METABELIAN GROUPS OF ORDER p^{n+m} WITH COMMUTATOR SUBGROUPS OF ORDER p^m*

BY

H. R. BRAHANA

INTRODUCTION

We consider a metabelian group G obtained by extending an abelian group H of order p^n and type $1, 1, \cdots$ by means of m operators $U_1, \cdots, U_m$ of order p from a Sylow subgroup of its group of isomorphisms. Every operator of $U=\{U_1, \cdots, U_m\}$ determines a partition of n and the fact that G is metabelian is equivalent to the requirement that no operator of U determine a partition of n in which the greatest term is greater than 2.† We require further that H be a maximal invariant abelian subgroup of G; this implies that no operator, except identity, in U determines a partition of n with greatest term smaller than 2. Throughout the first four sections we shall require that every operator of U, except identity, determine the partition $n=2+2+1+\cdots+1$. Such groups for $m=3$ as well as the groups such that every operator of U, except identity, determines the partition $n=2+1+\cdots+1$ have been classified.‡ In the case $m=3$ we found that there is but one group satisfying the conditions which we impose here, but the considerations necessary to show it indicated that extremely interesting results were to be found for larger values of m.

In §1 we suppose generators of G to satisfy a set of relations of a special type and are able to show that the problem of the classification of the resulting groups is exactly the problem of the classification of polynomials of degree m in a single variable x with coefficients in the modular field, mod p, under the group of projective transformations on x with coefficients also in the modular field. This is applied in §2 to the groups for $m=4$, where some obvious properties of the groups suggest a further analysis of the relation between polynomial and group. In particular it becomes apparent that the polynomial is in most cases independent of the special form of the generating relations used in §1; also there appears a group which belongs in the class but has no set of generators satisfying these special relations. In §3 it is shown that the classification of the groups with central of order p^{n-2} is equiva-

* Presented to the Society, April 6, 1934; received by the editors March 10, 1934.

† *On isomorphisms of abelian groups of type* 1, 1, $\cdots$, American Journal of Mathematics, vol. 56 (1934), p. 53.

‡ *On metabelian groups*, offered to the American Journal of Mathematics.

lent to the classification of matrices $M+xN$, where M and N are m-rowed square matrices with elements in the modular field, under "rational" projective transformations on x and "rational" elementary transformations on M and N simultaneously. This is extended in §5 to show the equivalence of the theory of groups with centrals of order p^{n-k} with the theory of matrices $x_1M_1+ \cdots +x_kM_k$ under the same set of transformations. In §4 the invariant factors of $M+xN$ are used to discover some of the properties of the groups.

1. A special case

Let the generators of H be $s_1, s_2, \cdots, s_n$. Let the generators of $G=\{H, U\}$ satisfy the following relations and no others except such as are consequences of these:

$$
\begin{gathered}
U_1^{-1} s_1 U_1 = s_1 s_4, \; U_2^{-1} s_1 U_2 = s_1 s_5, \qquad U_{m-1}^{-1} s_1 U_{m-1} = s_1 s_{m+2}, \\
U_1^{-1} s_2 U_1 = s_2 s_3, \; U_2^{-1} s_2 U_2 = s_2 s_4, \; \cdots, U_{m-1}^{-1} s_2 U_{m-1} = s_2 s_{m+1}, \\
U_m^{-1} s_1 U_m = s_1 s_3^{a_1} s_4^{a_2} \cdots s_{m+2}^{a_m}, \\
U_m^{-1} s_2 U_m = s_2 s_{m+2}.
\end{gathered}
\tag{1}
$$

The central of G is obviously of order p^{n-2}, being generated by $s_3, s_4, \cdots, s_n$, and the commutator subgroup is of order p^m, being generated by $s_3, s_4, \cdots, s_{m+2}$. If U contained an operator of type I, i.e. one which determines the partition $n=2+1+ \cdots +1$, then $\{s_1, s_2\}$ would contain an operator $s_1s_2^x$ permutable with some operator of U.* Any operator of U may be written $U'=U_1^{k_1}U_2^{k_2} \cdots U_m^{k_m}$. Transforming $s_1s_2^x$ by U' we have

$$
U'^{-1} s_1 s_2^x U' = s_1 s_2^x (s_4 s_3^x)^{k_1} (s_5 s_4^x)^{k_2} \cdots (s_{m+2} s_{m+1}^x)^{k_{m-1}} (s_3^{a_1} s_4^{a_2} \cdots s_{m+2}^{a_m} s_{m+2}^x)^{k_m} .
$$

The commutator in the above must be identity and we thereby obtain the following system of congruences linear and homogeneous in the k's,

$$
\begin{aligned}
xk_1 \qquad\qquad\qquad\qquad\qquad\qquad & + a_1k_m \equiv 0, \\
k_1 + xk_2 \qquad\qquad\qquad\qquad\qquad & + a_2k_m \equiv 0, \\
k_2 + xk_3 \qquad\qquad\qquad\quad & + a_3k_m \equiv 0, \\
\cdot \quad \cdot \quad \cdot \qquad\qquad\qquad\qquad & \quad \cdot \quad \cdot \quad \cdot \\
k_{m-2} + xk_{m-1} & + a_{m-1}k_m \equiv 0, \\
k_{m-1} & + (x + a_m)k_m \equiv 0.
\end{aligned}
$$

* Cf. the last reference where the question is considered for $m=3$.

