The group membership of a polynomial in an element algebraic over a field

By W. E. BARNES and H. SCHNEIDER in Pullman (Wash.)

Let F be a field, R an arbitrary extension ring of F, and let a be an element of R algebraic over F. Let $q(x)$ be a polynominal in an indeterminate x with coefficients in F. If there exists a subgroup of the multiplicative semi-group of R to which $q(a)$ belongs, we shall call $q(a)$ a *group-element* in R. FARAHAT and MIRSKY [1] have recently proved that the minimum polynominal of a matrix A of order n with elements in the complex field C has simple zeros (and hence that A is diagonable) if and only if, for every irreducible polynomial $q(x) = x - \omega$ in $C[x]$, $q(A)$ is a group-element in the ring of all n-th order matrices with elements in C. Our theorem 2 is a generalization of this result; however we are chiefly interested in finding a condition for $q(a)$ to be group-element in R for given polynomial $q(x)$.

Since a is assumed to be algebraic over F, the ideal of polynomials in $F[x]$ for which $p(a) = 0$ has a non-zero generator $m(x)$, which we shall call the minimum polynomial of a. By $(p(x), m(x))$ we shall denote the greatest common divisor of $p(x)$ and $m(x)$ in $F[x]$. Lemma 1 is related to some familiar results on principal ideal rings.

Lemma 1. *Let a be an element of R algebraic over F with minimum polynomial $m(x)$, and let $q(x)$ be a polynomial in $F[x]$. Then there exists an r in R such that*

$$r q(a)^{\varrho} = q(a)^{\varrho-1} \tag{1}$$

if and only if

$$(q(x)^{\varrho}, m(x)) = (q(x)^{\varrho-1}, m(x)) \tag{2}$$

in which case there is an r in $F[a]$ satisfying (1).

Proof. We set $d_\sigma(x) = (q(x)^{\sigma}, m(x)), \sigma = \varrho - 1, \varrho$, which of course implies that $d_{\varrho-1}(x)$ divides $d_\varrho(x)$. Suppose that $q(x)^\varrho \lambda(x) = q(x)^\varrho m(x)/d_\varrho(x)$ is the least common multiple of $q(x)^\varrho$ and $m(x)$. Thus $q(a)^\varrho \lambda(a) = 0$ and hence if (1) holds $q(a)^{\varrho-1} \lambda(a) = 0$.

We deduce that there is a polynomial $\mu(x)$ for which

$$q(x)^{\varrho-1} m(x)/d_\varrho(x) = m(x) \mu(x)$$

and we may now conclude that $d_\varrho(x)$ divides $q(x)^{\varrho-1}$, and therefore also $d_{\varrho-1}(x)$. We have proved that $d_{\varrho-1}(x) = d_\varrho(x)$.

Conversely assume that (2) holds. There are polynomials $\nu'(x)$ and $\tau'(x)$ such that

$$\nu'(x) q(x)^\varrho + \tau'(x) m(x) = d_\varrho(x) = d_{\varrho-1}(x)$$

whence

$$\nu(x)\, q(x)^{\varrho} + \tau(x)\, m(x) = q(x)^{\varrho-1}$$

for suitable $\nu(x)$ and $\tau(x)$. It follows that

$$\nu(a)\, q(a)^{\varrho} = q(a)^{\varrho-1}$$

and the lemma is proved since $\nu(a)$ lies in $F[a]$.

Lemma 2. *The polynomial $q(a)$ is a group-element of R if and only if*

$$r\, q(a)^2 = q(a) \tag{3}$$

for some r in R.

Proof. The condition is clearly necessary. If (3) is satisfied, then by lemma 1, we may assume that r lies in $F[a]$, and so commutes with $q(a)$. We set $b = q(a)$, $e = rb$ $c = r^2 b$. It is easily verified that $be = b$, $e^2 = e$, $ce = c$, and $bc = e$. Hence the semi-group generated by b and c in $F[a]$ is a group.

Combining lemmas 1 and 2 we obtain:

Theorem 1. *Let a be an element of the extension ring R of F, which is algebraic over F with minimum polynomial $m(x)$, and let $q(x)$ be a polynomial in $F[x]$. Then $q(a)$ is a group-element in R if and only if*

$$(q(x)^2, m(x)) = (q(x), m(x)), \tag{4}$$

in which case $q(a)$ is a group-element even in $F[a]$.

Thus $q(a)$ is a group-element in R if and only if it is a group-element in $F[a]$. We may note that if c is transcendental over F, then c is a group-element in $F(c)$, but not in $F[c]$.

Corollary. *There is a power of a which is a group-element in R.*

Proof of Corollary. Let x^{ϱ} be the highest power of x dividing $m(x)$. If $\sigma \geqq \varrho$, then $(x^{\varrho}, m(x)) = (x^{2\sigma}, m(x)) = x^{\varrho}$ whence a^{σ} is a group-element in R.

In the case of matrices with complex elements, this corollary was proved by Ranum [2]. We may add that it holds for matrices in any division ring, being a consequence of the decomposition of such a matrix into the direct sum of a non-singular and a nilpotent matrix.

It is easily seen that (4) holds for every polynomial $q(x)$ in $F[x]$ if and only if the irreducible factors of $m(x)$ are simple. Thus we have:

Theorem 2. *Let a be an element of the extension ring R of the field F, which is algebraic over F with minimum polynomial $m(x)$. Then $q(a)$ is a group-element in R for every polynomial $q(x)$ in $F[x]$ if and only if the irreducible factors of $m(x)$ are simple.*

Evidently in theorem 2 we could have put "every irreducible polynomial" for "every polynomial", and so our theorem includes that of Farahat and Mirsky [1].

As is known, the algebra $F[a]$ is semi-simple if and only if the irreducible factors of $m(x)$ are simple. Thus:

Corollary to theorem 2. *The algebra $F[a]$ is semi-simple if and only if $q(a)$ is a group-element in R for every $q(x)$ in $F[x]$.*

Theorem 2 and its corollary may also be derived from the decomposition of $F[a]$ (which is, of course, isomorphic to $F[x]/(m(x))$) into a direct sum of fields and primary rings; for each summand is a field if and only if the irreducible factors of $m(x)$ are simple.

Finally, we shall consider a slightly more general situation. Let I be a commutative principal ideal domain, $a \to a'$ a homomorphism of I onto I' with non-zero kernel (m), and let R be an arbitrary extension ring of I'. It is readily seen that all our results and their proofs apply to this situation. Thus the element q' of I' is a group-element in R if and only if $(q, m) = (q^2, m)$ in I (i. e. if and only if the homomorphic images of the ideals (q) and (q^2) are equal), in which case q' is a group-element even in I'. The assumption that $(m) \neq 0$ is essential to this result. For let I be the ring of integers and set $I = I'$. Then 3 is a group-element in $R = I\,[1/3]$ but not in I itself. This raises the question under which conditions an element of a ring S is a group-element in S if it is a group-element in an extension ring R.

References

[1] H. K. FARAHAT and L. MIRSKY, A condition for diagonability of matrices. Amer. Math. Monthly **63**, 410—412 (1956).

[2] A. RANUM, The group membership of singular matrices. Amer. J. Math. **31**, 18—41 (1909).

Eingegangen am 19.1.1957