On the Representation of a Group of Finite Order as a Permutation Group, and on the Composition of Permutation Groups.

By W. Burnside. Received November 4th, 1901. Read November 14th, 1901.

In writing of linear groups it is becoming almost necessary to have a phrase by which to distinguish substitution groups, in the older and narrower sense in which every operation effects a permutation of the symbols, from groups of linear substitutions in general. In this paper the former will be called *permutation groups.*

Any permutation group with which a given abstract group is either simply or multiply isomorphic will be called a *representation* of that abstract group as a permutation group.

Two such representations of an abstract group in the same number of symbols will be called *equivalent* when the one can be transformed into the other by a linear substitution of non-vanishing determinant. In dealing with the theory of permutation groups by themselves, it is both natural and convenient to consider first the question of equivalence when transformation by permutations only is permitted.

The *mark* of any sub-group of a permutation group is defined as the number of the symbols operated on which are unchanged by every operation of the sub-group. It will be seen that in the theory of the representation of a group as a permutation group, and also in the composition of permutation groups, the marks of the sub-groups in the distinct transitive representations play a part closely analogous to that of the characteristics of the operations in the distinct representations of the group as an irreducible group of linear substitutions.

The main object of this paper is to determine, for any two representations of a group as a permutation group, the question of equivalence or non-equivalence: first, when transformation by permutations only is permitted; and, secondly, for general transformation.

1. Let G be a group of finite order. All the sub-groups of G may be arranged in a series of conjugate sets. The number of these

conjugate sets, including G itself and that constituted by the identical operation alone, will be represented by μ. Let

$$g_1, g_2, \ldots, g_\mu$$

be representatives of the groups in the μ conjugate sets arranged in such a way that the order of g_{s+1} is not less than the order of g_s. The first, g_1, will then be the sub-group consisting of the identical operation alone, and the last g_μ will be G itself. The order of g_s will be denoted by n_s, that of G being n_μ or simply n. Herr Dyck has shown how G may be represented as a transitive permutation group of degree n/n_s in respect of g_s, so that to g_s there corresponds one of the sub-groups of the permutation group which leave a symbol unchanged.

If g_s' belongs to the same conjugate set of sub-groups in G as g_s, the representation of G in respect of g_s' is identical with that in respect of g_s. The μ representations of G in respect of

$$g_1, g_2, \ldots, g_s, \ldots, g_\mu$$

as transitive permutation groups of degrees

$$n, n/n_2, \ldots, n/n_s, \ldots, 1$$

will be denoted by $G_1, G_2, \ldots, G_s, \ldots, G_\mu$.

These include every possible representation of G as a transitive permutation group.

The *mark* of g_s in G_t will be denoted by m_s^t, each of these numbers being by definition either zero or a positive integer. The only sub-groups of G_t whose marks differ from zero are those contained in the sub-groups that leave a symbol unchanged, *i.e.*, in g_t and its conjugates. Hence, if $s \neq t$, and if $n_s \geqslant n_t$, then m_s^t must be zero. Each of the μ symbols m_t^t is greater than zero. Hence in the square array

$$\begin{array}{cccc} m_1^1, & m_2^1, & \ldots, & m_\mu^1, \\ m_1^2, & m_2^2, & \ldots, & m_\mu^2, \\ \ldots & \ldots & & \ldots \\ m_1^\mu, & m_2^\mu, & \ldots, & m_\mu^\mu, \end{array}$$

all terms to the right hand of the leading diagonal are zero, and each term in the leading diagonal is different from zero. It follows that the μ sets of marks

$$m_1^t, m_2^t, \ldots, m_\mu^t \quad (t = 1, 2, \ldots, \mu),$$

are linearly independent in the sense that there can be no system of equations

$$\sum_t a^t m_i^t = 0$$

for each i from 1 to μ.

2. When a permutation group, transitive or intransitive, is transformed by a permutation of the symbols on which it operates, every sub-group must have the same mark in the transformed group as the corresponding sub-group in the original group.* Hence, if we regard two representations of G in the form of permutation groups as equivalent only when one can be transformed into the other by a permutation, the μ representations $G_1, G_2, \ldots, G_\mu$ are distinct. This is, of course, obviously the case for G_s and G_t, when g_s and g_t are not simply isomorphic; but even when g_s and g_t are simply isomorphic, while the numbers of conjugate sub-groups in the s-th and t-th sets is the same, G_s cannot be transformed into G_t by a permutation, so that the set of sub-groups which correspond to g_i in G_s is transformed (for each i) into that which corresponds to g_i in G_t.

