

## ON COMPLETE SYSTEMS UNDER CERTAIN FINITE GROUPS

BY C. W. STROM

1. *Introduction.* The theory of complete systems of invariants for rational functions that are unaltered under the substitutions of a finite group finds a close parallel in the theory of the binary  $n$ -ic.

It is well known that all the invariants and covariants of a binary  $n$ -ic can be expressed as rational functions of just  $n$  explicitly known forms such that the denominators are powers of the  $n$ -ic itself. In the parallel case Lagrange's theorem states that every rational function  $F(x_1, \dots, x_n)$  that is unaltered under the substitutions of a finite group  $G$  on  $x_1, \dots, x_n$  can be expressed as a rational function of the elementary symmetric polynomials  $E_i, (i = 1, \dots, n)$ , and any particular  $F$  that belongs to  $G$ . In these representations the denominator is a particular symmetric polynomial depending only on  $F$ .

If complete integrality is insisted upon, it is well known that the number of members in the complete system of the binary  $n$ -ic is finite although the exact number and the explicit forms cannot in general be determined by known means. In this paper we study the problem of obtaining irreducible sets of polynomials such that all polynomials that are invariant under the substitutions of a certain finite group can be expressed as rational, integral functions of the members of the irreducible set. In the case of the symmetric group  $G_n^n$ , the answer is given by the fundamental theorem of symmetric functions. The results for the alternating group  $G_{n/2}^n$  and the identity group  $G_1$  are also well known. We present solutions for the cyclic groups, the solvable groups, and the simple group  $G_{168}^7$ . In the cases of the cyclic groups and the solvable groups, the number of members in the irreducible sets is shown to be finite but the determination of the exact number is resolved essentially into a problem of partitions and can therefore not be expressed in general by known means.

If we regard  $x_1, \dots, x_n$  as coordinates in  $S_{n-1}$ , we may regard the group  $G$  as a collineation group and the results may be in-

terpreted as giving complete systems of invariants for certain collineation groups.

2. *The Cyclic Groups.* We consider a cyclic substitution of order  $n$ :

$$s = (x_0 x_1 \cdots x_{n-1}).$$

If

$$y_i = x_0 + \epsilon^i x_1 + \cdots + \epsilon^{(n-1)i} x_{n-1}, \quad \epsilon = e^{2\pi i/n},$$

$$(i = 0, 1, \cdots, (n-1)),$$

then

$$n x_i = y_0 + \epsilon^{(n-i)} y_1 + \cdots + \epsilon^{(n-1)(n-i)} y_{n-1}.$$

Hence, if  $P(x)$  is any polynomial in  $x_0, x_1, \cdots, x_{n-1}$ , we have

$$P(x) = \Pi(y) = \sum_{\alpha_0, \cdots, \alpha_{n-1}} A_{\alpha_0, \cdots, \alpha_{n-1}} y_0^{\alpha_0} \cdots y_{n-1}^{\alpha_{n-1}}.$$

Since  $s(y_i) = \epsilon^i y_i$ , we have the following theorem.

**THEOREM 1.** *A necessary and sufficient condition that  $P(x)$  be invariant under the substitutions of the cyclic group  $G_n^n$  is that it be expressible as the sum of products of arbitrary powers of  $y_0$  and products like  $y_1^{\alpha_1} \cdots y_{n-1}^{\alpha_{n-1}}$ , where  $\alpha_1, \cdots, \alpha_{n-1}$  form a positive integral solution of the diophantine equation*

$$\alpha_1 + 2\alpha_2 + \cdots + (n-1)\alpha_{n-1} = rn, \quad (r = 1, 2, 3, \cdots).$$

The solution of this equation is easy in particular cases and is dependent in general on partitions. Any solution of this equation yields a polynomial that is invariant under the given substitution. A finite set of polynomials to form a complete system is obtained from the aggregate of solutions by elementary considerations.