The condition that the system have a solution is that the determinant of the matrix of coefficients be zero, which is

$$(2)\qquad x^m + a_m x^{m-1} - a_{m-1}x^{m-2} + a_{m-2}x^{m-3} - \cdots + (-1)^{m-1}a_1 \equiv 0, \bmod p.$$

This condition will not be satisfied by any x if the polynomial in (2) contains no linear factor in the modular field. Since there exist irreducible congruences of any degree it follows that $a_1, a_2, \cdots, a_m$ in (1) may be chosen so that U contains no operator of type I.

A different choice of generators $s_1, s_2, \cdots, s_n$ and $U_1, U_2, \cdots, U_m$ in the group G would be expected to result in a different congruence (2), it being understood that the new generators satisfy relations similar to (1) in that the commutator of U_i and s_2 is the same as that of U_{i-1} and s_1, $i=2, 3, \cdots, m$. We undertake to show first that if s_1 and s_2 are left unchanged and $U_1, U_2, \cdots, U_m$ are changed to any set which satisfy a set of relations similar to (1) then the congruence (2) remains unchanged.

It is evident that, since U is of order p^m and the commutator subgroups arising from transformation of s_1 and s_2 by U are both of order p^m, the choice of U_1 determines all the U's thereafter. We shall prove our statement by proving that (2) is unchanged

(a) by replacing U_1 by $U_1{}^k$,

(b) by replacing U_1 by U_2,

(c) by replacing U_1 by the product of U_i and U_j each of which gives the original congruence (2) when used for U_1.

If we replace U_1 by $U_1' = U_1{}^k$ the operators $U_2', U_3', \cdots, U_m'$ may be determined successively and it is obvious that they are $U_i' = U_i{}^k$. Consequently the commutator of U_m' and s_1 is

$$s_3^{a_1k}\, s_4^{a_2k} \cdots s_{m+2}^{a_mk}.$$

This operator expressed in terms of the preceding commutators is

$$s_3'^{a_1}\, s_4'^{a_2} \cdots s_{m+2}'^{a_m}.$$

This proves the statement for the case (a).

If we replace U_1 by $U_1' = U_2$, we have $U_i' = U_{i+1}$, $i=1, 2, \cdots, m-1$. The commutator of $U'_{m-1} = U_m$ and s_1 is

$$(3)\qquad s_3^{a_1} s_4^{a_2} \cdots s_{m+2}^{a_m}$$

and therefore we must have $U_m' = U_1{}^{a_1}U_2{}^{a_2} \cdots U_m{}^{a_m}$. Then the commutator of U_m' and s_1 is

$$(4)\qquad s_4^{a_1} s_5^{a_2} \cdots s_{m+2}^{a_{m-1}}(s_3^{a_1} s_4^{a_2} \cdots s_{m+2}^{a_m})^{a_m} = s_3^{a_1a_m}\, s_4^{a_1+a_2a_m}\, s_5^{a_2+a_3a_m} \cdots s_{m+2}^{a_{m-1}+a_m^2}$$

This may be expressed in terms of the preceding commutators $s'_{i-1}=s_i$, $i\leqq m+2$ and s'_{m+2} as given by (3). Or, if we evaluate

$$s_3'^{a_1} s_4'^{a_2} \cdots s_{m+2}'^{a_m}$$

in terms of $s_3, s_4, \cdots, s_{m+2}$, we have (4). This proves our statement for (b).

From the above facts it follows that (2) remains unchanged if U_1 is replaced by $U_1'=U_i^{k_i}$. Since the commutators are all permutable among themselves it follows that if U_i and U_j are such that each leaves (2) unchanged when used for U_1 in (1), then the product $U_1'=U_iU_j$ used for U_1 will determine a set $U_2', U_3', \cdots, U_m'$ and a set of commutators $s_3', s_4', \cdots, s'_{m+2}$ such that the commutator of U_m' and s_1 will be expressible as

$$s_3'^{a_1} s_4'^{a_2} \cdots s_{m+2}'^{a_m}.$$

This last relation holds regardless of whether or not the operators $U_1', U_2', \cdots, U_m'$ are independent, though we are interested only in the case where they are independent, as otherwise the U''s would not serve with H to generate G. This restriction is contained in (c). As a result of these considerations we have

(5) *The congruence* (2) *determined by a set of generators* $s_1, s_2, \cdots, s_n, U_1, U_2, \cdots, U_m$ *of* G *is independent of the choice of the* U*'s provided they are chosen from* $\{U_1, U_2, \cdots, U_m\}$ *and the commutators satisfy the relation*

$$U_{i-1}^{-1}s_1U_{i-1}s_1^{-1} = U_i^{-1}s_2U_is_2^{-1}, \qquad i = 2, 3, \cdots, m.$$

We consider next the effect of a new choice of generators of H. An essential of the relations (1) is that but two of the generators of H are outside the central of G, and since the congruence (2) depends on the form (1) it is obvious that a change in generators of H must be a change to a set of which but two are outside the central of G. If s_1 and s_2 are left fixed and $s_3', s_4', \cdots, s_n'$ are chosen from $\{s_3, s_4, \cdots, s_n\}$ the change amounts to a renaming of operators in the central and the commutator subgroup and does not affect the relations connecting operators. It is on these relations that (2) depends. Moreover, a choice

$$s_1' = s_1\prod_{i=3}^{n} s_i^{k_i}$$

and

$$s_2' = s_2\prod_{j=3}^{n} s_j^{k_j}$$

has no effect on (2), since the commutator of U_i and s_j' is the same as that of U_i and s_j. Consequently we need consider only the effect of a choice of s_1' and s_2' from the group $\{s_1, s_2\}$. We proceed to prove the following theorem:

(6) *If* $s_1'=s_1^as_2^b$ *and* $s_2'=s_1^cs_2^d$ *where* $s_1, \cdots, U_m$ *satisfy* (1) *and determine the congruence* (2), *then* $s_1', s_2', s_3, \cdots, U_m$ *satisfy a set of relations similar to* (1) *and determine a congruence which is obtained from* (2) *by subjecting* x *to the transformation* $x=(ax'+b)/(cx'+d)$.

