A Note on Resultants of Equations in a Cyclic Number System

By R. Wilson, University College, Swansea.

(*Received* 14*th September*, 1931. *Read* 6*th November*, 1931.)

§ 1. *Introduction.* Little is known concerning the theory of resultants of equations other than in the complex number system. The cyclic number systems provide a simple example which is not a division algebra. In such a system with n units e_r any number $y \equiv y_0 + y_1 e_1 + y_2 e_2 + \ldots + y_{n-1} e_{n-1}$ has coefficients y_r drawn from a field, and the units satisfy the product law:

$$e_s e_t = e_{s+t}, \quad (s+t<n); \quad e_s e_t = e_{s+t-n}, \quad (s+t \geqslant n); \quad e_0 = 1.$$

Divisors of zero, for which $N(y) = 0$, satisfy one or more of the n conditions

$$Y_s \equiv y_0 + \omega_s y_1 + \omega_s^2 y_2 + \ldots + \omega_s^{n-1} y_{n-1} = 0, \quad (s = 0, 1, 2, \ldots, n-1), \qquad (1)$$

where $\omega_s^n = 1$.

§ 2. *The Equation of Degree* m. In this system the equation of degree m,

$$ax^m + bx^{m-1} + \ldots + hx + k = 0, \qquad (2)$$

can be resolved into the system of n simultaneous equations

$$A_s X_s^m + B_s X_s^{m-1} + \ldots + H_s X_s + K_s = 0, \quad (s = 0, 1, 2, \ldots, n-1), \qquad (3)$$

over the field; for the units e_t are simply isomorphic with any set ω_s^t, $(t = 0, 1, 2, \ldots, n-1)$, ordered suitably, and substitution in (2), with $s = 0, 1, 2, \ldots, n-1$, in turn, results in equations (3).

In general there are m^n solutions of (3) and hence of (2), of which at most m are independent and of which some may be repeated. The following exceptions arise:

If $N(a) = 0$, one or more of (3), according to the number of conditions (1) satisfied by a, is reduced in degree, the defect depending on how many of the sequence $b, c, \ldots$ are divisors of zero satisfying one or more of the same conditions as a.

If all the coefficients except k are divisors of zero satisfying at least one of the same conditions, then unless $k = 0$, equations (3) are inconsistent and (2) has no solution.

If all the coefficients are divisors of zero satisfying at least one common condition, then at least one of equations (3) vanishes identically, and the corresponding X_s, being arbitrary, introduce arbitrary constants into the solutions of (2).

If $N(k) = 0$ and k satisfies one or more conditions not satisfied by every other coefficient, then $N(x) = 0$ and x satisfies those conditions. Conversely if solutions exist which are divisors of zero, k must be a divisor of zero also and satisfy the same conditions at least.

§ 3. *Resultants and Discriminants.* Since the cyclic number system is not a division algebra, Euclid's algorithm does not hold and the theory of resultants suffers a consequent modification.

In the cyclic system consider two equations

$$ax^m + bx^{m-1} + \ldots + hx + k = 0, \quad a'x^{m'} + b'x^{m'-1} + \ldots + h'x + k' = 0. \quad (4)$$

Each is reducible as in § 2 to a set of n simultaneous equations

$$\begin{gathered} A_s X_s^m + B_s X_s^{m-1} + \ldots + H_s X_s + K_s = 0, \\ A'_s X_s^{m'} + B'_s X_s^{m'-1} + \ldots + H'_s X_s + K'_s = 0, \\ (s = 0, 1, 2, \ldots, n-1). \end{gathered} \quad (5)$$

The necessary and sufficient condition for (4) to have a common solution is that (5) have at least one solution in common. For this it is necessary that

$$\rho_0 + \rho_1 \omega_s + \rho_2 \omega_s^2 + \ldots + \rho_{n-1} \omega_s^{n-1} = 0, \quad (s = 0, 1, 2, \ldots, n-1) \quad (6)$$

where the ρ_t are the resultants of the associated pairs of equations in (5); since (6) also form sufficient conditions, the resultant of (4) is

$$R \equiv \rho_0 + \rho_1 e + \rho_2 e + \ldots + \rho_{n-1} e_{n-1}.$$

In fact (6) form all possible conditions that $N(R) = 0$, giving $R = 0$.