3. If G is simply or multiply isomorphic with an intransitive permutation group Γ, each transitive constituent of Γ must be equivalent to one of the permutation groups $G_1, G_2, \ldots, G_\mu$. Hence Γ may be represented by the symbol

$$\sum_{i=1}^{i=\mu} a_i G_i,$$

where a_i (zero or a positive integer) denotes the number of transitive constituents of Γ which are equivalent to G_i. Suppose now that G_s and G_t are set up in two distinct sets of symbols—say x's and y's—n/n_s and n/n_t in number. To every operation of G will correspond a permutation of the $n^2/n_s n_t$ products of the x's and the y's. The permutation group that arises when G_s and G_t are thus *compounded* will be represented by $G_s G_t$ (or $G_t G_s$); it will in general be intransitive. The result of thus compounding G_s and G_t may be represented by the symbolical equation

$$G_s G_t = \sum_{i=1}^{i=\mu} k_{st i} G_i, \qquad \text{(i)}$$

where $k_{st i}$ denotes the number of transitive constituents of the permutation group on the products of the x's and y's which are

* It should be noted at once that this is not necessarily the case if a permutation group is transformed by a linear substitution on the symbols into another permutation group. This point will be considered later and examples will be given.

equivalent to G_i; and there will be an equation of this form for each pair of suffixes s and t. Moreover, these equations admit of a direct arithmetical interpretation. In fact, m_r^s denotes the number of x's which are unchanged by every operation of g_r, and m_r^t the number of similarly unchanged y's. Hence in the permutation group $G_s G_t$ on the products of the x's and the y's just $m_r^s m_r^t$ products are unchanged by every operation of g_r. The relation (i) therefore implies the system of μ arithmetical identities

$$m_r^s m_r^t = \sum_{i=1}^{i=\mu} k_{sti} m_r^i \quad (r = 1, 2, \ldots, \mu). \qquad \text{(ii)}$$

Conversely, since the determinant of the μ sets of marks is not zero, the system of equations last written determine the μ numbers k_{sti} $(i = 1, 2, \ldots, r)$ uniquely. The result of compounding any two of the transitive representations of G is therefore given directly by the complete system of marks.

4. For the tetrahedral group μ is 5, and g_1, g_2, g_3, g_4, g_5 are groups of orders 1, 2, 3, 4, 12. In the corresponding transitive representations G_1, G_2, G_3, G_4, G_5 the marks are given by the table

	g_1	g_2	g_3	g_4	g_5
G_1	12	0	0	0	0
G_2	6	2	0	0	0
G_3	4	0	1	0	0
G_4	3	3	0	3	0
G_5	1	1	1	1	1

In every case it is clear that

$$G_1 G_t = m_1^t G_1$$

and

$$G_\mu G_t = G_t.$$

The remaining relations in this case indicating the composition of the G's are

$$G_2^2 = 2G_1 + 2G_2, \qquad G_3^2 = G_1 + G_3,$$

$$G_2 G_3 = 2G_1, \qquad G_3 G_4 = G_1,$$

$$G_2 G_4 = 3G_2, \qquad G_4^2 = 3G_4.$$

5. Two permutation groups, given by the symbols $\sum_i a_i G_i$ and $\sum_i \beta_i G_i$, can be equivalent (in respect of transformations by permutations) only when they have the same marks for each set of conjugate sub-groups. But, since the sets of marks are independent, the μ equations

$$\sum_i a_i m_r^i = \sum_i \beta_i m_r^i, \quad (i = 1, 2, \ldots, \mu),$$

involve

$$a_i = \beta_i$$

for each i. Hence to each symbol such as $\sum_i a_i G_i$ corresponds a distinct permutation group which represents G. The determination of all the distinct ways in which G may be represented as a permutation group of degree m will therefore be given by the number of distinct solutions of the equation

$$\sum a_i m_1^i = m$$

in positive integers. For example, the number of distinct representations of the tetrahedral group as a permutation group of degree 7 is the number of solutions of

$$12a_1 + 6a_2 + 4a_3 + 3a_4 + a_5 = 7,$$

viz., 6. These six groups are represented by $G_2 + G_5$, $G_3 + G_4$, $G_3 + 3G_5$, $2G_4 + G_5$, $G_4 + 4G_5$, and $7G_5$.