To prove the theorem we need consider only the special cases

(a) $s_1' = s_1^a,\quad s_2' = s_2,$ and $x = ax',$

(b) $s_1' = s_1s_2,\quad s_2' = s_2,$ and $x = x' + 1,$

(c) $s_1' = s_2,\quad s_2' = s_1,$ and $x = 1/x'.$

It is not necessary to record the details of the computation here, for the operations are all rational. The two transformations, one on the generators of G and the other on the variable x, determine in each case the same transformation on the congruence (2). Any transformation on the generators of $\{s_1, s_2\}$ is a product of transformations of the above types; corresponding to it will be a product of transformations of the three types above on x. The matrices of the two products will be identical.

It results from the above considerations that the problem of the classification of groups whose generators satisfy (1) is exactly the problem of the classification of congruences (2), which have no roots in the modular field, under the group of projective transformations on the variable with coefficients in the modular field.

2. The groups G for $m=4$

The indicated classification of the congruences (2) has been carried out for $m=3$ and $m=4$.* These two cases present striking differences and the latter points the way to the results to be expected for a general m.

When $m=3$ and the left-hand side of (2), which we shall denote hereafter by $f(x)$, contains no linear factor in the modular field, then $f(x)$ is irreducible. This is not always true when $m=4$. All irreducible cubics are conjugate under the linear homogeneous group with coefficients in the modular field, and consequently any two groups G with a given H and $m=3$ are simply isomorphic. It is obvious that not all quartics with no linear factor are conjugate under that group, and further that not all irreducible quartics are conjugate under

* *On cubic congruences*, Bulletin of the American Mathematical Society, vol. 39 (1933), pp. 962–969; and *Irreducible quartic congruences*, also offered to the same Bulletin.

it, for a necessary condition for conjugacy is that their absolute invariants be the same. The identity of the absolute invariants is sufficient for conjugacy under the general projective group but not for conjugacy under its subgroup whose coefficients are in the modular field. If a given quartic is irreducible and a second quartic is conjugate to it under the general projective group but not under its "rational" subgroup, the second quartic is the product of two quadratic factors, one of which is irreducible.

When $m=4$ there are $p+1$ distinct groups G whose generators satisfy (1). They correspond to $p+1$ quartics none of which has a linear factor. We are not interested here in making the count of the polynomials, but rather in comparing groups corresponding to different types of polynomial and interpreting properties of the polynomials in terms of properties of the groups.

Let us denote the polynomial by $f(x)$. Let us consider an $f(x)$ of degree 4 which is the product of two irreducible quadratics. There exists a group G whose generators satisfy (1) where the a's are the coefficients of $f(x)$. For the sake of simplicity let us suppose that

$$f(x) = (x^2 - \lambda_1)(x^2 - \lambda_2)$$

where λ_1 and λ_2 are not squares. There is a group G' determined by H and four U's which satisfy the relations

$$\begin{aligned} &U_1^{-1}s_1U_1 = s_1s_4, \quad U_2^{-1}s_1U_2 = s_1s_3^{\lambda_1}, \quad U_3^{-1}s_1U_3 = s_1s_6, \quad U_4^{-1}s_1U_4 = s_1s_5^{\lambda_2}, \\ &U_1^{-1}s_2U_1 = s_2s_3, \quad U_2^{-1}s_2U_2 = s_2s_4, \quad U_3^{-1}s_2U_3 = s_2s_5, \quad U_4^{-1}s_2U_4 = s_2s_6. \end{aligned} \tag{7}$$

The generators which were selected for G' do not satisfy (1), nevertheless the condition that $\{U_1, \cdots, U_4\}$ contain no operator of type I is readily seen to be that $f(x)$ have no linear factor. Moreover, it can be shown that if λ_1 and λ_2 are distinct, generators of G' can be chosen which do satisfy (1). Such a set is obtained by taking $U_1' = U_1U_3$, in which case the resulting polynomial is $f(x)$. Therefore the two groups G and G' are simply isomorphic. From relations (7) it is easy to see that G', and consequently G, contains two subgroups $\{H, U_1, U_2\}$ and $\{H, U_3, U_4\}$ of order p^{n+2} each with commutator subgroup of order p^2. Looking at generators of G it is obvious that G, and consequently G', contains subgroups of order p^{n+2} with commutator subgroups of order p^3. These facts are dependent on the condition that $f(x)$ is the product of two distinct irreducible quadratics. If this condition is not satisfied there are two possibilities: (a) $f(x)$ is irreducible and then G contains no subgroup of order p^{n+2} with commutator subgroup of order p^2; and (b) $f(x)$ is the square of an irreducible quadratic, and G does not contain two subgroups of order p^{n+2} with commutator subgroups of order p^2 and with commutator subgroups distinct except for the identity. This last fact may be seen readily by considering a set of generators of G' which satisfy (7) where $\lambda_1=\lambda_2$. Such a group exists and determines the polynomial $f(x)=(x^2-\lambda_1)^2$. Every subgroup $\{H, U', U''\}$ has a commutator subgroup of order p^2 or of order p^4. G' cannot then be simply isomorphic with G whose generators satisfy (1) and whose polynomial is $f(x)$.

