GROUPS WHOSE ORDERS ARE POWERS OF A PRIME*

BY

WILLIAM BENJAMIN FITE

In this article two somewhat distinct methods are used to study the properties of groups whose orders are powers of a prime. What may, for the purpose of distinction, be called the usual method is applied in the first part to establish certain properties of the commutators of a group. The commutators are differentiated among themselves by the introduction of the notion of successive commutators. The second part of the article concerns itself with the representation of certain groups as irreducible linear homogeneous groups and then by the use of the theory of group characters as developed by FROBENIUS and BURNSIDE establishes some properties of abstract groups.

PART I.

By a second commutator of a group G, of finite order, we mean a commutator formed by a commutator and any operator of G. Proceeding by successive steps, we define *an ith commutator as a commutator formed by an $(i-1)$th commutator and any operator of the group.* It follows from the definition that any ith commutator is also a jth commutator if $j < i$. In particular, every commutator is a first commutator. All the ith commutators generate a subgroup which we shall call *the ith commutator subgroup.*† We shall represent it by K_i. It is evidently invariant in G.

If G is of class k, identity is the only kth commutator. Conversely, if identity is the only kth commutator of G, then G is of class l, where $l \leqq k$. Now in the quotient group G/K_i identity is the only ith commutator. This quotient group is therefore of class $l_i \leqq i$. Moreover if L is any invariant subgroup of G such that G/L is of class i, then L contains K_i. Hence if $l_i < i$, then K_i coincides with K_{i-1}.

THEOREM I. *A necessary and sufficient condition that a group G have an*

---

* Part I was presented to the Society September 16, 1904; part II, September 7, 1905. Received for publication March 18, 1905.

† This should not be confused with the ith derived group.

$\alpha, 1$ *isomorphism with a group of class* i *is that its* ith *and* $(i-1)$th *commutator subgroups be distinct.**

In order to make the foregoing statements apply to the case $i=1$, we agree that K_0 shall represent G itself.

If G has no invariant ith commutators, except identity, the group† $G^{(i)}$ has no invariant operators, except identity. Hence, if $i<k$, every group of class k contains invariant ith commutators besides identity.‡

THEOREM II. *The operators of* G *that correspond to the invariant operators of* $G^{(i)}$ *are commutative with all the* ith *commutators of* G.

The theorem is true for $i=1$.§ We shall prove it true in general by induction. Let $t_j(j=1, 2, \cdots)$ be any jth commutator and let s be any operator that corresponds to an invariant operator of $G^{(i)}$. We suppose that s' is commutative with t'_{i-1}. Then $s^{-1}t_{i-1}s=t_{i-1}h$, h being an invariant commutator of G. If A is any operator of G, then $A^{-1}t_{i-1}A=t_{i-1}t_i$, and $s^{-1}As=At$, where t is commutative with every $(i-1)$th commutator, since it corresponds to an invariant operator of $G^{(i-1)}$. Hence

$$(st^{-1})^{-1}t_{i-1}t_i(st^{-1})=t_{i-1}h\cdot s^{-1}t_is$$
$$=A^{-1}s^{-1}A\cdot A^{-1}t_{i-1}A\cdot A^{-1}sA=A^{-1}t_{i-1}hA=t_{i-1}t_ih.$$

Therefore s is communtative with t_i.

THEOREM III. *If the* ith *commutator subgroup of a group* G, *of order* p^m (p *a prime*), *is of order* p^α, *the class of* G *is equal to, or less than,* $\alpha+i$.‖

For identity is the only ith commutator of $G^{(\alpha)}$, and therefore $k^{(\alpha)}\leqq i$. Hence $k\leqq\alpha+i$.¶

If $s_j(j=1, 2, \cdots, k_i^{(i+1)})$ be a set of any $k_i^{(i+1)}$ operators (not necessarily distinct) of K_i, and if t_1 is any operator of K_i, we have

$$s_j^{-1}t_js_j=t_jt_{j+1}.$$

Now $t_{k_i^{(i+1)}}^{(i+1)}$ is invariant in $K_i^{(i+1)}$. Therefore $t_{k_i^{(i+1)}+1}$ is invariant in K_i and $k_i\leqq k_i^{(i+1)}+1$.

Suppose now that $k\leqq 2i+1$. Then $k^{(i+1)}\leqq i$, and in $G^{(i)}$ every ith commutator is invariant. Therefore $k_i=1$. Hence:

---

*Cf. MILLER, Bulletin of the American Mathematical Society, vol. 4 (1898), p. 135.