6. When the variables permuted by a permutation group Γ undergo a linear substitution S, the transformed group $S^{-1}\Gamma S$ is not in general a permutation group, though it may be so in particular cases. Thus any permutation group in n symbols is transformed into itself by the substitution

$$\begin{aligned} x_1' &= x_2 + x_3 + \ldots + x_n, \\ x_2' &= x_1 + x_3 + \ldots + x_n, \\ &\ldots \quad \ldots \quad \ldots \\ x_n' &= x_1 + x_2 + \ldots + x_{n-1}. \end{aligned}$$

A further question of the equivalence or non-equivalence of any two representations of G as a permutation group (in the same number of variables) thus arises when, in addition to transformation by permutations, transformations by linear substitutions which preserve the permutation form of the group are admitted.

In this connexion a theorem due to Herr Frobenius* is of great importance. It may be stated as follows:—

Two representations, G' and G'', of a group G of finite order as a group of linear substitutions in the same number of variables can be transformed into each other if, and only if, the sums of the multipliers of the substitutions of G' and G'' which correspond to a given operation S of G are the same for each operation S.

In any representation of G as a permutation group the sum of the multipliers of the permutation that corresponds to S is the mark of the cyclical sub-group generated by this permutation; for the sum of the multipliers that arise from any cyclical component of the permutation is zero. Hence it follows at once from Herr Frobenius's theorem that the necessary and sufficient conditions that $\sum_i \alpha_i G_i$ and $\sum_i \beta_i G_i$ should be equivalent when transformations by linear substitutions are admitted is that the equation

$$\sum_i (\alpha_i - \beta_i) m_t^i = 0$$

should be satisfied by the marks of each cyclical sub-group. Unless G is a cyclical group, the system of equations that thus arise when $\alpha_i - \beta_i$ $(i = 1, 2, \ldots, \mu)$ are regarded as unknown must have (integral) solutions other than all zero values; since their number cannot exceed $\mu - 1$. Hence there must always be representations of a non-cyclical group as a permutation group which, while not equivalent in respect of transformation by permutations, are, in fact, equivalent for transformation by linear substitutions.

7. Suppose that G has s distinct conjugate sets of cyclical sub-groups, and (slightly modifying the previous notation) let $g_1, g_2, \ldots, g_s$ be representatives of them. The equations

$$\sum \alpha_i m_t^i = 0, \quad (t = 1, 2, \ldots, s),$$

will have just $\mu - s$ linearly independent solutions in positive or negative integers, since the determinant

$$\| m_t^i \| \quad (t, i = 1, 2, \ldots, s)$$

---

* "Ueber die Darstellung der endlichen Gruppen durch lineare Substitutionen," *Berliner Sitzungsberichte*, 1897, pp. 1000–1005.

is different from zero. Moreover,* there is a set of solutions

$$\alpha_1^r,\ \alpha_2^r,\ \ldots,\ \alpha_\mu^r,\quad (r = 1, 2, \ldots, \mu - s),$$

in terms of which the general solution takes the form

$$\alpha_i = \sum_r k_r \alpha_i^r,$$

where the k's are $\mu - s$ arbitrary integers, positive or negative. Hence, if $\Sigma \alpha_i G_i$ and $\Sigma \beta_i G_i$ are equivalent representations of G in respect of transformation by linear substitutions, then there must be a set of integers k such that

$$\alpha_i - \beta_i = \sum_r k_r \alpha_i^r.$$

Every possible equivalence of the kind considered will therefore arise from the $\mu - s$ fundamental equivalences denoted symbolically by

$$\Sigma \alpha_i^r G_i = 0.$$

This is to be understood in the sense that, after removing to the right-hand side the terms with negative coefficients, the permutation groups denoted by the symbols on either side of the equation are equivalent.

