

G. A. MILLER.

ON THE GROUP OF ISOMORPHISMS OF AN ABELIAN GROUP.
 (O GRUPIE IZOMORFIZMÓW GRUPY ABELOWEJ.)

STRESZCZENIE ARTYKUŁU.

Niechaj P będzie grupa abelowa rzędu p^a (p jest liczbą pierwszą), zaś P_1, P_2, \dots, P_a szeregi podgrup grupy $P = P_a$ rzędów, odpowiednio równych p, p^2, \dots, p^a , tak że każda z nich jest zawarta w następujących po niej. Każdy holomorfizm grupy P , który otrzymać można, dobierając operatory podgrupy P_β , nie znajdujące się w podgrupie $P_{\beta-1}$ tak, aby odpowiadały samym sobie, pomnożonym przez operatory podgrupy $P_{\beta-1}$, odpowiada operatorowi rzędu p^α w grupie izomorfizmów I_1 grupy P ; wszystkie operatory, których rzędy są potęgami liczby p , można otrzymać w tenże sam sposób.

Jeżeli generatory niezależne t_1, t_2, \dots, t_m grupy P są odpowiednio rzędów $p^{n_1}, p^{n_2}, \dots, p^{n_m}$, wtedy I_1 zawiera podgrupę abelową A , będącą wprost iloczynem m grup izomorfizmów grup cyklicznych, utworzonych osobno przy pomocy t_1, t_2, \dots, t_m . Liczba grup sprężonych grupy A pomiędzy grupami izomorfizmów I_1 równa się liczbie różnych układów podgrup, tworzących grupy P . Rząd podgrupy A jest $p^{a-m}(p-1)^m$ i obejmuje wszystkie operatory niezmiennicze izomorfizmów I_1 . Jedynie operatory grupy I_1 , przekształcające podgrupę A na samą siebie i nie zawarte w A , przekształcają m podgrupy cykliczne, utworzonych przez t_1, t_2, \dots, t_m na same siebie, przekształcając porządek niektórych z nich. Stąd podgrupa A jest niezmienna w grupie szerszej, niż nią jest sama, tylko wtedy, gdy przynajmniej dwie z tych podgrup mają rząd równy.

If the order of any abelian group (G) is written in the form:

$$g = 2^{\alpha_1} p_1^{\alpha_2} \cdots p_{m-1}^{\alpha_{m-1}},$$

(p_1, p_2, \dots, p_{m-1} being distinct primes) it is well known that G is the direct product of its m subgroups of orders $2^{\alpha_1}, p_1^{\alpha_2}, \dots, p_{m-1}^{\alpha_{m-1}}$ respectively. It is also known that the group of isomorphisms (I) of G is the direct product of the groups of isomorphisms of these m subgroups¹⁾. The group of isomorphisms (I_1) of any abelian group (P) whose order is p^a (p being any prime) is therefore of especial interest. By making all the operators of P correspond to the same powers of themselves, the $\varphi(p^a) = p^{a-1}(p-1)$ invariant operators of I_1 are obtained; where p^a is the highest order of any operator of P ²⁾. We proceed to consider the holomorphisms of P which correspond to subgroups of order p^4 in I_1 .

Let $P_1, P_2, \dots, P_{a-1}, P_a$ be any series of subgroups of $P = P_a$, whose orders are $p, p^2, \dots, p^{a-1}, p^a$ respectively, such that each is included in all those which follow it; and consider all the possible holomorphisms of P which may be obtained by multiplying the operators of these subgroups only by operators in a preceding subgroup. It follows from a known formula:

$$t^{-n} s_\alpha t^n = s_{\alpha+n} s_{\alpha+n-1} \cdots s_{\alpha+n-r}^{\frac{n(n-1)\cdots(n-r+1)}{r!}} \cdots s_{\alpha+1}^n s_\alpha,$$

where $t^{-1} s_\beta t = s_{\beta+1} s_\beta$ ($\beta = a, a-1, \dots, a-n$)³⁾ that each of these holomorphisms of P corresponds to an operator in I_1 whose order is a power of p .