Granting that there are $p+1$ conjugate sets of quartics which have no linear factors, we are able to distinguish $p+2$ types of group G for $m=4$ which satisfy the conditions of the introduction. Of those there are $p+1$ which come under the special case of §1. We are able to separate these $p+2$ groups into three types by a consideration of their subgroups. Those with no subgroups of order p^{n+2} with commutator subgroup of order p^2 correspond to irreducible quartics. Those with such subgroups but also with subgroups of order p^{n+2} with commutator subgroup of order p^3 correspond to reducible quartics. The one with no subgroup of order p^{n+2} with commutator subgroup of order p^3 corresponds (not in the sense of §1) to the square of a quadratic.

An interesting question is that of the existence of some subgroup or set of subgroups by means of which we may distinguish among the $(p+1)/2$ groups whose quartics are irreducible and the $(p-1)/2$ groups whose quartics are products of two distinct quadratics. The question looks sufficiently interesting to warrant our posing it in detail for the simple case where $p=7$. The four conjugate sets of irreducible quartics are represented by

$$\begin{array}{ll}
\text{(a)} & x^4+4x^2+5x+2\equiv 0,\\
\text{(b)} & x^4+6x^2+4x+2\equiv 0,\\
\text{(c)} & x^4 \qquad\quad +2x+3\equiv 0,\\
\text{(d)} & x^4 \qquad\quad +4x+4\equiv 0.
\end{array}$$

Groups of order 7^{n+4} corresponding to these quartics are generated by operators satisfying (1) where

$$U_4^{-1}s_1U_4 = s_1s_k,$$
$$U_4^{-1}s_2U_4 = s_2s_6,$$

and s_k takes the respective forms

$$\text{(a)}\quad s_k=s_3^5s_4^5s_5^3,\quad \text{(b)}\quad s_k=s_3^5s_4^4s_5,\quad \text{(c)}\quad s_k=s_3^4s_4^2,\quad \text{(d)}\quad s_k=s_3^3s_4^4.$$

All of these groups are identical with respect to the following:

the order is 7^{n+4};

they are metabelian;

the central is of order 7^{n-2};

the commutator subgroup is of order 7^4;

G/H is abelian, of order 7^4 and type 1, 1, 1, 1;
every subgroup of order 7^{n+1} has a commutator subgroup of order 7^2;
no subgroup of order 7^{n+2} has a commutator subgroup of order 7^2;
every subgroup of order 7^{n+3} has a commutator subgroup of order 7^4.

It would seem that there is a possibility of difference in the numbers of subgroups of order 7^{n+2} with commutator subgroups of orders 7^3 and 7^4. However it seems extremely unlikely that such differences could correspond to the distinction implied by the differences in value of the absolute invariant of the corresponding quartics, especially since the absolute invariant does not distinguish between an irreducible and a reducible quartic.

While it is true that two groups which differ in the number of subgroups having a given property cannot be simply isomorphic, it is not to be assumed that the converse is true. There is no compelling reason to expect the non-isomorphism of two groups to be reflected in properties of their subgroups. Nevertheless, the author is not aware of any prior example where the non-isomorphism of two groups is not easily deducible from a consideration of their subgroups. The number of occasions where a number-theoretic argument is indispensable in the theory of groups is small, although the occasions themselves are crucial as is evidenced by the amount of the theory that depends on the existence of primitive roots in a Galois field.

3. Two general theorems

The statements of the last section for the case $m=4$ can all be established easily for that special case. The relation between properties of the polynomial $f(x)$ and properties of the group and the obvious direction in which a generalization of the results should proceed suggest a closer scrutiny of $f(x)$. This polynomial was obtained as the condition that U contain no operator of type I but it is obviously more important than that would imply. Also it seemed to be connected with a certain selection of the generators of U, but the last section has shown that it appears when the generators do not satisfy the conditions (1).

In this section we shall generalize the situation in §1 and we shall furnish incidentally the necessary proofs for the statements of §2. We require now only that G be metabelian, that the central and commutator subgroups be of orders p^{n-2} and p^m. We may assume in that case that a set of independent generators of H is chosen which contains m independent operators of the commutator subgroup and $n-2$ independent operators of the central. We also still require the U's to be of order p and permutable. The generalization consists in not requiring the generators of G to satisfy the relations (1). Under these conditions an independent set of relations on generators of G is completely described by a pair of m-rowed square matrices. We associate one matrix M with the operator s_1 and the other matrix N with s_2. We let the ith row of each matrix correspond to the generator U_i, and we let the jth column of each matrix correspond to s_{j+2}, where $s_3, s_4, \cdots, s_{m+2}$ are independent generators of the commutator subgroup of G. The elements in the ith row and the jth column of M and N are the exponents of s_{j+2} in the commutator of U_i with s_1 and s_2 respectively. For example, M and N for relations (1) are

$$M = \begin{pmatrix} 0 & 1 & 0 \cdots 0 \\ 0 & 0 & 1 \cdots 0 \\ \cdot & \cdot & \cdot \cdot \cdot \cdot \cdot \\ 0 & 0 & 0 \cdots 1 \\ a_1 & a_2 & a_3 \cdots a_m \end{pmatrix}, \qquad N = \begin{pmatrix} 1 & 0 & 0 \cdots 0 \\ 0 & 1 & 0 \cdots 0 \\ 0 & 0 & 1 \cdots 0 \\ \cdot & \cdot & \cdot \cdot \cdot \cdot \cdot \\ 0 & 0 & 0 \cdots 1 \end{pmatrix}.$$

In the case where the U's can be separated into sets each set satisfying (1), of which relations (7) describe the simplest case, the matrix M takes the form

$$M = \begin{pmatrix} M_1 & & & \\ & M_2 & & \\ \cdot & \cdot & \cdot & \cdot \\ & & & M_k \end{pmatrix},$$

where M_i is of the above form and all other elements are zeros. In this case also N is the identity matrix.

