[2]

Let K be a field with a finite number q of elements and let α 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^{α} is equal to the order of f.*

PROOF. Let β 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 β 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 $(xg(x))^{\beta} = \sum g_i x^{q^{i+1}} = (\sum g_i x^{q^i})^q = (g^{\beta}(x))^q$. That is,

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

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

$$(2) \qquad f \mid g \text{ implies } f^{\alpha} \mid g^{\alpha}.$$

Received by the editors August 12, 1957.

[1] The research in this document was supported jointly by the Army, Navy, and Air Force under contract with the Massachusetts Institute of Technology.

[2] Staff Member, Lincoln Laboratory, Massachusetts Institute of Technology.

[3] A. A. Albert, *Fundamental concepts of higher algebra*, University of Chicago Press, 1956, p. 132.

Now let f be irreducible, let g be arbitrary and let h be a factor of f^α of positive degree. We shall show that

$$h \mid g^\alpha \text{ implies } f \mid g. \tag{3}$$

Let $A = \{b \in K[x]: h \mid b^\alpha\}$. If $b \in A$ and $a \in K[x]$, $b^\alpha \mid (ab)^\alpha$ 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^α. Then $f \mid 1 - x^r$ and it follows from (2) that $h \mid 1 - x^{q^r - 1}$. Hence a splitting field of h, which has q^d elements, may be regarded as a subfield of a splitting field of $1 - x^{q^r - 1}$, which has q^r elements, and so $d \mid r$. On the other hand, $h \mid 1 - x^{q^d - 1}$ implies $f \mid 1 - x^d$ by (3) and hence $r \mid d$. 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^α is irreducible.*

MASSACHUSETTS INSTITUTE OF TECHNOLOGY