THE 'ODD' NUMBER SIX

By J. A. TODD

Received 7 July 1944

1. A few months ago, in the course of teaching an elementary class, I had occasion to discuss problems of the familiar type, 'if α, β, γ are the roots of the equation $x^3+qx+r=0$, form the equation whose roots are $\alpha^2+\beta\gamma, \beta^2+\gamma\alpha, \gamma^2+\alpha\beta$'. After I had explained the device of replacing $\beta\gamma$ by $\alpha\beta\gamma/\alpha = -r/\alpha$, so that the roots of the new equation are the same rational function of the separate roots of the original equation, I was asked 'whether such a transformation was always possible'. On investigation the answer to the question proved to be a surprising one.

2. The general problem suggested by the question is fairly obvious, though it requires a little care in its enunciation. Let us suppose that $a_1, a_2, \ldots, a_n$ are independent indeterminates and that

$$f(x) \equiv x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n. \tag{1}$$

Let $\mathbf{K}(a_1, a_2, \ldots, a_n)$ be the field obtained by adjoining $a_1, \ldots, a_n$ to the field $\mathbf{K}$ of complex numbers. Then there is an algebraic extension $\mathbf{K}^*$ of $\mathbf{K}(a_1, a_2, \ldots, a_n)$ in which the right-hand member of (1) breaks up into the product of n factors, so that

$$f(x) \equiv \prod_{i=1}^{n} (x-\alpha_i), \tag{2}$$

where $\alpha_i \subset \mathbf{K}^*$; and any rational symmetric function of $\alpha_1, \alpha_2, \ldots, \alpha_n$ with coefficients in $\mathbf{K}$ belongs to $\mathbf{K}(a_1, a_2, \ldots, a_n)$.

Suppose now that $\phi_1(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is a rational function of $\alpha_1, \alpha_2, \ldots, \alpha_n$, with coefficients in $\mathbf{K}$, with the property that, when $\alpha_1, \alpha_2, \ldots, \alpha_n$ undergo the $n!$ permutations of the symmetric group Σ_n of degree n, exactly n distinct functions $\phi_1, \phi_2, \ldots, \phi_n$ are obtained. Then, since the elementary symmetric functions of $\phi_1, \phi_2, \ldots, \phi_n$ are rational symmetric functions of $\alpha_1, \alpha_2, \ldots, \alpha_n$, the equation whose roots are $\phi_1, \phi_2, \ldots, \phi_n$ has its coefficients in $\mathbf{K}(a_1, a_2, \ldots, a_n)$. We now propose the following question: *If $\phi_1, \phi_2, \ldots, \phi_n$ are n rational functions of $\alpha_1, \alpha_2, \ldots, \alpha_n$ with coefficients in* $\mathbf{K}$, *which are all distinct and which are permuted transitively by the $n!$ permutations of $\alpha_1, \alpha_2, \ldots, \alpha_n$, is it possible to choose the suffixes of $\phi_1, \phi_2, \ldots, \phi_n$ in such an order that $\phi_r = \phi(\alpha_r)$, where ϕ is a rational function with coefficients in* $\mathbf{K}(a_1, a_2, \ldots, a_n)$?

3. The question is evidently one of pure group theory; and we shall see immediately that it is answered by the following known theorem†:

The symmetric group of degree n ($n \neq 6$) contains n and only n subgroups of order $(n-1)!$, which form a single conjugate set. The symmetric group of degree 6 *contains* 12 *subgroups*

† Burnside, *Theory of Groups of Finite Order*, 2nd ed. (Cambridge, 1911), p. 209.

https://doi.org/10.1017/S0305004100022374 Published online by Cambridge University Press

of order 5!, *which are simply isomorphic with one other and form two conjugate sets of* 6 *each.*

To see that this theorem answers the question just raised, we observe that those permutations of $\alpha_1, \alpha_2, \ldots, \alpha_n$ which keep ϕ_1 fixed form a subgroup of index n in Σ_n, so that the order of this subgroup is $(n-1)!$. Hence, if $n \neq 6$, this subgroup must consist of the set of permutations of $\alpha_1, \alpha_2, \ldots, \alpha_n$ which keep one symbol (say α_1) fixed. Therefore ϕ_1 is a symmetric function of $\alpha_2, \ldots, \alpha_n$, and can be expressed rationally in terms of the elementary symmetric functions of $\alpha_2, \ldots, \alpha_n$, the coefficients of these symmetric functions being in the field $\mathbf{K}(\alpha_1)$. But the elementary symmetric functions of $\alpha_2, \ldots, \alpha_n$ can be expressed rationally in terms of $a_1, a_2, \ldots, a_n$ and α_1. Hence ϕ_1 is a rational function of α_1 with coefficients in $\mathbf{K}(a_1, a_2, \ldots, a_n)$. On the other hand, if $n = 6$ this need not be the case, since the permutations of $\alpha_1, \alpha_2, \ldots, \alpha_n$ which leave ϕ_1 invariant may form a subgroup belonging to the second conjugate set (the first set consisting of the subgroups keeping one of the α_i unchanged).