8. In illustration, the tetrahedral group may be again considered. The cyclical sub-groups are those denoted by g_1, g_2, g_3 in the preceding table. The three equations among the α's are

$$\begin{aligned} 12\alpha_1 + 6\alpha_2 + 4\alpha_3 + 3\alpha_4 + \alpha_5 &= 0, \\ 2\alpha_2 \qquad\quad + 3\alpha_4 + \alpha_5 &= 0, \\ \alpha_3 \qquad\quad + \alpha_5 &= 0. \end{aligned}$$

The fundamental solutions of these are

$$\alpha_1 = 0,\quad \alpha_2 = -1,\quad \alpha_3 = 1,\quad \alpha_4 = 1,\quad \alpha_5 = -1;$$

and

$$\alpha_1 = 1,\quad \alpha_2 = -3,\quad \alpha_3 = 0,\quad \alpha_4 = 2,\quad \alpha_5 = 0.$$

The equivalences corresponding to these, from which all others arise by addition, are

$$G_3 + G_4 = G_2 + G_5,$$

and

$$G_1 + 2G_4 = 3G_2.$$

It will be perhaps not without interest to verify directly the equivalences thus indicated. The tetrahedral group is defined abstractly

* Elliott, *Algebra of Quantics*, p. 192.

by the relations $A^2 = 1, \quad B^3 = 1, \quad (AB)^3 = 1.$

In the form $G_2 + G_5$ it is represented as a permutation group of degree 7 in which one symbol x_0 is unaltered by every operation, and the others $x_1, x_2, \ldots, x_6$ are permuted transitively. We may take

$$A = (x_1x_4)(x_2x_5), \quad B = (x_1x_3x_3)(x_4x_5x_6).$$

Consider now the seven linear functions of the x's

$$\begin{aligned} y_1 &= x_0+x_1+x_2+x_3, \\ y_2 &= x_0+x_3+x_4+x_5, \\ y_3 &= x_0+x_1+x_5+x_6, \\ y_4 &= x_0+x_2+x_4+x_6, \\ z_1 &= x_1+x_4, \\ z_2 &= x_2+x_5, \\ z_3 &= x_3+x_6. \end{aligned}$$

They are obviously linearly independent, and therefore these seven equations give a linear substitution S. Moreover, when the x's undergo the permutations A and B, the y's and z's undergo the permutations

$$(y_1y_2)(y_3y_4)$$

and

$$(y_2y_3y_4)(z_1z_2z_3).$$

Hence the y's and z's are each permuted among themselves by every operation of the group, and the permutation group so arrived at is $G_3 + G_4$; or

$$S\,(G_2 + G_5)\,S^{-1} = G_3 + G_4.$$

Again, in the form $G_1 + 2G_4$ the tetrahedral group is represented as a permutation group of degree 18, interchanging 12 x's, 3 y's, and 3 z's among themselves. The permutations given by A and B may be taken as

$$(x_1x_2)(x_3x_4)(x_5x_6)(x_7x_8)(x_9x_{10})(x_{11}x_{12})$$

and

$$(x_1x_5x_9)(x_2x_7x_{11})(x_3x_6x_{12})(x_4x_8x_{10})(y_1y_2y_3)(z_1z_2z_3).$$

The 18 linear functions

$$\begin{aligned} u_1 &= y_1+x_1+x_2, & v_1 &= z_1+x_1+x_3, & w_1 &= x_1+x_4, \\ u_2 &= y_2+x_5+x_7, & v_2 &= z_2+x_5+x_6, & w_2 &= x_5+x_8, \\ u_3 &= y_3+x_9+x_{11}, & v_3 &= z_3+x_9+x_{12}, & w_3 &= x_9+x_{10}, \\ u_4 &= y_1+x_3+x_4, & v_4 &= z_1+x_2+x_4, & w_4 &= x_2+x_3, \\ u_5 &= y_2+x_6+x_8, & v_5 &= z_2+x_7+x_8, & w_5 &= x_6+x_7, \\ u_6 &= y_3+x_{10}+x_{12}, & v_6 &= z_3+x_{10}+x_{11}, & w_6 &= x_{11}+x_{12} \end{aligned}$$

