FINITE GROUPS REPRESENTED BY SPECIAL MATRICES*

BY

G. A. MILLER

The direct object of this paper is to prove that every possible finite group which contains an abelian subgroup of half its own order can be represented by square matrices all of whose elements are equal to zero with the exception of those which appear in one of the diagonals, and these are all ordinary complex numbers. The fact that every finite group which can be represented by such matrices must contain an abelian subgroup of half its own order is at once evident. The proof of the stated theorem may be based upon several interesting theorems relating to a possible choice of the independent generators of an abelian group. As these auxiliary theorems seem to be quite fundamental, we proceed to develop them in a somewhat more general form than would be necessary for the particular application in view.

1. Independent generators of an abelian group corresponding to a set of independent generators of a quotient group

Let G be any abelian group of order p^m, p being a prime number, and let H represent an arbitrary subgroup of G. If $s_1, s_2, \cdots, s_\lambda$ represent a set of independent generators of G which has been so chosen that as many as possible of these generators are found in H, it is evident that the number of the latter generators cannot exceed λ diminished by the number of independent generators of the quotient group G/H, since at least one independent generator of G in every possible set of such generators must correspond to some power, whose exponent is prime to p, of each operator in every possible set of independent generators of this quotient group. It is, however, not always possible to find a set of independent generators of G such that the number of those contained in H is equal to this upper limit. In fact, if G is of order p^4 and has two independent generators s_1, s_2 of orders p and p^3 respectively, and if we let H represent the subgroup of G which is generated by $s_1 s_2^p$, it is evident that G/H is the cyclic group of order p^2 but that it is impossible to find a set of two independent generators of G such that one of them is contained in H.

The preceding considerations may serve to illustrate the following general

* Presented to the Society, January 1, 1916.

theorem: *If G is an abelian group of order p^m and if H is a subgroup of order p^α, then a set of independent generators of G can always be so selected that at most $m - \alpha$ of them are not contained in H whenever G contains more than $m - \alpha$ independent generators. Moreover, it is possible to construct a group having k independent generators and an arbitrary quotient group of order p^α such that the subgroup corresponding to the identity of this quotient group cannot involve more than $k - \alpha$ of the operators in any possible set of independent generators of the group.*

To prove the first part of this theorem it is only necessary to observe that if $t_1, t_2, \cdots, t_\gamma$ represent a set of independent generators of the quotient group G/H, it is possible to select a set of independent generators of G in such a way that all except one of them are contained in the subgroup corresponding to the group generated by $t_1^p, t_2, \cdots, t_\gamma$.[*] Let s_1 represent this excepted independent generator of G and consider the subgroup of G generated by the remaining independent generators $s_2, \cdots, s_\lambda$ in any possible set involving s_1. If the order of t_1 exceeds p the independent generators of this subgroup can be selected in such a way that either all of them or all of them with the exception of one are contained in the subgroup of G which corresponds to the subgroup generated by $t_1^{p^2}, t_2, \cdots, t_\gamma$ in the given quotient group. As this process can be continued until we reach the identity in the quotient group, the first part of the theorem in question has been established.

To prove the second part of this theorem we shall first let G be the group generated by β independent operators $s_1, s_2, \cdots, s_\beta$ of orders $p, p^3, \cdots, p^{2\beta-1}$ respectively; and assume that the subgroup H is generated by the $\beta - 1$ independent operators $s_1 s_2^p,\ s_2 s_3^p,\ \cdots,\ s_{\beta-1} s_\beta^p$. The quotient group G/H is cyclic and of order p^β. Since every operator of order p contained in H is generated by operators of G whose order exceeds the order of all the operators of H which generate this operator of order p it results that H cannot contain an independent generator of any possible set of independent generators of G.[†] This proves the second part of the theorem under consideration whenever G/H is cyclic.

The proof of the theorem when G/H is non-cyclic results almost immediately from what precedes. In fact, if this quotient group has a set of independent generators $t_1, t_2, \cdots, t_\gamma$ of orders $p^{\beta_1}, p^{\beta_2}, \cdots, p^{\beta_\gamma}$ respectively, it is possible to construct a G having $\beta_1 + \beta_2 + \cdots + \beta_\gamma$ independent generators such that none of the operators of any one of the possible sets of independent generators of G appears in H. In fact, to construct such a group it is only necessary to employ successively the process explained in the preceding paragraph for each of the independent generators $t_1, t_2, \cdots, t_\gamma$.

[*] G. A. Miller, Tôhoku Mathematical Journal, vol. 5 (1914), p. 10.

[†] G. A. Miller, American Journal of Mathematics, vol. 27 (1905), p. 19.