4. The interest of this rather trivial theorem, of course, centres entirely around the anomalous case $n = 6$; and this anomaly arises from the exceptional property of the symmetric group of degree 6 implied by the theorem quoted in the last section. It may, therefore, not be amiss to point out that this theorem is at bottom the explanation of another curious phenomenon associated with the number 6, which arises in some well-known geometrical configurations. This is the fact that the fifteen pairs ij formed by two out of six symbols 1, 2, ..., 6 can be arranged in fifteen ways in sets (such as 12, 34, 56) of three pairs containing between them all six symbols, and that these fifteen sets can be arranged in six ways in sets of five, so that each set of five contains all the fifteen pairs.† These sets are‡

I (14, 25, 36) (16, 24, 35) (13, 26, 45) (12, 34, 56) (15, 23, 46);

II (14, 25, 36) (15, 26, 34) (12, 35, 46) (16, 23, 45) (13, 24, 56);

III (16, 24, 35) (15, 26, 34) (14, 23, 56) (13, 25, 46) (12, 36, 45);

IV (13, 26, 45) (12, 35, 46) (14, 23, 56) (15, 24, 36) (16, 25, 34);

V (12, 34, 56) (16, 23, 45) (13, 25, 46) (15, 24, 36) (14, 26, 35);

VI (15, 23, 46) (13, 24, 56) (12, 36, 45) (16, 25, 34) (14, 26, 35).

The point to be observed is that the 6! permutations of the symbols 1, 2, ..., 6 effect the 6! permutations of the sets I, II, ..., VI. But those permutations which keep 1 unaltered form a subgroup which is transitive on the sets I, II, ..., VI, since the two permutations (23), (24) effect the respective permutations (I, VI) (II, V) (III, IV) and (I, III) (II, VI) (IV, V). Thus we have a representation of the two conjugate sets of subgroups of index 6 in Σ_6, one such set consisting of the subgroups keeping one of the

† Sylvester, *Collected Papers*, 1, p. 92. See, e.g., Baker, *Principles of Geometry*, 2 (Cambridge, 1922), p. 221, and some remarks by Room, *Geometry of Determinantal Loci* (Cambridge, 1938), p. 301.

‡ Baker, loc. cit.

https://doi.org/10.1017/S0305004100022374 Published online by Cambridge University Press

symbols 1, 2, ..., 6 unchanged, and the other consisting of the subgroups keeping one of the sets I, II, ..., VI unchanged.

We may remark, finally, that this arrangement of triads of pairs of symbols enables us to construct six rational functions of $\alpha_1, \alpha_2, \ldots, \alpha_6$ which are permuted among themselves transitively by the permutations of Σ_6 but cannot be expressed as rational functions of a single one of the α's. Thus we may take

$$\phi_{\mathrm{I}} = (\alpha_1\alpha_4+\alpha_2\alpha_5+\alpha_3\alpha_6)(\alpha_1\alpha_6+\alpha_2\alpha_4+\alpha_3\alpha_5)(\alpha_1\alpha_3+\alpha_2\alpha_6+\alpha_4\alpha_5)$$
$$(\alpha_1\alpha_2+\alpha_3\alpha_4+\alpha_5\alpha_6)(\alpha_1\alpha_5+\alpha_2\alpha_3+\alpha_4\alpha_6)$$

and $\phi_{\mathrm{II}}, \ldots, \phi_{\mathrm{VI}}$ as the similar expressions obtained from II, ..., VI. The construction, in terms of $a_1, \ldots, a_6$, of the equation satisfied by $\phi_{\mathrm{I}}, \ldots, \phi_{\mathrm{VI}}$ appears formidable!

Trinity College
Cambridge

EXPANSIONS OF COORDINATES OF POINTS OF A PLANE CURVE IN TERMS OF s OR ψ

By H. T. H. PIAGGIO

Received 18 July 1944

If O is an ordinary point of a plane curve and the tangent and inward normal at O are taken as axes, then, under certain conditions, the coordinates x and y of a neighbouring point P on the curve can be expanded in powers of s, the arc OP, or of ψ, the angle between the tangents at O and P. Lamb(3) gives these expansions as far as the terms in s^4 and ψ^3. Dockeray(1) goes as far as the terms in s^6, but there seem to be three errors in his results. No one, I believe, has given the general terms. I obtain these for both pairs of expansions. Fowler(2) gives the term in s^{2r+1} in the expansion of x in the special case where, owing to the vanishing of the curvature and of its first $r-2$ derivatives, the expansion of y begins with the term in s^{r+1}. I shall give reasons for disagreeing with this result.

Expansions in terms of ψ. Use the suffix r to denote the result of differentiating r times with respect to ψ and then putting $\psi = 0$. Since

$$\frac{d(x+iy)}{d\psi} = \frac{ds}{d\psi}\frac{d(x+iy)}{ds} = \rho(\cos\psi + i\sin\psi) = \rho e^{i\psi};$$

$$\frac{d^{n+1}(x+iy)}{d\psi^{n+1}} = e^{i\psi}\sum_{k=0}^{n}\binom{n}{k} i^k \frac{d^{n-k}\rho}{d\psi^{n-k}},$$

and so

$$x_{n+1} + iy_{n+1} = \sum_{k=0}^{n}\binom{n}{k} i^k \rho_{n-k}.$$

Hence

$$x_{n+1} = \rho_n - \binom{n}{2}\rho_{n-2} + \ldots + (-)^l\binom{n}{2l}\rho_{n-2l} + \ldots,$$

and

$$y_{n+1} = n\rho_{n-1} - \binom{n}{3}\rho_{n-3} + \ldots + (-)^l\binom{n}{2l+1}\rho_{n-2l-1} + \ldots.$$

https://doi.org/10.1017/S0305004100022374 Published online by Cambridge University Press