

## ON THE COMMUTATORS OF A GIVEN GROUP.

BY DR. G. A. MILLER.

LET  $s_1, s_2, s_3, \dots, s_g$  represent all the operators of a given group  $G$ , and let  $t$  represent any operator whatsoever. From the identities

$$s_\beta^{-1} s_a^{-1} t^{-1} s_a t s_\beta \equiv (s_a s_\beta)^{-1} t^{-1} s_a s_\beta t \cdot t^{-1} s_\beta^{-1} t s_\beta, \quad (a, \beta < g + 1)$$

$$s_\beta^{-1} t^{-1} s_a^{-1} t s_a s_\beta \equiv (t s_\beta)^{-1} s_a^{-1} t s_\beta s_a \cdot s_a^{-1} s_\beta^{-1} s_a s_\beta$$

we observe that the transform, with respect to any operator of  $G$ , of the commutators formed with  $t$  and the operators of  $G$  is the product of two such commutators. All of these commutators must, therefore, form a group which is transformed into itself by  $G$ . When  $t$  transforms  $G$  into itself the given commutators generate the smallest self-conjugate subgroup of  $G$  which has the property that all of the operators of the corresponding quotient group are commutative to  $t$ ; i. e.,  $t$  transforms each of the divisions of  $G$  with respect to this self-conjugate subgroup into itself. By letting  $t$  represent, in succession, all the operators of  $G$  we arrive at the known theorem that the commutator subgroup of a group is the smallest self-conjugate subgroup with respect to which the group is isomorphic to an abelian group.\*

From the fact that the commutator subgroup of  $G$  is a characteristic subgroup it follows that it is self-conjugate in every group that contains  $G$  self-conjugately. In particular, if  $G$  is of order  $p^\alpha$  and is not the abelian group of the type  $(1, 1, 1, \dots, 1)$ , then every group that contains  $G$  self-conjugately must also contain a self-conjugate subgroup of order  $p^\beta$ ,  $\alpha > \beta > 0$ . When  $G$  is the abelian group of the type  $(1, 1, 1, \dots, 1)$ , it is clearly always possible to construct a group which contains  $G$  self-conjugately and which transforms none of the subgroups of  $G$  besides identity into itself.†

If  $t$  remains fixed in the commutator  $C \equiv s^{-1} t^{-1} s t$  while  $s$  is multiplied on the left by all the operators of  $G$  we observe that  $C$  remains unchanged when this multiplier is commutative to  $t$  and that it is changed for every other multiplier. Arranging all the operators of  $G$  in the following

---

\* *Quar. Jour. of Math.*, vol. 28 (1896), p. 268.

† Moore, *BULLETIN*, vol. 2 (1896), p. 33.

manner, the first row being composed of the operators that are commutative to  $t$ ,

$$\begin{array}{ccccccc} 1, & s_2, & s_3, & \cdots & s_\gamma, \\ r_2, & s_2 r_2, & s_3 r_2, & \cdots & s_\gamma r_2, \\ r_3, & s_2 r_3, & s_3 r_3, & \cdots & s_\gamma r_3, \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ r_\lambda, & s_2 r_\lambda, & s_3 r_\lambda, & \cdots & s_\gamma r_\lambda, \end{array}$$

$C$  has the same value when  $s$  is multiplied on the left by each one of the  $\gamma$  operators of a row, and if  $s$  is multiplied by two operators from different rows the corresponding values of  $C$  must evidently be different. Hence  $C$  has just  $\lambda = g \div \gamma$  distinct values when  $s$  is multiplied by all the operators of  $G$  and each value of  $C$  corresponds to the same number of operators of  $G$ . This result is independent of whether  $s$  or  $t$  belong to  $G$  or not. When  $s$  belongs to  $G$  we may say that  $C$  has  $\lambda$  distinct values when  $s$  is successively replaced by all the operators of  $G$  and that each value of  $C$  corresponds to the same number of the operators of  $G$ .

While  $C$  has the same number of different values as  $t$  has conjugates when it is transformed by all the operators of  $G$ , yet these different values of  $C$  need not include any of these conjugates of  $t$  nor is it necessary that these form a complete system of conjugates with respect to the operators of  $G$ , *e. g.*, when  $t$  is one of the operators of order three in the alternating group of order twelve while  $s$  assumes successively all the values of the operators of this group, the four values of  $C$  are the operators of order two and identity. If  $s$  had assumed all the values of the operators of the symmetric group of order twenty-four,  $C$  would have assumed the values of four operators of order three in addition to the given four values.