The congruence (2) is immediately recognizable as the condition for the vanishing of the determinant $|M+xN|$. The condition that the U's be all of type II is that $|M+xN|$ have no linear factor in the modular field. The general case requires no further argument in these respects.

A change of generators of the commutator subgroup amounts to replacing s_i, $i=3, 4, \cdots, m+2$, by

$$s_i' = s_3^{c_{i1}} s_4^{c_{i2}} \cdots s_{m+2}^{c_{im}},$$

where C, the matrix of the c_{ij}'s, is non-singular. The effect on M and N is to replace them by MC^{-1} and NC^{-1} respectively. Likewise a change in generators of U is equivalent to replacing U_i by

$$U_i' = U_1^{d_{i1}} U_2^{d_{i2}} \cdots U_m^{d_{im}},$$

where D is also non-singular. The effect of this is to replace M and N by DM and DN respectively. The theory of the groups described in the introduction is therefore equivalent to the theory of pairs of matrices with elements in a modular field.* Applying the theory of pairs of matrices we have the following theorem:

(8) *Two groups satisfying the conditions of the introduction and determined by M, N and M', N' are simply isomorphic if and only if $M+xN$ and $M'+xN'$ have invariant factors which are conjugate under some operator of the projective group of transformations on x with coefficients in the modular field.*

We proceed to our second theorem. We consider a group G whose generators satisfy (1) and determine the congruence $f(x)\equiv 0$. We suppose that G contains a subgroup $G'=\{H, V_1, \cdots, V_{m'}\}$ with commutator subgroup of order $p^{m'}$. Let the congruence determined by G' be $f'(x)\equiv 0$. We wish to prove that $f'(x)$ is a factor of $f(x)$. Let x_1 be a root of $f'(x)\equiv 0$.† Then by means of a set of linear homogeneous congruences similar to that preceding (2) x_1 determines a set of numbers $l_1, l_2, \cdots, l_{m'}$ such that $V_1^{l_1}V_2^{l_2}\cdots V_{m'}^{l_{m'}}$ is permutable with $s_1s_2^{x_1}$. The V's are expressible in terms of the U's and consequently the l's determine a set of numbers $k_1, k_2, \cdots, k_m$ such that $U_1^{k_1}U_2^{k_2}\cdots U_m^{k_m}$ is permutable with $s_1s_2^{x_1}$. Consequently, x_1 is a root of $f(x)\equiv 0$. Hence,

(9) *If G determines the congruence $f(x)\equiv 0$, if G contains a subgroup G' of order $p^{n+m'}$ with commutator subgroup of order $p^{m'}$, and if G' determines the congruence $f'(x)\equiv 0$ where the s_1 and s_2 used to determine $f'(x)$ are those used to determine $f(x)$, then $f'(x)$ is a factor of $f(x)$.*

These two theorems establish and generalize all the unsubstantiated statements of §2. The first determines a canonical form for the generating relations of G and the second interprets the irreducible factors of $f(x)$ in terms of subgroups of G.

4. Classification of the groups G and discussion of properties

It has been shown elsewhere‡ that m cannot be greater than $2n-4$, if U contains an operator of type II and no operator except those of types I and II. Since here we require every operator of U to be of type II it is obvious that m is limited by the order of the commutator subgroup. We must have $m\leqq n-2$. To find all the groups for a given m we may first determine all the conjugate sets of polynomials $f(x)$ of degree m under the "rational" linear fractional group. There exists at least one group for each conjugate set. If

* For the theory of pairs of matrices, cf. Dickson, *Modern Algebraic Theories*, 1930, p. 112.

† x_1 is not in the modular field. We beg to be excused from interpreting $s_1s_2^{x_1}$ and $V_1^{l_1}V_2^{l_2}\cdots V_{m'}^{l_{m'}}$. This, however, does not affect the argument.

‡ *On metabelian groups*, loc. cit.

$f(x)$ is irreducible, or if the irreducible factors of $f(x)$ are relatively prime, then there exists but one group for the conjugate set to which $f(x)$ belongs, for the invariant factors of $M+xN$ are $f(x)$, 1, 1, $\cdots$. Let us suppose that $f(x)$ has one irreducible factor $f_1(x)$ which is repeated, so that $f(x)=[f_1(x)]^r f_2(x)$ where the factors of $f_2(x)$ are relatively prime and prime to $f_1(x)$. Then the invariant factors of $M+xN$, having the property that each is divisible by all those which follow it and being such that their product is $f(x)$, may be selected in as many ways as there are partitions of r. The number of such groups is therefore $\theta(r)$. In general,

(10) *If $f(x)$ has the distinct irreducible factors $f_1(x), \cdots, f_k(x)$ and they appear to the powers $r_1, \cdots, r_k$, then the number of distinct groups G determined by $f(x)$ is equal to the product $\Pi_{i=1}^{k}\theta(r_i)$ of the numbers of partitions of the r_i's.*

