ON THE USE OF THE CO-SETS OF A GROUP*

BY

G. A. MILLER

§ 1. *Introduction.*

ABBATI proved in a letter addressed to RUFFINI and dated September 30, 1802, that it is possible to divide all the operators of a group G into sets with respect to an arbitrary subgroup H so that no two of the sets have a common operator. That is, every subgroup of G may be regarded as a modulus with respect to either right or left multiplication. For any subgroup H a set of operators $S_2, S_3, \cdots, S_\rho$ may be selected so that this division can be effected in each of the following four ways:†

$$\begin{aligned} G &= H + HS_2 + HS_3 + \cdots + HS_\rho, \\ &= H + S_2H + S_3H + \cdots + S_\rho H, \\ &= H + S_2^{-1}H + S_3^{-1}H + \cdots + S_\rho^{-1}H, \\ &= H + HS_2^{-1} + HS_3^{-1} + \cdots + HS_\rho^{-1}. \end{aligned}$$

The sets HS_α, $S_\alpha H$ $(\alpha = 2, 3, \cdots, \rho)$ have been called Nebengruppen‡ or *co-sets* of G as regards H, the former being called the right co-sets and the latter the left co-sets. When H is added to these co-sets they are called the augmented right co-sets and the augmented left co-sets, respectively.

It has been observed that the operators of each right co-set are evenly distributed among a certain number of the left co-sets, or among all of them, and that the operators of each left co-set are distributed in the same way among the right co-sets. When a right co-set involves an operator which transforms H into itself all of its operators have this property and this right co-set involves exactly the same operators as some left co-set, and vice versa. A necessary and sufficient condition that H gives rise to a multiply transitive substitution group K, when G or one of its quotient groups is represented transitively as regards H in the usual manner,§ is that the operators of each right co-set of G as regards H are distributed among all the left co-sets as regards H, ρ being greater than 2.‖ The same condition is expressed by saying that whenever S

* Presented to the Society (Chicago) December 28, 1910.

† Quarterly Journal of Mathematics, vol. 41 (1910), p. 384.

‡ WEBER, *Lehrbuch der Algebra*, 2d edition, 1899, vol. 2, p. 8.

§ DYCK, Mathematische Annalen, vol. 22 (1883), p. 91.

‖ Proceedings of the American Philosophical Society, vol. 49 (1910), p. 307.

is any operator of G which is not also in H every operator of G is included in the two sets H and HSH, and that ρ exceeds 2.

GALOIS called attention to the importance of the special case when each right co-set of G as regards H is identical with some left co-set. That this case expresses the necessary and sufficient condition that H is invariant under G follows from the more general theorem noted above that a necessary and sufficient condition that H is transformed into itself by the operators of a right co-set is that this co-set is identical with some left co-set, and vice versa. This theorem is, in turn, included in the still more general statement that a necessary and sufficient condition that the operators of a co-set transform H into a group having exactly γ operators in common with H is that this co-set has exactly γ operators in common with some other co-set with respect to H. This statement may again be regarded as a special case of the more general theorem which affirms that the total number of operators in G which transform H into a group having exactly ρ operators in common with some other subgroup K is a multiple of the product of the orders of H and K divided by ρ.*

When H_1 and H_2 are any two groups the product H_1H_2 represents the totality of distinct operators obtained by multiplying on the left each operator of H_2 by each operator of H_1. The number of distinct operators in this totality is evidently the product of the orders of H_1 and H_2 divided by the number of their common operators. A necessary and sufficient condition that this totality constitutes a group is that $H_1H_2 = H_2H_1$. This is a special case of a more general theorem which may be stated as follows: A necessary and sufficient condition that the continued product of the λ groups $H_1, H_2, \cdots, H_\lambda$ is a group is that this product is not affected by the cyclic permutations of its factors. That is, $H_1H_2 \cdots H_\lambda$ is a group whenever

$$H_1H_2 \cdots H_\lambda = H_2 \cdots H_\lambda H_1 = \cdots = H_\lambda H_1 H_2 \cdots,$$

as may easily be verified.

The given method of arranging the operators of G in distinct sets, called augmented co-sets, can easily be generalized by observing that the co-sets are completely determined by H and do not depend upon the choice of the operators $S_2, S_3, \cdots, S_\rho$. Hence it follows directly that the *double co-set* $HS_\alpha H_1$, H_1 being an arbitrary subgroup of G, remains unchanged when S_α is replaced by any other operator of this double co-set. That is, two double co-sets $HS_\alpha H_1$, $HS_\beta H_1$ either have all their operators in common or they have no operator in common.† Each operator of G may therefore be uniquely represented by such double co-sets and HH_1; that is, the group may be represented by a system of augmented double co-sets, as follows:

*Bulletin of the American Mathematical Society, vol. 16 (1910), p. 510.