are linearly independent and give a linear substitution T. Moreover, the operations A and B give the permutations

$$(u_2u_5)(u_3u_6)(v_1v_4)(v_3v_6)(w_1w_4)(w_2w_5)$$

and $$(u_1u_3u_3)(u_4u_5u_6)(v_1v_2v_3)(v_4v_5v_6)(w_1w_2w_3)(w_4w_5w_6).$$

The u's, v's, and w's therefore undergo a permutation group denoted by $3G_2$ and

$$T(G_1+2G_4)\,T^{-1} = 3G_2.$$

9. It may happen that among the $\mu-s$ fundamental equivalences

$$\Sigma a_i^r G_i = 0$$

one or more of the form $$G_i - G_j = 0$$

occur; indicating that two distinct transitive representations of G can be transformed the one into the other by a suitably chosen linear substitution. The necessary and sufficient conditions for this are that the marks of each cyclical sub-group shall be the same in G_i and G_j. Hence g_i and g_j must be of the same order, the conjugate sets to which g_i and g_j belong must contain the same number of conjugate sub-groups, and any cyclical sub-group which enters in a number of sub-groups of the one set must enter in an equal number of the other set.

As an example, these conditions are satisfied by the two distinct sets of octahedral sub-groups which enter in the simple group G of order 168. In respect of an octahedral sub-group g of the one set, G is represented as the transitive group of degree 7 generated by

$$S = (x_1x_2x_3x_6x_4x_5x_7), \quad T = (x_2x_3x_4)(x_5x_6x_7), \quad U = (x_2x_7x_6x_3)(x_4x_5);$$

and an octahedral group g' of the second set is generated by T and V, where

$$V = (x_1x_7x_5x_6)(x_2x_3).$$

The seven linear functions

$$\begin{aligned} y_1 &= x_2+x_3+x_4, \quad y_2 = x_3+x_5+x_6, \quad y_3 = x_4+x_6+x_7, \\ y_4 &= x_2+x_5+x_7, \quad y_5 = x_1+x_3+x_7, \quad y_6 = x_1+x_4+x_5, \\ y_7 &= x_1+x_2+x_6 \end{aligned}$$

are independent; so that these equations give a linear substitution. When G is transformed by this substitution, it remains a permuta-

tion group, and

$$S = (y_1y_2y_3y_0y_4y_5y_7), \quad T = (y_2y_3y_4)(y_5y_0y_7), \quad U = (y_1y_4y_3y_2)(y_6y_7),$$
$$V = (y_2y_7y_5y_4)(y_3y_0).$$

Hence in the transformed group g' is the sub-group which leaves one symbol y_1 unchanged, while g permutes the symbols in the two transitive sets y_1, y_2, y_3, y_4 and y_5, y_6, y_7. The given linear substitution therefore transforms the transitive representation of G in respect of g into that in respect of g'.

Linear Null Systems of Binary Forms. *By* J. H. GRACE.

Read November 14th, 1901. Received November 18th, 1901.

As an exercise on Hilbert's paper "Ueber vollen Invariantensysteme," *Math. Ann.*, Vol. XLI., I propose to investigate the necessary and sufficient condition that all the combinants of three binary forms which are pure invariants should vanish. The method used applies equally well to any number of binary forms.

Suppose the three forms are

$$f = a_0x_1^n + na_1x_1^{n-1}x_2 + \ldots + a_nx_2^n = a_x^n,$$
$$\phi = b_0x_1^n + nb_1x_1^{n-1}x_2 + \ldots + b_nx_2^n = b_x^n,$$
$$\psi = c_0x_1^n + nc_1x_1^{n-1}x_2 + \ldots + c_nx_2^n = c_x^n;$$

then the combinants in question are such mutual invariants of f, ϕ, ψ as remain unaltered when any of the forms is replaced by a linear combination $lf + m\phi + n\psi$.

The combinants are well known to be rational integral functions of the determinants of the type

$$\begin{vmatrix} a_\alpha & a_\beta & a_\gamma \\ b_\alpha & b_\beta & b_\gamma \\ c_\alpha & c_\beta & c_\gamma \end{vmatrix},$$

whether they involve the variables or not. We shall denote the above determinant by $p_{\alpha\beta\gamma}$.