Let us consider a group G and its corresponding polynomial $f(x)$ where the irreducible factors of $f(x)$ are relatively prime. The invariant factors of $M+xN$ are $f(x)$, 1, 1, $\cdots$. Generators of U and of the commutator subgroup may be chosen so that the transformed determinant $M'+xN'$ is in canonical form. If this is done the generators of G satisfy relations (1) where the a's are the coefficients of $f(x)$. Looking at the present case from another point of view let us suppose the irreducible factors of $f(x)$ to be $f_1(x), \cdots, f_k(x)$ of degrees $m_1, \cdots, m_k$. Let us consider k sets of U's, $U_{i1}, \cdots, U_{im_i}$, each set satisfying relations (1), the resulting commutator subgroups being distinct, all the U's being permutable, and the a's in (1) for the ith set being the coefficients of $f_i(x)$. The group generated by H, $U_{11}, \cdots, U_{km_k}$ obviously determines the congruence $f(x)\equiv 0$, and since its irreducible factors are relatively prime, the invariant factors of $M+xN$ are necessarily $f(x)$, 1, 1, $\cdots$. This group is therefore the same as the group described at the beginning of the paragraph. Consequently, when the irreducible factors of $f(x)$ are relatively prime, G contains a set of k subgroups of orders p^{n+m_i}, $i=1, \cdots, k$, with commutator subgroups of orders p^{m_i}, and G contains no other subgroup of order $p^{n+\alpha}$ with commutator subgroup of order p^α except such as are obtained by combining these. In fact these subgroups are characteristic.

The essential condition on G in order that it be possible to write the two sets of generating relations made use of above is that the invariant factors be all unity except one. This may still hold if some or all of the irreducible factors are repeated. In that case, however, there will exist subgroups of order $p^{n+\alpha}$ with commutator subgroups of order p^α where α is not one of the m_i's, or a combination of them. Let us suppose that $f(x)=[f_1(x)]^r$, where $f_1(x)$ is irreducible and of degree m_1, and let us suppose further that the invariant factors of $M+xN$ are $f(x)$, 1, 1, $\cdots$. Now let us consider two sets of $(r-1)m_1$

and m_1 U's respectively. Let the first set satisfy relations (1) where the a's are the coefficients of $[f_1(x)]^{r-1}$. Let the second set determine with H a group whose commutator subgroup is of order p^{m_1+1}, and let the commutator subgroup determined by the two sets be of order p^m. This can obviously be done by selecting the commutator of U_m and s_1 from the group generated by the rm_1 commutators which precede it and not in either of the groups generated by the first $(r-1)m_1$ or the last m_1 commutators. Clearly this commutator of U_m and s_1 can be chosen so that the invariant factors of $M+xN$ are $f(x)$, 1, 1, $\cdots$, since it is simply a question of requiring the canonical form of $M+xN$ to have certain coefficients and there is so much freedom in the choice of the commutator. From this it follows that the group G contains at least one subgroup of order $p^{n+\alpha}$ with commutator subgroup of order p^α where $\alpha=km_1$ and k is any number from 1 to r.

If in the above case we selected the commutator of U_m and s_1 in the group generated by the preceding m_1 commutators and selected it so that the congruence determined by H and the set of m_1 U's was $f_1(x)$, we should have the canonical form for $M+xN$ with invariant factors $[f_1(x)]^{r-1}, f_1(x)$, 1, 1, $\cdots$. In this case G contains two groups of order p^{n+m_1} with commutator subgroups of order p^{m_1}. The two sets of U's which determine these groups give with H a group of order p^{n+2m_1} with commutator subgroup of order p^{2m_1} none of whose subgroups of order p^{n+m_1} has a commutator subgroup of order p^{m_1+1}.

The effects on G of an increase in the number of repeated factors of $f(x)$ or of the invariant factors of $M+xN$ different from unity can be determined by considerations similar to the above. Rather than pursue this further we shall give a brief description of the groups G for $m=6$. We omit $m=5$ because in that case $f(x)$ could have no repeated factors.

When $m=6, f(x)$ may be (1) irreducible, (2) the product of an irreducible quartic and a quadratic, (3) the product of two irreducible cubics, or (4) the product of three quadratics.

Case (1). There are as many groups as there are conjugate sets of irreducible sextics under the "rational" projective group, a number as yet undetermined. None of these groups has a subgroup of order $p^{n+\alpha}$ with commutator subgroup of order p^α, $\alpha<6$.

Case (2). The quartic may be transformed into one of $(p+1)/2$ depending on the value of the absolute invariant. The operator of order $2i$, $i=1, 2$, which transforms the quartic into itself transforms its roots into their $p^{2/i}$th powers and consequently transforms every element in the Galois field determined by it into its $p^{2/i}$th power. The roots of the quadratic are in that $GF(p^4)$ and the quadratic is also transformed into itself. Therefore for each of the $(p+1)/2$ quartics there are as many groups as there are irreducible quadratics belonging to the modular field. This number is $p(p-1)/2$. The number of groups is $p(p^2-1)/4$. Each of the groups has generators which satisfy relations (1). Each has subgroups of orders p^{n+2} and p^{n+4} with commutator subgroups of orders p^2 and p^4 respectively, and no other subgroups of order $p^{n+\alpha}$ with commutator subgroup of order p^α.

Case (3). One of the cubics can be transformed into a given irreducible cubic and no further specialization may be made. The other cubic may then be any one of $p(p^2-1)/3$, one of which is the first one. There are therefore $(p^3-p+3)/3$ groups of this kind. All but one have generators which satisfy relations (1). The odd group contains no subgroups of order p^{n+3} with commutator subgroup of order p^4. One other contains one subgroup of order p^{n+3} with commutator subgroup of order p^3, and all the others contain two.