The number of roots common to (4) is the product of the n numbers each giving the number of solutions common to a pair of (5). Forming the sequence of subresultants of (4), R, R_1, R_2, ..., from the pairs of equations (5), it follows that, if R_p is the first that does not vanish, then p is the smallest of the n numbers and thus *p is the number of the common solutions of* (5) *which are independent.* Any pair of (5), which have $q > p$ solutions in common, will contribute one condition of type (6) to each of R_p, R_{p+1}, ..., R_{p+q-1}. Hence these latter are all divisors of zero, and the conditions they satisfy as such, properly allocated, are sufficient to determine exactly the number of common roots of (4), a number $\geqslant p^n$.

https://doi.org/10.1017/S0013091500013754 Published online by Cambridge University Press

The number of *independent* common roots is thus given, as in the orthodox theory, by the index of the first non-vanishing subresultant, while the total number of common roots requires, in addition, the further (unbroken) sequence of subresultants which are divisors of zero and a knowledge of the corresponding conditions.

The theory requires only conventional modifications for repeated roots and hence applies to discriminants.

When the coefficients y_r of (1) are all real numbers, special results arise owing to the fact that if (6) holds for one complex ω_s it holds for all complex ω_s, as is reflected in the fact that real cyclic systems have only two types of divisors of zero.

§ 4. *Systems of Linear Equations.* Consider the system of q linear equations in q unknowns $x, y, z, \ldots\ldots w$, over the cyclic system with n units,

$$a^{(r)}x + b^{(r)}y + c^{(r)}z + \ldots\ldots + h^{(r)}w = k^{(r)}, \quad (r = 1, 2, 3, \ldots\ldots, q). \tag{7}$$

As in § 2 these are equivalent to the n independent sets of linear equations

$$A_s^{(r)}X_s + B_s^{(r)}Y_s + C_s^{(r)}Z_s + \ldots + H_s^{(r)}W_s = K_s^{(r)}, \quad (r = 1, 2, 3, \ldots, q) \quad (s = 0, 1, 2, \ldots\ldots, n-1), \tag{8}$$

with the respective discriminants

$$\delta_0 + \delta_1\omega_s + \delta_2\omega_s^2 + \ldots + \delta_{n-1}\omega_s^{n-1} = 0, \quad (s = 0, 1, 2, \ldots, n-1). \tag{9}$$

If all of (9) are non-zero then unique solutions exist for (8) and thus (7) is satisfied uniquely. We can, in fact, solve (7) by Cramer's rule: but difficulties arise when the discriminant

$$D \equiv \delta_0 + \delta_1 e_1 + \delta_2 e_2 + \ldots\ldots + \delta_{n-1}e_{n-1}$$

is a divisor of zero. Hence, in order that (7) may have a unique solution, not only must $D \neq 0$, but D must not be a divisor of zero, a condition which is also sufficient.

If $D \neq 0$ but is a divisor of zero, certain of (9) vanish. For consistency the corresponding determinants, obtained by replacing any column of coefficients by a column of K's, must be of no higher rank than the vanishing members of (9). In other words the other q-order determinants from the array

$$\begin{vmatrix} a^{(1)} & b^{(1)} & c^{(1)} & \ldots\ldots & h^{(1)} & k^{(1)} \\ a^{(2)} & b^{(2)} & c^{(2)} & \ldots\ldots & h^{(2)} & k^{(2)} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & & & & & \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & & & & & \\ a^{(q)} & b^{(q)} & c^{(q)} & \ldots\ldots & h^{(q)} & k^{(q)} \end{vmatrix} \tag{10}$$

https://doi.org/10.1017/S0013091500013754 Published online by Cambridge University Press

must be divisors of zero satisfying at least the same conditions as D. In this case the solutions arising are not unique, arbitrary constants being introduced according to the total defects in rank below q of the vanishing members of (9). (11)

If some of the determinants in (10), other than D, vanish or are divisors of zero satisfying more conditions than D, then certain of (8) have only zero solutions, so that the solutions of (7) are divisors of zero satisfying those conditions.

If $D = 0$ and the other q-order determinants in (10) are of rank not higher than the rank l of D, then (7) and (8) are consistent; but arbitrary constants are introduced into the solution. This case differs from (11) in which certain of the unknowns in *some* only of (8) may be taken arbitrarily, for here certain unknowns in (7) may be taken arbitrarily, so that the corresponding unknowns in *all* of (8) are arbitrary. However, further arbitrary constants may arise as in (10), giving a total $\geqslant lq$.

The cases of fewer or more equations than unknowns, and the case when the right-hand sides of (7) are all zero, can be dealt with similarly.

https://doi.org/10.1017/S0013091500013754 Published online by Cambridge University Press