The theorem which has just been established is a generalization of a theorem established by the present writer in the first article cited above. In the same article was established a necessary and sufficient condition that the subgroup H should contain a minimum number of the independent generators of G. In many considerations it is desirable to assume that a set of independent generators has been selected in such a manner that a given subgroup H involves a maximum number of the operators of this set. This maximum number can clearly not exceed the total number of independent generators of the group diminished by the number of independent generators in its quotient group with respect to H. In fact, it results from the preceding considerations that *a necessary and sufficient condition that a subgroup H of an abelian group G of order p^m can contain all the independent generators of G with the exception of one for each invariant of G/H is that the ratios of the orders of all the powers, besides the identity, of the independent generators of this quotient group and the lowest orders of the corresponding operators of G are equal to each other for the different powers of each independent generator of G/H.*

The maximum number of independent generators of an abelian group G of order p^m which can appear in a given subgroup H may be determined as follows: Select a set of independent generators $t_1, t_2, \cdots, t_\gamma$ of the quotient group G/H and select any operator s_α of lowest order which corresponds to the independent generator t_α, $1 \leqq \alpha \leqq \gamma$. The operator s_α clearly belongs to one of the possible sets of independent generators of G. If the order of t_α is p^{α_1} and if $s_\alpha^{p^\beta}$ is one of the operators of lowest order which correspond to $t_\alpha^{p^\beta}$ $(\beta = 1, 2, \cdots, \alpha_1 - 1)$ then a set of independent generators of G can be so selected that s_α is the only one which corresponds to the various powers of t_α which are not equal to the identity.

In general, the least number of independent generators of such a set which correspond to the various powers of t_α which differ from the identity is equal to one plus the number of times that the lowest order of an operator which corresponds to $t_\alpha^{p^\beta}$ is less than the pth power of the lowest order of an operator which corresponds to $t_\alpha^{p^{\beta-1}}$, $\beta = 1, 2, \cdots, \alpha_1 - 1$. By adding these least numbers for the different independent generators $t_1, t_2, \cdots, t_\gamma$ and subtracting the sum thus obtained from the total number of the independent generators of G there results a remainder which is exactly equal to the maximum number of operators belonging to a set of independent generators of G which can occur in the subgroup H.

In the following section it will be necessary to consider automorphisms of order 2 of an abelian group. It is well known that the multiplying group in such an automorphism is simply isomorphic with the quotient group with respect to the subgroup formed by the invariant operators under this automorphism and that each operator of this multiplying subgroup is transformed into its inverse under this automorphism. In particular, *if G is an abelian group of order p^m, p being an odd prime, and if t transforms G according to an automorphism of order 2, then G is the direct product of the subgroup formed by its invariant operators under t and the corresponding quotient group.* As all the operators of this quotient group are transformed into their inverses by t there results the known theorem that in any automorphism of order 2 of an abelian group of odd order it is always possible to select a set of independent generators in such a way that each of these generators is transformed under this automorphism either into itself or into its inverse.*

When the order of the abelian group G is 2^m, and t transforms G according to an automorphism of order 2, the invariant operators under t constitute a subgroup H and each operator of the quotient group G/H is again transformed into its inverse. In this case G is, however, not the direct product of this quotient group and H, since this quotient group must have at least one operator besides the identity in common with H. Hence we cannot always select the independent generators of G in such a way that each one is transformed into a power of itself by t. It results, however, from the preceding considerations that *if t transforms an abelian group G of order 2^m according to an automorphism of order 2 and if H is the subgroup of G formed by its operators which are invariant under t, then a set of independent generators of G can be so chosen that H contains all of them with the exception of at most three for each invariant of G/H.*

When three independent generators of G must correspond to a particular independent generator of G/H and its powers which differ from the identity in an automorphism of order 2 then these three independent generators must have three different orders and these generators can always be so chosen that the one of highest order is transformed under this automorphism into itself multiplied by the one of next lower order. The latter operator is then transformed into its inverse under this automorphism while the operator of lowest order in the given set of three independent generators is transformed into itself multiplied by a power of the independent generator of next to the highest order whose order is equal to that of this operator of lowest order.

In the other extreme case where a set of independent generators of G can be so selected that only one of these generators corresponds to an independent generator in G/H, this independent generator s must be transformed under this automorphism of order 2 into itself multiplied by an operator whose order is either equal to that of s or to just half of this order. The latter case can occur only when the order of G is 2^m. When the order of G is of this form the automorphism of order 2 can be so chosen that this multiplying operator is any operator whose order has either one of the two given values and

* G. A. Miller, These Transactions, vol. 10 (1909), p. 472.

which occurs in the co-set, with respect to H, involving s^{-2}. Finally, when two independent generators of G must correspond to the powers, which differ from the identity, of an independent generator in G/H, the order of the larger of these two generators is at least four times that of the smaller. If the latter cannot be so chosen that it is the multiplier of the former under this automorphism then the order of this multiplier is either exactly half the order of the former independent generator or twice the order of the latter.

