SAME LEFT CO-SET AND RIGHT CO-SET MULTIPLIERS FOR ANY GIVEN FINITE GROUP *

BY G. A. MILLER

1. *Introduction.* Let G represent any group of finite order g and let H represent any subgroup of G. It is known that a set of distinct operators $s_2, s_3, \cdots, s_\lambda$ can always be so selected that every operator of G appears once and only once in each of the following two sets of augmented co-sets of G:

$$H + Hs_2 + Hs_3 + \cdots + Hs_\lambda,$$
$$H + s_2H + s_3H + \cdots + s_\lambda H.$$

This theorem was proved by means of the theory of substitution groups in the QUARTERLY JOURNAL OF MATHEMATICS (vol. 41 (1910), p. 382). A few years later H. W. Chapman gave an abstract proof of the same theorem in the MESSENGER OF MATHEMATICS (vol. 42 (1913), p. 132). In view of the facts that this theorem relates to very fundamental properties of a group and that errors appear in the latter article, we proceed to give here another abstract proof, and to develop a few new related theorems, as well as a generalization of the theorem itself.

2. *New Proof of the Theorem.* From the theory of double co-sets † it results that all the operators of G can be represented as follows:

$$H + Hs_\alpha H, \qquad (\alpha = 2, \cdots, \gamma).$$

For a particular value of α the double co-set $Hs_\alpha H$ represents all the operators of a certain number ρ of right co-sets and the same number of left co-sets. A necessary and sufficient condition that H be invariant under G is that $\rho = 1$ for every value of α. Hence an invariant subgroup can be defined as a subgroup which gives rise to no double co-set involving

* Presented to the Society, April 13, 1923.

† Cf. Miller, Blichfeldt and Dickson, *Finite Groups*, 1916, p. 24.

more distinct operators than the subgroup does. Every right co-set contained in $Hs_\alpha H$ has the same number of operators in common with every left co-set contained therein and vice versa.

The ρ right co-sets and the ρ left co-sets involved in the double co-set $Hs_\alpha H$ for a particular value of α can be placed in a (1, 1) correspondence in $\rho!$ ways. In any one such correspondence every two corresponding co-sets have exactly h/ρ common operators. As any one of these common operators can be used for the multiplier of the right co-set and the left co-set which correspond, these multipliers can be chosen in $(h/\rho)^\rho$ ways after the correspondence between the right co-sets and the left co-sets involved in $Hs_\alpha H$ has been established. Necessary and sufficient conditions that $h/\rho = 1$ are that G can be represented as a transitive substitution group with respect to H. When G is thus represented, the subgroup composed of all the substitutions which omit a given letter involves a regular group as transitive constituent corresponding to the double co-set $Hs_\alpha H$. In particular, H can contain no subgroup besides the identity which is invariant under G, and it cannot itself be an invariant subgroup of G when $h/\rho = 1$.

A necessary and sufficient condition that the double co-set $Hs_\alpha H$ for a particular value of α contain all the operators of G which are not found in H is that the transitive substitution group of degree λ to which H gives rise be at least doubly transitive.* In this theorem it is not assumed that this substitution group is simply isomorphic with G. In fact, this is a special case of the theorem that the number of the different double co-sets $Hs_\alpha H$ is equal to the number of the transitive constituents in the subgroup composed of all the substitutions which omit a given letter of the transitive group of degree λ to which H gives rise. A proof of this theorem results directly from the fact that a right co-set is composed of all the substitutions which replace by a given other letter the omitted

* A special case of this theorem was given by W. A. Manning, *Primitive Groups*, 1921, p. 41.

letter in the subgroup to which H corresponds in the transitive group of degree λ.

The double co-set $Hs_\alpha H$ either contains all the inverses of its operators or it contains no inverse of any operator included in it, since $Hs_\alpha^{-1}H$ is composed of the inverses of the operators contained in $Hs_\alpha H$. To obtain a set of operators $s_2, s_3, \cdots, s_\lambda$ which may be used both for right co-set multipliers and also for left co-set multipliers we may therefore proceed as follows: Let s_2 be an arbitrary operator of G which is not found in H. If s_2^{-1} does not appear in Hs_2 it cannot appear in s_2H and vice versa, since the right co-sets are composed of the inverses of the operators in left co-sets and vice versa. If s_2^{-1} does not appear in Hs_2 use it for s_3. The two right co-sets Hs_2 and Hs_2^{-1} will then be composed of the inverses of the operators of the two left co-sets $s_2^{-1}H$ and s_2H. If s_2^{-1} is in Hs_2 each of the co-sets Hs_2 and s_2H is composed of the inverses of the operators found in the other. In the latter case s_3 can be any operator of G such that its inverse is not in Hs_2 and it is not found in $H + Hs_2$. We proceed now in the same way with s_3 as with s_2.