The total number of these holomorphisms depends, in general, upon the type of P , the subgroup P_1 , and the way in which the subgroups P_2, \dots, P_{a-1} are chosen after P_1 has been selected. For instance, when P is cyclic, this

number is p^{a-1} and when P contains no operator of order p^2 it is $p^{\frac{a(a-1)}{2}}$. In these two cases it depends only upon the type of P . However, when P is of type $(a-1, 1)$ this number may clearly have either of the two values p^a , p^{a-1} , and is therefore not entirely determined by the type of P .

All of the possible holomorphisms which correspond to a particular series of subgroups such as P_1, P_2, \dots, P_a must correspond to a subgroup of order p^4 in I_1 . Moreover, from the fact that every invariant subgroup of any group of order p^m contains at least p invariant operators, it follows

that all the holomorphisms of P which correspond to a subgroup of order p^4 in I_1 can be obtained in the above manner. If two subgroups of order p , can be made to correspond in any holomorphisms of P the corresponding subgroups of order p^4 are conjugate under I_1 . It should, however, be observed that the subgroups which may be obtained by a different selection of P_2, \dots, P_{a-1} after P_1 has been chosen are not necessarily conjugate. In fact, they may have different orders.

Let t_1, t_2, \dots, t_m be any set of independent generators of P and suppose that their orders are $p^{a_1}, p^{a_2}, \dots, p^{a_m}$ respectively. Consider the holomorphisms of P in which each of the operators t_1, t_2, \dots, t_m corresponds to some power of itself. The total number of these holomorphisms is $p^{ma-m}(p-1)^m$ and it is easy to see that they correspond to an abelian subgroup (A) of I_1 which is the direct product of the m cyclic groups of orders $(p-1)p^{a_1-1}, (p-1)p^{a_2-1}, \dots, (p-1)p^{a_m-1}$ respectively. The only cyclic subgroups of P which correspond to themselves in all of these holomorphisms are powers of the separate independent generators t_1, t_2, \dots, t_m .

Since any set of independent generators of P may be made to correspond separately, in some holomorphism of P , with any other set, it follows that the number of conjugates of A under I_1 is equal to the number of different sets of independent generating subgroups of P . All of these conjugates have the $p^{a_i}(p-1)$ invariant operators of I_1 in common. The only operators of I_1 which transform A into itself without being included in A are those which transform the m cyclic subgroups generated by t_1, t_2, \dots, t_m into themselves but interchange their order. Since the generating subgroups of the same order may be permuted according to a symmetric group it is easy to determine the total number of different sets of independent generating subgroups of P . In particular, when no two of the operators t_1, t_2, \dots, t_m have the same order this number is the order of I_1 divided by the order of A .

In all the holomorphisms considered in the second and third paragraphs each of the subgroups P_1, P_2, \dots, P corresponds to itself. All the holomorphism of P in which this is the case correspond to a subgroup (I_2) of I_1 which contains only one maximal subgroup (I_3) whose order is of the form p^4 , viz. the subgroup considered above.

Let s_β be any operator of P_β which is not contained in $P_{\beta-1}$, $\beta = 1, 2, \dots, a$. In every holomorphism of P which corresponds to an operator of I_3 the product of s_β into some operator of $P_{\beta-1}$ corresponds to s_β . In the remaining holomorphisms under consideration the quotient group of some P_β with respect to $P_{\beta-1}$ must correspond to the $2, 3, \dots$, or $p-1$ power of itself; i. e. the totality of the operators s_β must correspond to one of these powers of itself.

¹⁾ Transactions of the American Mathematical Society, vol. 1, 1900, p. 396.

²⁾ Loc. cit., vol. 2, 1901, p. 260.

³⁾ Bulletin of the American Mathematical Society, vol. 7, 1901, p. 351.

In the particular case, when P involves no operator of order p^2 it is easy to see that the operators of each of these quotient groups may correspond independently to all of these powers, so that I_2 includes I_3 and the direct product of m cyclic subgroups of order $p-1$. In this case the quotient group of I_2 with respect to I_3 , $\frac{I_2}{I_3}$ is of order $(p-1)^m$. It is clear that this quotient group is always contained in the largest subgroup of A which includes no operator of order p and hence is always abelian irrespective of the type of P . We proceed to find its order.