2. Special matrices

To prove the theorem in question by means of the developments of the preceding section it seems desirable to direct attention to the following elementary facts. A square matrix in which each of the elements, with a possible exception of those of the principal diagonal, is equal to zero is called a *quasi-scalar matrix.* Since the product of two such matrices of the same order is a similar matrix in which each element of the principal diagonal is the product of the corresponding elements of the two factors, it results directly that a quasi-scalar matrix whose elements are ordinary complex numbers cannot represent an operator of a finite group unless each of its elements is either zero or a root of unity. In what follows it will be assumed that each of the elements of the principal diagonals of the quasi-scalar matrices under consideration is a root of unity.

A finite set of such quasi-scalar matrices of the same order generates an abelian group of finite order whose rank cannot exceed the common rank of these matrices. Moreover, the operators of every abelian group of rank r can be represented by a set of quasi-scalar matrices of order r. In particular, each operator of a given set of independent generators of an arbitrary abelian group of rank r can be represented by a matrix of order r having all the elements of its principal diagonal, with the exception of one, equal to unity while this one is a root of unity with an index equal to the order of the independent generator which it is to represent, and different independent generators are represented by differently located elements in such matrices.

A square matrix whose secondary diagonal is composed of ordinary complex numbers, none of which is zero, while each of the other elements is zero, will be called a *secondary diagonal matrix.* The product of two such matrices of order n

$$\begin{bmatrix} 0 & 0 & \cdots & a_1 \\ 0 & 0 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & a_{n-1} & \cdots & 0 \\ a_n & 0 & \cdots & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 & \cdots & b_1 \\ 0 & 0 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & b_{n-1} & \cdots & 0 \\ b_n & 0 & \cdots & 0 \end{bmatrix} = \begin{bmatrix} a_1 b_n & 0 & \cdots & 0 \\ 0 & a_2 b_{n-1} & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & a_n b_1 \end{bmatrix}$$

is a quasi-scalar matrix of order n in which the elements of the principal diagonal are the products of elements equidistant from the opposite extremities of the secondary diagonals of the factors. Hence it results that a necessary and sufficient condition that a secondary diagonal matrix whose elements are ordinary complex numbers generates a group of finite order is that the product of every pair of numbers equidistant from the extremities of its secondary diagonal is a root of unity.

A secondary diagonal matrix of order n transforms a quasi-scalar matrix of this order

$$\begin{bmatrix} 0 & 0 & \cdots & b_1 \\ 0 & 0 & \cdots & 0 \\ \cdot & \cdot & \cdot\;\cdot\;\cdot & \cdot \\ 0 & b_{n-1} & \cdots & 0 \\ b_n & 0 & \cdots & 0 \end{bmatrix}^{-1} \cdot \begin{bmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 \\ \cdot & \cdot & \cdot\;\cdot\;\cdot & \cdot \\ 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & a_n \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 & \cdots & b_1 \\ 0 & 0 & \cdots & 0 \\ \cdot & \cdot & \cdot\;\cdot\;\cdot & \cdot \\ 0 & b_{n-1} & \cdots & 0 \\ b_n & 0 & \cdots & 0 \end{bmatrix}$$

$$= \begin{bmatrix} a_n & 0 & \cdots & 0 \\ 0 & a_{n-1} & \cdots & 0 \\ \cdot & \cdot & \cdot\;\cdot\;\cdot & \cdot \\ 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & a_1 \end{bmatrix}$$

into a quasi-scalar matrix which may be obtained from the original quasi-scalar matrix by interchanging the numbers equidistant from the extremities of its principal diagonal. Moreover, the product of a quasi-scalar matrix of order n and a secondary diagonal matrix of this order is a secondary diagonal matrix of order n. Hence it results that *if a group of finite order is represented by quasi-scalar matrices and by secondary diagonal matrices of a common order this group must contain an abelian subgroup of half its order, which is composed of the operators represented by its quasi-scalar matrices.* In fact, the entire group may be abelian but the given subgroup composed of the quasi-scalar matrices *must* be abelian.

The fact that every abelian group can be represented by quasi-scalar matrices and that every abelian group of even order can be represented also by quasi-scalar and secondary diagonal matrices is evident. It is not quite so evident that every possible non-abelian group G which involves an abelian group H of half its order can be represented by quasi-scalar and secondary diagonal matrices. The case where the order of the H is either odd or twice an odd number is easily treated since in this case the independent generator of this subgroup can be represented by quasi-scalar matrices in such a way that a secondary diagonal matrix, whose square is an arbitrary one of these quasi-scalar matrices, transforms any arbitrary number of them into themselves and each of the remaining ones into its inverse, and every automorphism of period 2 of such an abelian group can be obtained in this way, as was observed in the preceding section.

Since Sylow subgroups of the same order must correspond to themselves in every possible automorphism of an abelian group it remains only to prove that quasi-scalar matrices representing independent generators of the Sylow subgroup of order 2^m in H can be so chosen that any possible automorphism of order 2 of this subgroup may be secured by the given secondary diagonal matrix. That this can be done results almost directly from the theorems established at the end of the preceding section. Hence the following theorem: *Every possible group which involves an abelian subgroup of half its own order can be represented by square matrices of a common order whose elements are all zero except those in one of the two diagonals, which are ordinary complex numbers.*