NEW PROOFS FOR TWO THEOREMS OF CAPELLI

Elizabeth Rowlinson

(received November 18, 1963)

The following two theorems are due to Capelli.

THEOREM 1. Let $g(x)$ and $h(x)$ be polynomials over a field R of characteristic 0; let $f(x) = g(h(x))$. Then $f(x)$ is irreducible over R if and only if

(i) $g(x)$ is irreducible over R

and

(ii) $h(x) - \beta$ is irreducible over $R(\beta)$, where β is a root of $g(x)$.

THEOREM 2. Let $f(x)$, $g(x)$, $h(x)$, $g_1(x)$, $h_1(x)$ be polynomials over a field R of characteristic 0 such that

(i) $f(x) = g(h(x)) = g_1(h_1(x))$

and

(ii) the degrees of $g(x)$, $h(x)$, $g_1(x)$, $h_1(x)$ are m, n, n, m respectively, where $(m, n) = 1$.

Then $f(x)$ is irreducible over R if and only if both $g(x)$ and $g_1(x)$ are irreducible over R.

These theorems are proved in [1], pp. 288-291; the following proofs are somewhat simpler.

Canad. Math. Bull. vol. 7, no. 3, July 1964.

Proof of theorem 1. Let $g(x)$ and $h(x)$ have degrees m and n respectively. Then $f(x)$ has degree mn. Let α be a root of $h(x) - \beta$; since $\beta = h(\alpha)$ we have $R(\alpha, \beta) = R(\alpha)$. Hence by [2] p. 103,

$$(1) \qquad [R(\alpha): R] = [R(\alpha, \beta): R] = [R(\alpha, \beta): R(\beta)]\,[R(\beta): R] .$$

Also, α satisfies $f(\alpha) = g(h(\alpha)) = g(\beta) = 0$.

(a) Suppose that conditions (i) and (ii) are satisfied. Since $g(x)$ is irreducible over R, $[R(\beta): R] = m$; since $h(x) - \beta$ is irreducible over $R(\beta)$, $[R(\alpha, \beta): R(\beta)] = n$. Thus, from (1), $[R(\alpha): R] = mn$. But $f(x)$ is of degree mn and has the root α; it is therefore the minimum polynomial of α, or a constant multiple of it, and so is irreducible over R.

(b) Suppose that $f(x)$ is irreducible. Then $g(x)$ is irreducible. For if it is reducible, we have $g(x) = g_1(x)g_2(x)$ (degree $g_i(x) > 0$, $i = 1, 2$) and so

$$f(x) = g(h(x)) = g_1(h(x))\, g_2(h(x)) = f_1(x)f_2(x) \qquad (\text{degree } f_i(x) > 0,\ i = 1, 2),$$

which contradicts the supposition that $f(x)$ is irreducible.

Since $f(x)$ is irreducible, $[R(\alpha): R] = mn$; since $g(x)$ is irreducible $[R(\beta): R] = m$. Thus from (1) $[R(\alpha, \beta): R(\beta)] = n$. $h(x) - \beta$ is therefore the minimum polynomial of α over $R(\beta)$, or a constant multiple of it, and so is irreducible over $R(\beta)$.

Proof of theorem 2. (a) Suppose that $g(x)$ and $g_1(x)$ are both irreducible. Let α be a root of $f(x)$; let $h(\alpha) = \beta$ and $h_1(\alpha) = \beta_1$. Then $g(\beta) = g_1(\beta_1) = 0$. Since $g(x)$ and $g_1(x)$ are irreducible, $[R(\beta): R] = m$ and $[R(\beta_1): R] = n$. Let $[R(\alpha, \beta): R(\beta)] = a$; since α is a root of $h(x) - \beta$, we conclude that $a \mid n$. As we have again $\beta = h(\alpha)$, equation (1) holds. Thus $[R(\alpha): R] = am$. Similarly, if $[R(\alpha, \beta_1): R(\beta_1)] = a_1$, $[R(\alpha): R] = a_1 n$ and therefore $a_1 \mid m$. So $am = a_1 n$; since $(m, n) = 1$, it follows that $m \mid a_1$ and $n \mid a$. Therefore $m = a_1$, $n = a$, and $[R(\alpha, \beta): R(\beta)] = a = n$, so that $h(x) - \beta$

https://doi.org/10.4153/CMB-1964-042-9 Published online by Cambridge University Press

is the minimum polynomial of α over $R(\beta)$ or a constant multiple of it. $h(x) - \beta$ is therefore irreducible over $R(\beta)$, and by theorem 1 $f(x)$ is irreducible.

(b) Suppose that $f(x)$ is irreducible. By theorem 1, $g(x)$ and $g_1(x)$ are both irreducible.

REFERENCES

1. N. Tschebotaröw and H. Schwerdtfeger, Grundzüge der Galois'schen Theorie, Noordhoff, Groningen (1950).

2. B. L. Van der Waerden, Modern Algebra, Vol. I, Ungar (1953).

McGill University

https://doi.org/10.4153/CMB-1964-042-9 Published online by Cambridge University Press