The determination of a complete system for the polynomials that belong to the cyclic group  $G_n^n$  requires  $q$  sets of cogredient  $y_i$ 's like those above and the solution of the diophantine equation

$$\sum_{j=1}^q [\alpha_1^{(j)} + 2\alpha_2^{(j)} + \cdots + (n-1)\alpha_{n-1}^{(j)}] = rn, \quad (r = 1, 2, 3, \cdots).$$

3. *The Solvable Groups.* If a polynomial  $P$  belongs to a subgroup  $H$  of index  $n$  under a finite group  $G$ , then  $P$  is  $n$ -valued under  $G$ . If  $H$  is self-conjugate under  $G$ , then the conjugates of  $P$  are permuted under  $G$  according to the factor group  $G/H$ . If the complete system of  $H$  is known consisting of  $q$  polynomials, and if the factor group  $G/H$  is cyclic, we have  $q$  sets of  $n$  quantities each permuted according to the cyclic group  $G_n^{qn}$ . A complete system for  $G$  can then be found by the methods outlined above. A repetition of this process enables us to obtain a complete system of invariants for the polynomials that belong to any composite group  $G$  whose series of composition  $G, G_1, \dots, G_\mu, 1$  is such that the factor groups  $G_\mu, G_{\mu-1}/G_\mu, \dots, G/G_1$  are all cyclic. If we assume, as we may without loss of generality, that each of the subgroups in the series of composition of  $G$  is a maximal self-conjugate subgroup, then the groups defined are just the solvable groups. For if the self-conjugate subgroups are all maximal, the factor groups are all simple. If the factor groups are also cyclic they must be of prime order and  $G$  is a solvable group.

4. *The Simple Group  $G_{168}^7$ .* The elementary symmetric polynomials on seven letters,  $E_i$ , ( $i=1, \dots, 7$ ), are clearly invariant under this group. However,  $E_3$  and  $E_4$  break up into parts that are themselves invariant under the group. We shall call these parts *S-polynomials*. They play a role in this theorem analogous to that of the  $E_i$  in the fundamental theorem of symmetric functions. For the sake of uniformity we adopt the following notation:\*

$$E_1 \equiv S_1, \quad E_2 \equiv S_2, \quad E_3 \equiv S_{123} + S_{234}, \quad E_4 \equiv S_{1237} + S_{1 \cdot 234},$$

$$E_5 \equiv S_{1 \cdot 26 \cdot 35}, \quad E_6 \equiv S_{14 \cdot 35 \cdot 36}, \quad E_7 \equiv S_{1234567}.$$

The group  $G_{168}^7$  is the group of the finite geometry of seven points in a plane, transforming three points of this geometry that are on a line into three points on a line, and three points that are not on a line into three points not on a line. Hence, in  $S_{234}$  the subscripts run over the triads that are on the seven lines of this geometry and in  $S_{123}$  they run over the triads that form

---

\* In these and following identities connecting  $S$ - and  $\Sigma$ -polynomials the subscripts themselves are written in place of the letters to which they are attached.

the twenty-one triangles. Thus  $S_{234} \equiv x_2x_3x_4 + x_1x_2x_6 + x_1x_3x_5 + x_1x_4x_7 + x_2x_5x_7 + x_3x_6x_7 + x_4x_5x_6$  is the invariant that defines the subgroup  $G_{168}^7$  of  $G_{71}^7$ , as well as the finite geometry. Similarly, in  $S_{1237}$  the subscripts run over the sets of four points each that form the seven quadrangles of the geometry, etc.

When the letters are affected with exponents, the symmetric polynomials break up still farther into parts that are separately invariant under this group, as follows:

$$\begin{aligned} \Sigma_1^i &\equiv S_1^i, \quad \Sigma_1^{i_2j} \equiv S_1^{i_2j}, \quad \Sigma_1^{i_2j_3k} \equiv S_1^{i_2j_3k} + S_2^{i_3j_4k}, \\ \Sigma_1^{i_2j_3k_4l} &\equiv S_1^{i_2j_3k_4l} + S_1^{j_2k_3l_4i} + S_1^k \cdot 2^l_3^i_4^j \\ &\quad + S_1^l \cdot 2^i_3^j_4^k + S_1^{i_2j_3k_7l}, \\ \Sigma_1^{i_2j_3k_4l_5m} &\equiv P(S_1^{i_2j_6k_3l_5m}), \\ \Sigma_1^{i_2j_3k_4l_5m_6n} &\equiv P(S_1^{i_4j_2k_5l_3m_6n}). \end{aligned}$$

In the identity of extent five the operator  $P$  indicates the sum of all the distinct  $S$ -polynomials of extent five obtained by taking the exponents  $i, j, k, l$ , and  $m$  in groups of two, two, and one, and similarly in the identity of extent six.