†FROBENIUS, Journal für reine und angewandte Mathematik, vol. 101 (1887), p. 274.

$$G = HH_1 + HS_2H_1 + \cdots + HS_\lambda H_1.$$

When $H_1 = H$ and G or one of its quotient groups is represented as a transitive substitution group with respect to H in the ordinary way, the number of transitive constituents in the subgroup composed of all the substitutions which omit one letter of this substitution group is λ, if the omitted letter or letters are counted as constituents; and the numbers of distinct operators in these various double co-sets are equal to the products of the order of H and the degrees of the various transitive constituents of this subgroup.* When $H_1 = 1$ these double co-sets reduce to right co-sets and when $H = 1$ they reduce to left co-sets.

The general properties of double co-sets were first studied by FROBENIUS in an article entitled *Ueber die Congruenz nach einem aus zwei endlichen Gruppen gebildeten Doppelmodul*, Journal für die reine und angewandte Mathematik, volume 101 (1887), page 273. Since then the concept of equivalence of operators as regards a double modulus has been employed by various writers. The object of the present article is to extend the abstract theory as regards co-sets with a view to a greater usefulness of this concept. This article is practically a continuation of the one entitled, *Some relations between substitution group properties and abstract groups*, Proceedings of the American Philosophical Society, volume 49 (1910), page 307. The theorem of § 3 which exhibits a dual relation between the degrees of the transitive constituents of various subgroups when the group is represented with respect to these subgroups is perhaps the most useful result of the present paper.

§ 2. *Double co-sets with respect to a single subgroup.*

The double co-set $HS_\alpha H$ involves all the right co-sets which are conjugate under H with HS_α. It also includes all the conjugates under H of the left co-set $S_\alpha H$. In fact, each of these two complete sets of conjugates involves exactly the same operators, and is identical with $HS_\alpha H$. The number of distinct conjugates in each of these two sets may be obtained by dividing the order of H by the number of operators common to H and $S_\alpha^{-1}HS_\alpha$ since this is also the number of operators common to the two co-sets HS_α and $S_\alpha H$, and hence it represents the number of left co-sets among which all the operators of HS_α are evenly distributed as well as the number of right co-sets among which the operators of $S_\alpha H$ are evenly distributed. We shall prove in the next paragraph that this same number is also the degree of a transitive constituent of the subgroup composed of all the substitutions omitting one letter in the transitive substitution group K which corresponds to the permutations of the rows when all the operators of G are arranged in the ordinary rectangular form and the operators of H constitute the first row.†

* Proceedings of the American Philosophical Society, vol. 49 (1910), p. 311.

† DYCK, Mathematische Annalen, vol. 22 (1883), p. 91.

To prove this theorem we shall at first assume that K is simply isomorphic with G. This is equivalent to assuming that H contains no invariant subgroup of G besides the identity, or that K represents G. Let K_1 represent the subgroup of K which corresponds to H in this simple isomorphism. Hence K_1 is composed of all the substitutions of K which omit a given letter (a) and HS_α corresponds to all the substitutions of K which replace a by a given other letter. The conjugates of HS_α are then all the operators of G which correspond to those substitutions of K which replace a by the different letters in a transitive constituent of K_1. That is, *if the operators of G are arranged into double co-sets with respect to a single subgroup in the following manner:*

$$G = H + HS_2H + HS_3H + \cdots + HS_\lambda H,$$

and if H does not involve any invariant subgroup of G besides the identity, so that G may be represented as a transitive substitution group K with respect to H, then the operators in each of these double co-sets correspond to all the substitutions of K which replace the letter omitted in the subgroup corresponding to H by the letters in a transitive constituent of this subgroup.

When H includes an invariant subgroup of G or is itself invariant under G, it gives rise to the transitive representation of a quotient group of G and the preceding theorem applies to this quotient group. Hence λ represents the number of transitive constituents (each omitted letter being also regarded as a transitive constituent) in the subgroup composed of all the substitutions of this quotient group which omit a given letter, and we may establish a $(1, 1)$ correspondence between the double co-sets and the transitive constituents of this subgroup in such a way that the number of distinct operators in each double co-set is equal to the product of the order of H into the degree of the corresponding transitive constituent. In particular when H is invariant this quotient group is regular and the number of these double co-sets is equal to the degree of this quotient group, as each of the transitive constituents of the given subgroup is of degree one in this special case. Hence we have as a corollary of the given theorem the known theorem that necessary and sufficient conditions that H gives rise to a multiply transitive group are that H contains less than half the operators of G and that $\lambda = 2$.

