

GRAPHICAL METHOD OF FINDING THE POSSIBLE
SETS OF INDEPENDENT GENERATORS
OF AN ABELIAN GROUP.

BY PROFESSOR G. A. MILLER.

(Read before the American Mathematical Society, April 22, 1916.)

If the order of an abelian group G is not a power of a prime number, a set of independent generators of G can be obtained by taking an arbitrary set of independent generators of each of the Sylow subgroups of G and regarding the totality of operators in the sets thus obtained as a single set. This is true irrespective of which of the two common definitions of a set of independent generators may be adopted. According to one of these two definitions any set of l operators of G which generate G and are such that no $l - 1$ of them generate G is said to be a set of independent generators of G . This is sometimes called the general definition of a set of independent generators, and every possible group has at least one such set of independent generators. According to the restricted definition of a set of l independent generators, the additional condition is imposed that the group generated by every $l - 1$ of these operators has only identity in common with the group generated by the remaining one.

It is evident that not every possible group has a set of independent generators according to the restricted definition. For instance, the quaternion group does not have any such set of independent generators. It is well known that every possible abelian group has at least one set of independent generators according to each of these two definitions, and that the number of the operators in such a set is the same under both definitions whenever the group is of prime-power order and has at least one set of independent generators satisfying both definitions. The latter statement remains true even when the group of prime-power order is non-abelian.

Since the determination of a set of independent generators of an abelian group whose order is not a power of some prime number may be made to depend upon the determination of such a set of independent generators for each of its Sylow subgroups, irrespective of which of the two given definitions

of a set of independent generators is adopted, we shall confine ourselves, in what follows, to the consideration of the possible sets of independent generators of an abelian group G whose order is p^m , p being a prime number. For brevity it will always be assumed, in what follows, that the independent generators under consideration satisfy the restricted definition unless the contrary is explicitly stated.

Let H be the characteristic subgroup of G composed of the operators obtained by raising each operator of G to its p th power. The quotient group G/H is of type $(1, 1, 1, \dots)$, and if the order of this quotient group is p^k , G has exactly k independent generators. Moreover, whenever G has exactly k independent generators the order of this quotient group is p^k . None of the operators of H can be used as an independent generator of G , irrespective of which of the two definitions of independent generators is adopted. According to the general definition of independent generators, H is composed of all the operators of G which cannot appear in some one of the possible sets of independent generators of G ; that is, H is the ϕ -subgroup of G .

A necessary and sufficient condition that every operator of G which does not occur in H appears in at least one of the possible sets of independent generators of G is that no two invariants of G have a quotient which exceeds p , and a necessary and sufficient condition that all the operators of G which are not contained in H are conjugate under the group of isomorphisms of G is that all the invariants of G are equal to each other. When the latter condition is satisfied a set of independent generators of G can be chosen in

$$p^{mk-k^2}(p^k - 1)(p^k - p)(p^k - p^2) \dots (p^k - p^{k-1})$$

different ways. The first of the factors in this product represents the number of ways in which these independent generators can be selected after the co-sets from which they are to be taken have been determined, while the product of the other factors represents the number of ways in which these co-sets can be chosen.

Since the order of the group of isomorphisms of any abelian group is equal to the number of different ways in which a set of independent generators of the group can be selected, it results that the above formula represents the order of the group of isomorphisms of G whenever all the k invariants

of G are equal to each other and only then. The same formula clearly represents the number of ways in which a set of general independent generators of G can be chosen irrespective of whether the k invariants of G are equal to each other or do not have this property.

Suppose that a set of independent generators of G contains k_1 operators of order p^{α_1} , k_2 of order p^{α_2} , \dots , k_λ of order p^{α_λ} , $\alpha_1 < \alpha_2 < \dots < \alpha_\lambda$. Then $k_1 + k_2 + \dots + k_\lambda = k$, and G contains exactly $p^{k_1} - 1$ co-sets with respect to H which involve operators of order p^{α_1} but no operators of lower order. These co-sets together with H constitute a subgroup H_1 of G which includes all the operators of G whose orders do not exceed p^{α_1} . The co-sets which involve operators of order p^{α_2} , but no operators of lower order, together with H_1 constitute a subgroup H_2 of G which includes all the operators of G whose orders do not exceed p^{α_2} , etc.

A necessary and sufficient condition that any given operator of G appears in at least one set of independent generators is that it belongs to a co-set of G with respect to H and that it is one of the operators of lowest order in this co-set. If such an operator is of order p^α , the co-set in which it occurs has as many operators of order p^α as there are operators in H whose orders divide p^α , $\alpha_1 \leq \alpha \leq \alpha_\lambda$. Hence the following diagram

H		Co-sets of G as regards H whose smallest operators are of order			
		p^{α_1}	p^{α_2}	\dots	p^{α_λ}
Operators of H whose orders divide	p^{α_1}	Possible independent generators of order p^{α_1}	Possible independent generators of order p^{α_2}		
	p^{α_2}				
	\dots			\dots	Possible independent generators of order p^{α_λ}
	\dots				
	\dots				
	$p^{\alpha_\lambda - 1}$				

may serve to exhibit the operators from which a set of independent generators must be selected:

This diagram exhibits not only the operators from which the independent generators of different orders must be selected and the operators which cannot be used as such generators, but also the number of ways in which the independent generators of any possible order can be chosen. For instance, if G contains independent generators of order $p^{\alpha\gamma}$ and if $p^{\alpha\gamma}$ is the order of the subgroup of H which is composed of all its operators whose orders divide $p^{\alpha\gamma}$, then the k_γ generators of order $p^{\alpha\gamma}$ can be chosen in a number of ways represented by the following product:

$$p^{(\alpha'_\gamma + k_1 + k_2 + \dots + k_{\gamma-1})k_\gamma}(p^{k_\gamma} - 1)(p^{k_\gamma} - p) \dots (p^{k_\gamma} - p^{k_\gamma-1}),$$

where $k_{\gamma-1} = 0$ when $\gamma = 1$. The order of the group of isomorphisms of G is therefore equal to

$$\prod_{\gamma=1}^{\gamma=\lambda} p^{(\alpha'_\gamma + k_1 + k_2 + \dots + k_{\gamma-1})k_\gamma}(p^{k_\gamma} - 1)(p^{k_\gamma} - p) \dots (p^{k_\gamma} - p^{k_\gamma-1}).$$

Instead of considering the co-sets of G with respect to H we may consider the co-sets of H_1 with respect to H , then those of H_2 with respect to H_1 , etc. Finally, those of G with respect to $H_{\lambda-1}$ are considered for the purpose of finding the possible independent generators of highest order. According to this method, the determination of the possible sets of independent generators of G is simply a repetition of the process employed to determine the independent generators of G which are of order p^{α_1} and are contained in H_1 . This method of determining the possible sets of independent generators of G has contact with the method described by the writer in the *Tôhoku Mathematical Journal*, volume 2, 1912, page 137. Its main advantage is due to the fact that it exhibits clearly the operators which can appear in some possible set of independent generators.