The following two equations

$$\begin{aligned} a_1 a_2 \cdot b_1 b_2 \cdot c_1 c_2 \cdot \cdots \cdot l_1 l_2 \cdot m_1 m_2 &\times a_2 b_1 \cdot b_2 c_1 \cdot \cdots \cdot l_2 m_1 \\ &= a_1 b_1 c_1 \cdots m_1 m_2 l_2 \cdots c_2 b_2 a_2, \\ a_1 a_2 \cdot b_1 b_2 \cdot c_1 c_2 \cdot \cdots \cdot k_1 k_2 \cdot l_1 l_2 &\times a_2 b_1 \cdot b_2 c_1 \cdot \cdots \cdot k_2 l_1 \cdot l_2 m \\ &= a_1 b_1 c_1 \cdots k_1 l_1 m l_2 k_2 \cdots c_2 b_2 a_2 \end{aligned}$$

show that every substitution is the product of two substitutions of order two that do not involve any element except those involved in the given substitution.\* The given sub-

\* It may be observed that each of these substitutions transforms the given product into its inverse.

stitutions of order two are similar when the given cyclical product involves an odd number of letters; when this product involves an even number of letters, one of the given substitutions of order two contains one more transposition than the other. Hence every positive substitution is the product of two similar substitutions of order two. Since these two similar substitutions can be transformed into each other by some substitution we have the theorem:

*Every positive substitution is the commutator of two substitutions involving only elements that are contained in the given positive substitution.*

From the following examples we see that any circular substitution of an odd order is the product of two similar circular substitutions which may have either one or three common elements,

$$\begin{aligned}
 a_1 a_3 \cdot a_1 a_2 &= a_1 a_3 a_2 \\
 a_1 a_2 a_3 \cdot a_1 a_2 a_3 &= a_1 a_3 a_2 \\
 a_1 a_3 a_4 \cdot a_1 a_2 a_3 &= a_1 a_3 a_4 a_2 a_3 \\
 a_1 a_2 a_3 a_4 \cdot a_1 a_2 a_3 a_5 &= a_1 a_3 a_4 a_2 a_5 \\
 \dots & \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots \\
 a_1 a_3 a_4 \cdots a_{n+2} \cdot a_1 a_2 a_{n+3} a_{n+4} \cdots a_{2n+1} \\
 &= a_1 a_3 a_4 \cdots a_{n+2} a_2 a_{n+3} a_{n+4} \cdots a_{2n+1} \\
 a_1 a_2 a_3 \cdots a_{n+2} \cdot a_1 a_2 a_3 a_{n+3} a_{n+4} \cdots a_{2n+1} \\
 &= a_1 a_3 a_4 \cdots a_{n+2} a_2 a_{n+3} a_{n+4} \cdots a_{2n+1}
 \end{aligned}$$

Hence we observe that any cycle of an odd order greater than three is the product of two smaller similar cycles each of which is of an odd order. It is evident that the two given similar cycles can always be transformed into the inverse of each other by some even substitution; *i. e.*, every positive cycle whose degree exceeds three is a commutator of two positive substitutions which do not involve any elements except those which are contained in the given cycle.

From the following equations, in which  $0 < 2a < n + 1$ ,

$$\begin{aligned}
 a_1 a_2 \cdots a_{n+1} \cdot a_1 a_{n+2} a_{n+3} \cdots a_{2n} a_{2a+1} \\
 &= a_1 a_2 \cdots a_{2a} \cdot a_{2a+1} a_{2a+2} \cdots a_{2n}, & n > 1 \\
 a_1 a_2 \cdots a_{n+2} \cdot a_1 a_2 a_3 a_{n+3} a_{n+4} \cdots a_{2n} a_{2a+2} \\
 &= a_1 a_3 a_4 \cdots a_{2a+1} \cdot a_{2a+2} a_{2a+3} \cdots a_{n+2} a_{2a+3} \cdots a_{2n}, & (n > 2),
 \end{aligned}$$

we observe that two negative cycles of degrees  $2a$  and  $2(n-a)$  are always the product of two positive cycles in-

volving the same elements and of degree  $n + 1$  if  $n$  is even but of degree  $n + 2$  if  $n$  is odd. Since not all the elements of these positive cycles are common, one of them may always be transformed into the inverse of the other by some positive substitution involving the same elements.\* We have now proved that every positive substitution which does not include a cycle of order three is the commutator of two positive substitutions that do not involve any element except those of the given positive substitution. If a positive substitution consists of a cycle of order three it is evidently a commutator of positive substitutions with five but no smaller number of elements. If it contains a cycle of order three and some other elements it can clearly be expressed as the product of two positive substitutions such that the one can be transformed into the inverse of the other by a positive substitution in the same elements. Hence