This process may be continued until all the operators of G have been exhausted. If this were not the case we would reach a point when each of the two sets of augmented co-sets

$$H + Hs_2 + \cdots + Hs_\rho,$$
$$H + s_2H + \cdots + s_\rho H$$

would be composed of the inverses of the operators found in the other and each of the operators of G which does not appear in the former would have its inverse therein. Hence all of these operators would appear in

$$H + s_2H + \cdots + s_\rho H.$$

Since each of the operators of G appears in one or the other of the two given augmented ρ co-sets it results that if there are any additional right co-sets they can have no operator in common with any one of the additional left co-sets.

An additional right co-set could therefore not appear in a double co-set with respect to H which would involve an additional left co-set. If one of any two of the given corresponding $\rho - 1$ co-sets appears in such a double co-set the other must also appear therein. Hence it results that if any double co-set with respect to H should involve an additional right co-set it would also involve an additional left co-set. As this is impossible it follows that no additional co-set exists and hence $\rho = \lambda$.

3. *Related Theorems.* We have incidentally proved the following theorem: *If the multipliers of the right co-sets, or of the left co-sets, with respect to the same subgroup are so chosen that the inverse of a multiplier is used as the multiplier of the following co-set whenever a co-set does not involve this inverse, and that the other multipliers satisfy the condition that neither they nor their inverses appear in any preceding co-set, then it cannot happen that there are remaining operators if all the inverses of such operators appear in the preceding co-sets.*

Each of the double co-sets with respect to H is evidently invariant under H. In fact, the ρ right co-sets which appear in $Hs_\alpha H$ constitute a complete set of conjugates under H, and this is also true of the ρ left co-sets which appear therein. To prove this fundamental theorem it is only necessary to note the conjugates of Hs_α under H. The number of these may be found by first finding the subgroup of H composed of all its operators which transform s_α into some operator of Hs_α. If $t_1, t_2, \cdots, t_k$ are the operators of this subgroup and if

$$s_\alpha, h_2 s_\alpha, \cdots, h_k s_\alpha$$

are the distinct operators into which s_α is transformed under this subgroup, then s_α is also transformed into

$$s_\alpha, s_\alpha h_2, \cdots, s_\alpha h_k$$

under H. That is, s_α is transformed into as many distinct operators in $s_\alpha H$ as in Hs_α by the operators of H, and vice versa.

The ρ right co-sets $Hs_2, \cdots, Hs_{\rho+1}$ which form a complete set of conjugates under H evidently include s_2H and hence they include the ρ conjugates of s_2H under H. Hence we have the following theorem: *The double co-set $Hs_\alpha H$ is composed of the right co-sets which form a complete set of conjugates under H of the right co-set Hs_α. It coincides also with the complete set of conjugates under H of the left co-set $s_\alpha H$.*

4. *Generalized Theorem.* A double co-set of G with respect to two distinct subgroups does not have all the properties noted above of the double co-set with respect to a single subgroup. In particular, the former may involve the inverses of some of its operators without involving the inverses of all of them, as can readily be verified. On the other hand, every right co-set involved in the double co-set H_1sH_2 with respect to two distinct subgroups has the same number of operators in common with each of the left co-sets involved therein, and vice versa. This follows directly from the fact that the operators of $s^{-1}H_1s$ are equally distributed in the left co-sets with respect to H_2 of the double co-set $s^{-1}H_1s \cdot H_2$. The double co-set H_1sH_2 involves a certain number of right co-sets with respect to H_1 and a certain number of left co-sets with respect to H_2. Since the operators of each of these right co-sets are equally distributed among all of these left co-sets, and vice versa, it results that *it is always possible to select the multipliers in such a way that those of the right co-sets contained in H_1sH_2 are the same as those of the left co-sets contained therein whenever H_1 and H_2 have a common order, and that all the multipliers for the larger subgroup are included among those for the smaller when they have different orders.*

This theorem may be regarded as a double generalization of the one noted in the opening paragraph. In fact, when H_1 and H_2 have a common order but are distinct groups, the present theorem includes the former, and when H_1 and H_2 have different orders there results a further generalization. Hence the present note furnishes a generalization as well as a new proof of the theorem in question.

THE UNIVERSITY OF ILLINOIS