Since  $\Sigma_1^{i_2j_3k_4l_5m_6n_7p}$  has 5040 terms if all the exponents are different, while any single term has only 168 values under the group, we have

$$\Sigma_1^{i_2j_3k_4l_5m_6n_7p} \equiv P(S_1^{i_2j_3k_4l_5m_6n_7p}).$$

It is clear from their definitions that all the  $S$ -polynomials are unaltered by the substitutions of the group  $G_{168}^7$  and that every polynomial that is unaltered by these substitutions is a polynomial in the  $S$ -polynomials. We have to determine an irreducible set of  $S$ -polynomials in terms of which all  $S$ -polynomials can be expressed as polynomial functions.

We may take  $x_1, \dots, x_7$  as the roots of the equation

$$(x - x_1) \cdots (x - x_7) = 0.$$

By means of this equation we may express powers of  $x_i \geq 7$  in terms of the  $E_i$  and powers of  $x_i \leq 7$ . In the solution of our problem we need therefore consider only those  $S$ -polynomials for which  $1 \leq i, j, k, l, m, n, p \leq 7$ .

Our method of procedure is to investigate the  $S$ -polynomials in order beginning with these of extents 1 and 2. In the case of

$S$ -polynomials of extent  $i$ , ( $i=1, \dots, 7$ ), we determine a limited number such that all can be expressed as polynomial functions of this limited number and  $S$ -polynomials of extent  $>i$ . This process terminates when  $i=7$ , leaving us a limited number of  $S$ -polynomials of each extent from which an irreducible set may be selected to form a complete system. The actual work of reduction is very similar to that used in reducing symmetric polynomials. The procedure is illustrated in the following:

$$S_1^{i_2 j_3 k_7 l} \equiv S_1^{i-1_2 j-1_3 k-1_7 l-1} \cdot S_{1237}$$

minus  $S$ -polynomials of extent  $>4$ .

By means of this identity we make the reduction of  $S_1^{i_2 j_3 k_7 l}$  depend on the reduction of  $S_1^{i_2 j_3 k_7}$ .

$$\begin{aligned} S_1^{i_2 j_3 k_7} &\equiv S_1^{i-1_2 j-1_3 k-1_7} \cdot S_{123} - S_1^{i_2 j_3 k-1_7^2} - S_1^{i_2 j-1_3 k_7^2} \\ &\quad - S_1^{i-1_2 j_3 k_7^2} \text{ minus } S\text{-polynomials of extent } > 4 \\ &\equiv S_1^{i-1_2 j-1_3 k-1_7} \cdot S_{123} - (S_1^{i-1_2 j-1_3 k-2_7} + S_1^{i-1_2 j-2_3 k-1_7} \\ &\quad + S_1^{i-2_2 j-1_3 k-1_7}) \cdot S_{1237} \text{ minus } S\text{-polynomials of extent } > 4; \\ S_1^{i_2 j_3 7} &\equiv S_{1237} \cdot \Sigma_1^{i-1_2 j-1} \text{ minus } S\text{-polynomials of extent } > 4. \end{aligned}$$

The identities exhibited above show that all  $S$ -polynomials of the type  $S_1^{i_2 j_3 k_7 l}$  can be expressed as polynomials in  $S_{123}$ ,  $S_{1237}$ , and  $E_i$ , ( $i=1, \dots, 7$ ), together with  $S$ -polynomials of extent  $>4$ . An exactly similar procedure is used for the reduction of all the types of  $S$ -polynomials listed above. From the polynomials that are isolated, the following 19, forming an irreducible set, may be conveniently chosen as a complete system for the polynomials that are invariant under the group  $G_{168}^7$ :

$$\begin{aligned} &E_i, (i = 1, \dots, 7), \quad S_{123}, \\ &S_1^{j \cdot 234}, (j = 1, \dots, 6), \quad S_1^{k \cdot 26 \cdot 35}, (k = 2, \dots, 6). \end{aligned}$$