**THEOREM I.** *Every substitution of the alternating group of degree  $n$  ( $n > 4$ ) is a commutator of two substitutions of the same group.*

The inverse of each of the two similar cycles having one common element whose product may be made any desired odd cycle can evidently be transformed into the other by a substitution of any arbitrary order. Hence any odd cycle is the product of two similar substitutions whose order is entirely arbitrary. Similarly we observe that any two negative cycles are the product of two similar substitutions whose order is arbitrary. In particular, any given operator is the product of two operators of the same arbitrary order. Hence the commutators of two operators may be employed to give a very simple proof of this special case of the general theorem. If  $l, m, n$  are any integers greater than unity it is always possible to find three operators  $L, M, N$  whose orders are  $l, m, n$  and which satisfy the relation  $L = MN$ .

The holomorph of a cyclical group is evidently isomorphic to an abelian group with respect to this cyclical subgroup.† When the order of the given cyclical group is odd the given holomorph must contain systems of conjugate operators each of which includes as many operators as the order of the given cyclical subgroup. When this order is even the number of conjugates in a system must be half as large. Hence

**THEOREM II.** *If the order of a cyclical group is odd, it is the commutator subgroup of its holomorph and all its operators are*

\* Since  $ab \cdot cd$  and  $abcd \cdot ef$  are the commutators of  $abc, ad \cdot bc$  and  $bdec, ac \cdot ef$  respectively, we do not need to consider the cases when  $n = 2$  or  $3$ . In fact, the general method is not directly applicable to these cases.

† Cf. Burnside, *Theory of Groups*, 1897, p. 240.

commutators of this holomorph. When this order is even, the commutator subgroup of the holomorph includes half of the operators of this cyclical group and all of these operators are commutators of this holomorph.

Since  $s^{-1}t^{-1}$  is similar to  $ts$  and this is similar to  $st$ , we observe that the commutator of two operators is similar to the commutator formed by means of one of these operators and the inverse of the other. The preceding results are, in part, supplementary to those contained in the paper "On the commutator groups," BULLETIN, Vol. IV., pp. 135-139.

CORNELL UNIVERSITY.

### THE CALCULUS OF GENERALIZATION.

*Calcul de Généralisation.* Par G. OLTRAMARE, Doyen de la Faculté des Sciences de l'Université de Genève. Paris, A. Hermann, 1899. 8vo, viii + 191 pp.

THIS work is the magnum opus of the venerable dean of the faculty of sciences, of Geneva, who is probably the oldest living pupil of Cauchy. The volume recapitulates and completes the works of the author published during the last twenty years.

Oltramare regards every function as developable in a series of exponentials; thus,  $a$  designating an independent variable, he puts

$$\varphi(a) = A_a e^{a\alpha} + A_\beta e^{\beta a} + A_\gamma e^{\gamma a} + \dots,$$

where  $\alpha, \beta, \gamma, \dots$  are any constants real or imaginary, in number finite or infinite. He adopts the shorter notation  $Ge^{au}$  for the series  $\sum A_u e^{au}$ ,  $u$  taking successively the values  $\alpha, \beta, \gamma, \dots$ , and the equation

$$\varphi(a) = Ge^{au}$$

then expresses that the function  $\varphi(a)$  is generated from  $e^{au}$  by generalization.

This is in fact an extension of Liouville's generalized derivatives; the latter defined the derivative of index  $\mu$  of the function  $\varphi(a)$  as given by the equation

$$\frac{d^\mu \varphi}{da^\mu} = A_a e^{a\alpha} \alpha^\mu + A_\beta e^{\beta a} \beta^\mu + A_\gamma e^{\gamma a} \gamma^\mu + \dots;$$

and Oltramare proposed to construct a more general calculus\* by considering expressions of the form

\* See Laisant's introduction to Oltramare's lithographed essay on the calculus of generalization published previously.