Case (4). One of the quadratics can be transformed into $(x^2-\lambda)$ and a second into one of $(p+1)/2$ quadratics which are taken one from each of the conjugate sets of quadratics under the group which leaves $(x^2-\lambda)$ fixed. Having decided which of the three quadratics are first and second and having transformed them to the desired form, no other simplification is possible. Hence, the third quadratic may be any one of $p(p-1)/2$. If the three quadratics are the same, then we may suppose $f(x)$ to be $(x^2-\lambda)^3$ and there are three groups: one, corresponding to the invariant factors $f(x), 1, 1, \cdots$, which contains subgroups of orders p^{n+2} and p^{n+4} with commutator subgroups of orders p^3 and p^5 respectively; one, corresponding to invariant factors $(x^2-\lambda)^2$, $(x^2-\lambda)$, $1, 1, \cdots$, which contains subgroups of the first type but none of the second; and one, corresponding to invariant factors $(x^2-\lambda)$, $(x^2-\lambda)$, $(x^2-\lambda)$, $1, 1, \cdots$, which contains no subgroups of either type. If two of the quadratics are the same and the third is distinct from this, we may transform the repeated one into $(x^2-\lambda)$ and then the third may be any one of $(p-1)/2$. For each of these there are two groups, according as one or two of the invariant factors of $M+xN$ are different from one. The two groups corresponding to the same $f(x)$ are again distinguished by their subgroups of order p^{n+2}. There are $p-1$ of these groups. If the three quadratics are distinct, $f(x)$ can be reduced to one of $(p-1)(p^2-p-4)/4$ forms, but the reduction can be made in more than one way since it involved the selection of a first and a second quadratic. A different selection of the first and second quadratics may or may not change $f(x)$, depending on the relations of the three quadratics. We shall not make the count of the number of groups, but shall note that for each such $f(x)$ there is but one group, and that each such group contains three and only three subgroups of order p^{n+2} with commutator subgroup of order p^2 and that it contains subgroups of orders p^{n+2} and p^{n+4} with commutator subgroups of orders p^3 and p^5 respectively.

5. A generalization

There are two obvious directions in which the results so far obtained may be generalized. The theory of pairs of matrices as expounded by Dickson (cf. the reference above) does not require the matrices to be non-singular, whereas the condition that U contain no operator of type I does require that M and N be non-singular. If U contains an operator of type I we have seen that $M+xN$ contains a linear factor. Obviously, there exists in that case a transformation on x which transforms one of the roots of $f(x)\equiv 0$ to zero, and such a transformation replaces M and N by M' and N' where M' is singular. The new generator s_1' is therefore permutable with one of the operators of U. If $f(x)$ has a linear factor which is repeated, then after the above transformation more than one of the U's will be permutable with s_1'. If $f(x)$ has two distinct linear factors, then a transformation on x will put one of the roots of $f(x)\equiv 0$ into zero and another into infinity, in which case both M' and N' will be singular.* We shall not pursue this question at this time but shall consider another extension.

Let us remove the restriction that the operators of U be of type II, assuming that U contains an operator of type K where the type K is distinguished by the fact that the operator determines the partition

$$n = 2+2+\cdots+2+1+1+\cdots+1$$

in which there are k 2's. The central of G will then be of order at most p^{n-k}. On the other hand if the central of G is of order p^{n-k} and U contains no operator corresponding to a partition of n with a greatest term greater than 2, then U can contain no operator of type J where $j>k$. We shall require further that the commutator subgroup of G and that U be of order p^m. The considerations of the first paragraph of this section indicate that groups satisfying these restrictions are of fundamental importance.

The U's are assumed to be permutable as before. Now generators of H can be selected so that $n-k$ of them are in the central and m of those are in the commutator subgroup. The relations among generators of G are then completely described by k matrices $M_1, M_2, \cdots, M_k$, one corresponding to each of the non-invariant generators $s_1, s_2, \cdots, s_k$, and defined exactly as M and N in §3. The condition that all the operators of U be of type K is obtained by considering the commutator of $s_1^{x_1}s_2^{x_2}\cdots s_k^{x_k}$ and $U_1^{k_1}U_2^{k_2}\cdots\cdot U_m^{k_m}$. This leads to a system of linear homogeneous congruences in $k_1, k_2, \cdots, k_m$, the condition for whose solution is $|x_1M_1+x_2M_2+\cdots$

[*] Compare with the classification of groups for $m=3$, *On metabelian groups*, loc. cit.

$+x_kM_k| \equiv 0$, mod p. There will be no operator of a lower type in U if this polynomial $f(x_1, x_2, \cdots, x_k)$ contains no linear factor.

Exactly as before we may restrict our attention to changes in $f(x_1, \cdots, x_k)$ due to changes in the generators which satisfy the following conditions: the U's are selected from the group U; m of the independent generators of H are in the commutator subgroup; and k of the independent generators of H are in the group $\{s_1, s_2, \cdots, s_k\}$. The first condition makes certain that the U's are permutable and disregards all transformations that leave the M's simultaneously invariant; the second is necessary if the M's are to remain square matrices; and the third is necessary if the number of M's is to remain unchanged. A selection of new sets of generators of U and the commutator subgroup subject to these conditions results in the transformation $M_i' = CM_iD$, where C and D are non-singular. This does not change the polynomial $f(x_1, \cdots, x_k)$, and does not change the invariant factors* of the matrix $x_1M_1 + \cdots + x_kM_k$.