A necessary and sufficient condition that the transitive substitution group K to which H gives rise is primitive is that G is generated by each double co-set as regards H, since this condition is equivalent to the condition that H is a maximal subgroup. A necessary and sufficient condition that the subgroup of K composed of all its substitutions which omit one letter omits exactly α letters is that there are $\alpha - 1$ double co-sets as to H each involving the same number of distinct operators as H does. This results directly from the more general theorem that all the operators of such a double co-set transform H into

groups all having the same number of operators in common with H and that the number of the distinct operators in this co-set is equal to the square of the order of H divided by the number of these common operators. This is, in turn, a special case of a theorem which will be proved in the following section.

§ 3. *Double co-sets with respect to two distinct subgroups.*

A special case of a double co-set with respect to two distinct subgroups was developed by Cauchy to prove the fundamental theorem that every group whose order is divisible by a given prime number involves a subgroup whose order is this prime.* This theorem was announced by Galois, who however did not give any proof in his published papers. Frobenius extended, in the article cited at the close of § 1, the development of the theory of double co-sets and employed this theory to re-establish Sylow's theorem as well as to prove other fundamental related theorems. Recently the present writer pointed out that Sylow's theorem may be proved directly by a slight extension of Cauchy's theorem relating to double co-sets and then following the steps which Cauchy took to establish the special but fundamental case noted above.† These facts may suffice to indicate that the concept of double co-sets relates to fundamental matters in group theory and seems to deserve more attention than it has recently received.

If H_1 and H_2 are any two subgroups of G, all the operators of G may be represented uniquely in either of the following two forms in accord with the results stated above:

$$G = H_1 H_2 + H_1 S_2 H_2 + \cdots + H_1 S_\lambda H_2,$$
$$= H_2 H_1 + H_2 S_2^{-1} H_1 + \cdots + H_2 S_\lambda^{-1} H_1.$$

The second augmented system of double co-sets is evidently composed of the inverses of the operators in first system. To obtain a concrete illustration of some of the properties of these augmented double co-sets it may be observed that when G can be represented as a transitive substitution group K with respect to H_1, the substitutions corresponding to $H_1 H_2$ will be composed of all those of K which replace the letter a omitted in all the substitutions of the subgroup K_1 corresponding to H_1 by the letters of the transitive constituent to which a belongs in the subgroup K_2 corresponding to H_2. In a similar manner we may observe that all the operators of the double co-sets $H_1 S_\alpha H_2$ ($\alpha = 2, 3, \cdots, \lambda$) correspond to all the substitutions which replace the letter by which a is followed in S_α by all the letters of a transitive constituent in K_2. The number of the distinct operators in the double co-set $H_1 S_\alpha H_2$ is therefore equal to the order of

*CAUCHY, *Oeuvres complètes*, 1st series, vol. 9 (1896), p. 358.

†Bulletin of the American Mathematical Society, vol. 16 (1910), p. 510.

H_1 multiplied by the degree of the corresponding transitive constituent of K_2. In particular, this number is the order of H_1 whenever the letter which follows a in S_a does not occur in K_2. As a special case we have also the theorem that a necessary and sufficient condition that $H_1 H_2 = G$ is that K_2 be transitive.

From the preceding results we may deduce a general theorem as regards the transitive substitution groups which are simply isomorphic with G. This theorem may be stated as follows: *If G is represented as a transitive substitution group K and if K_1 is the subgroup composed of all the substitutions of K which omit a given letter, then any subgroup K' of K has the same number of transitive constituents as the subgroup which corresponds to K_1 has when K is represented as a transitive group with respect to K'. Moreover, the transitive constituents in the two given subgroups have the same relative degrees in the two different representations of G.*

The significance of this theorem may be inferred from the following illustrations. When the icosahedral group is represented as the alternating group of degree 5, K_1 is the alternating group of degree 4 and all the subgroups of order 12 in K are conjugate. If we let K' represent one of the subgroups of order 4 in K it is evident that K' has two transitive constituents of degrees 4 and 1 respectively. Hence when K is represented as a transitive group of degree 15 with respect to K' its subgroups of order 12 will have two transitive constituents of degrees 12 and 3 respectively. On the other hand, if we let K' represent a subgroup of order 6 in K, it is clear that it has two transitive constituents of degrees 3 and 2 respectively. Hence when K is represented as a transitive group of degree 10 its subgroups of order 12 will have two transitive constituents of degrees 6 and 4 respectively. Finally, if we let K' be a subgroup whose order is either 5 or 10, it is transitive, and hence the subgroups of order 12 in the icosahedral group are transitive when this group is represented transitively on either 6 or 12 letters.