To attain this end it is convenient to observe that after the independent generators of P have been selected in any particular manner, it is always possible, by changing at most one of them, to assume that any arbitrary operator of order p in P is a power of one of its independent generators. In the group generated by the remaining independent generators we may select an independent generator in the same manner, etc. Let P_α be the smallest of the subgroups $P_1, P_2, \dots, P_\alpha$ which contains an independent generator (t_1) of P such that the powers of t_1 include P_1 . Let P_{β_1} ($\beta \leqslant \alpha$) be the largest of these subgroups which is generated by t_1 . The operators of P_{β_1+1} which are not contained in P_{β_1} , $(P_{\beta_1+1} - P_{\beta_1})$ do not include any power of t_1 . If they include any operator of order p , this is necessarily true when $\beta_1 = \alpha$, let t_2 be the independent generator of P whose powers include this operator. It is clear that in the holomorphisms under consideration the independent generators t_1, t_2 can be made isomorphic with their various powers independently of each other.

On the other hand, if $P_{\beta_1+1} - P_{\beta_1}$ contains no operator of order p all its operators are of order p^{β_1+1} and t_2 may represent an independent generator of P which includes an arbitrary operator of order p obtained by multiplying one of these operators of order p^{β_1+1} into a power of t_1 . In this case the holomorphisms under consideration require that t_2 should correspond, to its γ power ($\gamma = 1, 2, \dots, p-1$) multiplied by an operator of P_{β_1} . whenever t_1 corresponds, to this power of itself. Let P_{β_2} be the largest of the subgroups $P_1, P_2, \dots, P_\alpha$ which is generated by t_1 and t_2 . None of these operators are found in $P_{\beta_1+1} - P_{\beta_1}$. If this contains an operator of order p the independent generator (t_3) of P whose powers include this operator, may again be made to correspond to its $1, 2, \dots, p-1$ powers independently of the correspondence of the others, etc. Hence the order of I_2 is equal to the order of I_3 multiplied by $(p-1)^l$, where l is the number of times that a set of operators like $P_{\beta_1+1} - P_{\beta_1}$ includes operators of order p .

A. PRZEBORSKI.

NIEKTÓRE ZASTOSOWANIA TEORYI KONGRUENCYJ LINIOWYCH.

W S T E P.

Początek teori kongruencyj liniowych, t. j. układów linij prostych w przestrzeni, których równanie zależy od dwu parametrów, dał Monge w 1781 r. w Rozprawach Akademii nauk w Paryżu. Dalsze rozwinięcie tej teorii w przypadku, w którym proste kongruencyi tworzą układ normalnych do pewnej powierzchni, znajdujemy w znakomitej pracy tego geometry: „Application de l'Analyse à la Géométrie” oraz w jego „Théorie des déblais et des remblais”. Badanie tego szczególnego przypadku kongruencyj liniowych wiąże Monge ściśle z nauką o krzywiznie powierzchni, t. j. z pytaniem, mającym znaczenie pierwszorzędne w teorii powierzchni.

Z innego zupełnie punktu widzenia rozważają kongruencye normalnych Malus i Dupin¹. Geometrowie ci doszli do badania tych kongruencyj przy rozpatrywaniu pytania o rozchodzeniu się światła w ośrodkach izotropowych, a zwłaszcza przy badaniu załamania i odbicia światła. Wynikiem tych badań był cały szereg twierdzeń, odgrywających ważną rolę w optyce geometrycznej. Najważniejsze z tych twierdzeń znajdziesz czytelnik w pierwszym rozdziale pracy niniejszej.

Szczególnie ważnym jest twierdzenie, noszące nazwę twierdzenia Malusa-Dupina; istota jego polega na tem, że układy promieni normal-

¹) Malus. Optique. Journal de l'École Polytechnique, XVI Cahier 1807.

²) Dupin, Sur les routes suivies par la lumière et par les corps élastiques en général dans les phénomènes de la réflexion et de la réfraction (Application de géométrie et de mécanique à la marine, aux ponts et chaussées, etc. Paris 1822).