For the effect of changes in the generators of $\{s_1, \cdots, s_k\}$ let us consider the transformation

$$s_i' = s_1^{a_{i1}} s_2^{a_{i2}} \cdots s_k^{a_{ik}} \qquad (i = 1, 2, \cdots, k).$$

The matrix M_i' is obtained by considering the commutators of s_i' with $U_1, \cdots, U_m$ and is obviously $a_{i1}M_1 + a_{i2}M_2 + \cdots + a_{ik}M_k$. The operator $s_1^{x_1}s_2^{x_2} \cdots s_k^{x_k}$ expressed in terms of the s''s is $s_1'^{x_1'}s_2'^{x_2'} \cdots s_k'^{x_k'}$, where the x's are obtained from the x''s by a linear transformation whose matrix is the matrix A of exponents a_{ij} above. After this transformation we have the matrix $x_1'M_1' + x_2'M_2' + \cdots + x_k'M_k'$ in place of $M = x_1M_1 + \cdots + x_kM_k$. If now instead of carrying out the transformation on the generators we subject the x's to the transformation just described, the matrix M becomes, when the terms in x_i' are collected,

$$x_1'(a_{11}M_1 + a_{12}M_2 + \cdots + a_{1k}M_k) + x_2'(a_{21}M_1 + a_{22}M_2 + \cdots + a_{2k}M_k) \\ + \cdots + x_k'(a_{k1}M_1 + a_{k2}M_2 + \cdots + a_{kk}M_k)$$

which is $x_1'M_1' + x_2'M_2' + \cdots + x_k'M_k'$. Therefore,

(11) *Two metabelian groups $G = \{H, U\}$ and $G' = \{H, U'\}$ in which both the U's and the U''s are permutable and of order p, and such that generating relations are defined by sets of matrices $M_1, \cdots, M_k$ and $M_1', \cdots, M_k'$ respec-*

* The term "invariant factor" is used here in a sense which is merely an extension to k matrices of the definition given by Dickson, loc. cit., p. 104, for two matrices M and N. It is clear that the polynomials are homogeneous and are left unchanged when the matrix $M = x_1M_1 + \cdots + x_kM_k$ is replaced by CMD.

tively, are simply isomorphic if and only if the invariant factors of $x_1M_1+x_2M_2+\cdots+x_kM_k$ *and* $x_1'M_1'+x_2'M_2'+\cdots+x_k'M_k'$ *are conjugate under some operator of the linear homogeneous group on the variables* $x_1,\cdots,x_k$.

We return again briefly to the ideas of the first paragraph of this section. In the situation we have been considering we have assumed that all the operators of U were of type K and this implies that each of the M_i's is non-singular and also that $f(x_1,\cdots,x_k)$ contains no linear factor. If $f(x_1,\cdots,x_k)$ contains a linear factor, then U contains an operator of type J where $j<k$. It is obvious that under those circumstances there are several possibilities. If the operator in question is of type I it would be possible to select the generators $s_1',\cdots,s_k'$ and $U_1',\cdots,U_m'$ so that all but one of the matrices M_i' would be singular. If however the operator were of type $(K-1)$, generators of G could not be selected to make more than one of the M_i''s singular. Thus the condition that $f(x_1,\cdots,x_k)$ have a single linear factor in the modular field seems to permit the possibility of many distinct groups. This seems to lead to a large subject in the theory of forms on which not much is to be found in the literature. Dickson has considered* the types of forms that can be written as determinants with linear elements. The classification of these forms involves the theory of modular invariants. The classification of the groups involves considerations beyond the modular invariants since the latter do not take account of the invariant factors of M.

6. Concluding remarks

In conclusion we wish to point out the relation of our investigations to the practically impossible problem of the classification of groups of order p^α. One important sub-class of these groups, which from some points of view may be considered as the most elementary, is made up of those groups whose operators are all of order p, in other words, those groups which are conformal with the abelian group of type $1, 1, \cdots$. It is with groups of this class that we have been concerned. Every such group contains a maximal invariant abelian subgroup of type $1, 1, \cdots$. Of these groups the most elementary are the metabelian groups. Our plan of classification is to determine all of those such that U contains at least one operator of type K and no operator of type greater than K. In the cases where k is 1 or 2 this plan of classification never allows a given group to appear in more than one class, but for $k>2$ it is necessary to look out for repetitions. For example, if $k=3$ and $m=2$, G contains a maximal invariant abelian subgroup $\{U_1, U_2, s_4, s_5, \cdots, s_n\}$ of order p^{n-1} and the operators s_1, s_2, s_3 which now serve as the U's are all of type I or

* These Transactions, vol. 22 (1921), p. 167.

type II. However those repetitions and all others are avoided by insisting that m be at least as great as k.

But we are not yet willing to consider all metabelian groups which are conformal with the abelian group of type 1, 1, $\cdots$, for a restriction which has been important throughout is that the U's be permutable. It is obvious that U's can be chosen, in the groups which we have considered, which are not permutable, for example, $U_1' = s_1U_1$ is not permutable with U_2. Consequently, the removal of that restriction will not only increase our difficulties in managing the groups but will increase greatly the number of repetitions. It appears quite likely that the best method of procedure when the restriction in question is removed is to arrange the groups according to the differences in orders of the commutator subgroup of G and the commutator subgroup arising from transformation of H by U. In all the groups we have considered these orders are equal; the question as to whether or not the converse is true does not seem to have an obvious answer.

University of Illinois,
Urbana, Ill.