It should be observed that the given theorem remains true even when K does not represent G but represents merely a quotient group of G; that is when H_1 either involves an invariant subgroup of G or is itself invariant under G. In these cases it is evidently necessary to consider the groups which correspond to the subgroups K_1 and K' in the transitive representation instead of these subgroups themselves. The given development exhibits not only an interesting dual relation between the forms of the various subgroups when a group is represented transitively in the various possible ways, but it also exhibits a dual relation between certain abstract group properties and substitution groups, since not only does λ express the number of transitive constituents in the group corresponding to H_2 when G is represented transitively as regards H_1, but the number of distinct operators in each of the double co-sets is equal to the product of the order of H_1 and the degree of the corresponding transitive constituent.

The number of distinct operators in each one of the augmented double co-sets is a multiple of the orders of the two subgroups H_1, H_2. That is, *if K' is any subgroup of any transitive group whatever of order g and of degree n, and if n_1 is the degree of a transitive constituent of K', then the order of K' is a divisor of $n_1 g/n$.* This limits the orders of the intransitive subgroups of any transitive substitution group and it reduces to Lagrange's theorem when the subgroups are transitive. It may therefore be regarded as a generalization of Lagrange's theorem. It should be observed that this theorem may also be proved directly by employing the fact that the order of the subgroup composed of all the substitutions of K' which omit a given letter is a divisor of g/n.

To illustrate the usefulness of the theorem in the last paragraph we may again make use of transitive representations of the icosahedral group. When this group is represented as the alternating group of degree 5, K' can have a transitive constituent of degree 2 only when the order of K' is a divisor of 24, and it can have a transitive constituent of degree 3 only when this order is a divisor of 36, in accord with the given theorem. The only non-cyclic subgroups which have constituents of degree 2 or 3 are those of order 6, and as 6 is a divisor of both the numbers 24 and 36 this agrees with the theorem. On the other hand, when the icosahedral group is represented as a transitive group of degree 6, K' can have a transitive constituent of degree 2 only when the order of K' is a divisor of 20. As a subgroup whose order is divisible by 5 in a transitive group of degree 6 could clearly not have a transitive constituent of degree 2, it results that the order of K' is a divisor of 4 whenever it has a transitive constituent of degree 2. In fact, it is evident that the subgroups of orders 2 and 4 are the only ones which have transitive constituents of degree 2 in the present case. Similarly we observe that the order of K' is a divisor of 6 whenever it has a transitive constituent of degree 3, and that in the present case the subgroups of order 6 have two constituents of this degree. These illustrations may suffice to exhibit how the theorem under consideration may be employed to gain an insight into the structure of transitive substitution groups.

It is known that a necessary and sufficient condition that the product $H_1 H_2$ constitutes a group is that it is equal to its inverse $H_2 H_1$. We proceed to inquire what is implied by the condition that each double co-set is identical with the inverse of a double co-set as regards the same subgroups. That is, we suppose that the two series of augmented double co-sets

$$\begin{aligned} G &= H_1 H_2 + H_1 S_2 H_2 + \cdots + H_1 S_\lambda H_2 \\ &= H_2 H_1 + H_2 S_2^{-1} H_1 + \cdots + H_2 S_\lambda^{-1} H_1 \end{aligned}$$

are identical if the order is not considered. Since each of the two products $H_1 H_2$ and $H_2 H_1$ involves the identity it results that these must be identical when the given condition is satisfied, and hence a first result is that $H_1 H_2$ must be a sub-

group of G. The assumption that $H_1 S_\alpha H_2 = H_2 S_\alpha H_1$ clearly implies that $H_1 H_2$ is invariant under S_α. That is, *whenever a double co-set as regards two permutable subgroups coincides with the inverse of a double co-set as regards the same two subgroups then the product of these subgroups is invariant under each of these double co-sets.* In particular, a necessary and sufficient condition that $H_1 H_2$ is an invariant subgroup under G is that each double co-set as regards H_1, H_2 is identical with the inverse of some double co-set as regards these subgroups. If either H_1 or H_2 is assumed to be the identity we obtain as a special case the theorem noted in the third paragraph of the Introduction.

When G or a quotient group of G is represented as a substitution group as regards H_1, the preceding results may also be employed to establish a useful criterion to determine when $H_1 H_2$ constitutes a subgroup of G. In fact, since $H_1 H_2$ is composed of all the operators of G corresponding to the substitutions which replace the letter (a) omitted in the subgroup corresponding to H_1 in this substitution group by the letters of a transitive constituent which involves a in the subgroup corresponding to H_2, it results that *a necessary and sufficient condition that $H_1 H_2$ is a group is that the transitive constituent which involves a in the subgroup corresponding to H_2 involves all the letters of one or more transitive constituents in the group corresponding to H_1 when G, or one of its quotient groups, is represented transitively as regards H_1 and a is the letter omitted in the group corresponding to H_1.*

The preceding theorem is a special case of another theorem which we proceed to establish. Since $H_1 H_2$ is composed of all the operators of G which correspond to the substitutions, in the transitive group to which H_1 gives rise, which replace the letter a omitted in all the substitutions corresponding to H_1 by all the letters of the transitive constituent involving a in the subgroup corresponding to H_2, the number of operators common to $H_1 H_2$ and $H_2 H_1$ can be directly determined from this substitution group. In fact, a necessary and sufficient condition that $H_1 H_2$ and $H_2 H_1$ have in common all the operators which correspond to the total number of substitutions which replace a by the letter c is that all the letters in the constituent to which c belongs in the subgroup corresponding to H_1 are found in the transitive constituent to which a and c belong in the subgroup corresponding to H_2. In particular, if all the letters in the latter constituent constitute the letters of two or more constituents in the group corresponding to H_1 it results that $H_1 H_2$ and $H_2 H_1$ are identical, as was proved in the preceding paragraph. This proves also that *$H_1 H_2$ cannot involve the inverses of all the operators of a double co-set with respect to H_1, H_2.*

The co-sets which contain the inverse of at least one of the operators in $H_1 H_2$ can readily be determined when G or a quotient group of G is represented with respect to H_1. In fact, if a letter in the transitive constituent involving a in the subgroup corresponding to H_2 is replaced, in the subgroup

corresponding to H_1, by a letter of another transitive constituent of the former of these two subgroups the double co-set corresponding to the latter constituent involves the inverse of an operator of $H_1 H_2$ and vice versa. To determine the double co-sets which involve the inverse of at least one of the operators of $H_1 H_2$ it is therefore only necessary to observe which of the transitive constituents of the subgroup corresponding to H_2 involves at least one letter that succeeds in the subgroup corresponding to H_1 a letter of the constituent involving a in the former subgroup. When a set of constituents, including the one involving a, of this subgroup involves all the letters of a set of constituents of the group corresponding to H_1, the letters of these constituents clearly represent a system of imprimitivity of the substitution group with respect to H_1. In particular this group is always imprimitive when $H_1 H_2 \equiv H_2 H_1 < G$.

When G is written as the sum of the subgroup H and a series of corresponding co-sets, as follows:

$$G = H + HS_2 + HS_3 + \cdots + HS_\rho,$$

the series of operators $S_2, S_3, \cdots, S_\rho$ may be so selected that the same totality of co-sets is obtained by replacing each of these operators by its inverse, as was observed in the opening paragraph. This can evidently also be done as regards double co-sets with respect to a single subgroup, but it cannot always be done as regards double co-sets with respect to two distinct subgroups. The truth of this statement may be verified if we let G be the transitive substitution group of order 32 and of degree 8 generated by the substitution $aebf \cdot cgdh$ and the two subgroups

$$H_1 = 1,\ eg \cdot fh,\ bd \cdot eg,\ bd \cdot fh, \qquad H_2 = 1,\ ac \cdot eg.$$

Hence it results that G must have special properties when it is possible to select the operators $S_2, \cdots, S_\lambda$ so that both of the following arrangements are possible when every operator of G is uniquely represented by the former:

$$G = H_1 H_2 + H_1 S_2 H_2 + \cdots + H_1 S_\lambda H_2,$$
$$= H_1 H_2 + H_1 S_2^{-1} H_2 + \cdots + H_1 S_\lambda^{-1} H_2.$$

From the theorem that $H_1 H_2$ cannot involve the inverses of all the operators of a double co-set with respect to $H_1 H_2$ it results that G may always be represented in these two ways if $S_2, \cdots, S_\lambda$ are properly chosen and $\lambda < 4$. It is also clear that this is always possible when H_1 gives rise to a doubly transitive substitution group, since all the double co-sets involve operators of order 2 in this special case.