† By $G^{(i)}$ we mean the ith cogredient of G (see DE SÉGUIER, *Éléments de la théorie des groupes abstraits*, p. 87); by $K_j^{(i)}$ we mean the jth commutator subgroup of $G^{(i)}$.

‡ Cf. MILLER, loc. cit., vol. 11 (1905), p. 367.

§ See Transactions of the American Mathematical Society, vol. 3 (1902), p. 351.

‖ See Transactions of the American Mathematical Society, vol. 3 (1902), p. 350.

¶ Throughout this article we shall denote the class of G by k, that of its ith commutator subgroup by k_i, and that of its jth cogredient group, $G^{(j)}$, by $k^{(j)}$.

THEOREM IV. *If a group G is of order p^m (p a prime), then $k_i \leqq k/(i+1)$,* $(i < k)$.*

If L_2 is the second derived group of G, it is a divisor of K_3. This follows from the fact that K_1/K_3, being the commutator subgroup of G/K_3, which is of class 3, is abelian.

Suppose K_i is non-abelian. Then $k \geqq 2(i+1)$; and since the commutators that correspond to the invariant commutators of $G^{(i)}$ are invariant in K_i, the commutator subgroup of $G^{(j)}$ $(j \leqq i+1)$ could not be cyclic.

If K_i is of order p^α, $k \leqq \alpha + i$. Hence $k_i \leqq (\alpha+i)/(i+1)$. But since the operators of G that correspond to operators of $G^{(i)}$ are commutative with all the operators of K_i, it follows that K_i must either be abelian or contain at least p^{i+1} invariant operators, if G is of order p^m. Now if $k_i = (\alpha+i)/(i+1)$ and $\alpha > 1$, then the xth cogredient group of K_i would be of class 2 and order p^{i+2} when $x = (\alpha+i)/(i+1) - 2$. But this is impossible. We have therefore the

THEOREM V. *If the ith commutator subgroup of a group of order p^m (p a prime) is of order p^α, it is of class $k_i < (\alpha+i)/(i+1)$, except when $\alpha = 1$, and then $k_i = (\alpha+i)/(i+1) = 1$.*

Suppose now that G, of order p^m, is non-abelian and contains two abelian subgroups, G_1 and G_2, of order p^{m-1}. Let H denote the greatest common divisor of G_1 and G_2. It is of order p^{m-2}. Every operator of H is invariant in G. Therefore G' is of order p^2 and $k = 2$.

We proceed to show that if G_1 and G_2 are of class k_1, then $k \leqq \frac{1}{2}(k_1^2 + k_1 + 2)$. We have just seen that this relation holds when $k_1 = 1$. We assume that it holds for all values of k_1 that are less than i. If $k_1 = i$ and $k > i+1$, then every operator of G all of whose commutators are invariant is in H. For if such an operator were not in G_1 (or G_2) every invariant operator of G_1 (or G_2) would have all its commutators in G invariant and $k'' \leqq i-1$. Hence $k \leqq i+1$.

We suppose now that $k > i+1$. If every invariant operator of G_1 (or G_2) is in H, its $(i-1)$th commutators in G must be invariant. Hence the subgroup of $G^{(i)}$ that corresponds to G_1 (or G_2) must be of class $l \leqq i-1$. If G_1 (or G_2) has an invariant operator that is not in H, while every invariant operator of G_2 (or G_1) is in H, then the subgroup of G' that corresponds to G_1 (or G_2) is of class $l \leqq i-1$. If both G_1 and G_2 have invariant operators not in H, every invariant operator of H is invariant in G, and every invariant operator of G is in H, since otherwise we should have $k = i$. Hence the subgroups of G' that correspond to G_1 and G_2 are of class $i-1$. In every case therefore $G^{(i)}$ has two subgroups of $1/p$th its order of classes equal to, or less than, $i-1$. By supposition then $k^{(i)} \leqq \frac{1}{2}\{(i-1)^2 + (i-1) + 2\}$. This gives $k \leqq \frac{1}{2}(i^2 + i + 2)$, and the proof by induction is complete.

*See Bulletin of the American Mathematical Society, vol. 9 (1902), p. 139.

If G_2 is of class $k_2 > k_1$, we proceed to show that $k \leqq \frac{1}{2}\{k_1(2k_2 - k_1) + k_1 + 2\}$. As we have just seen, this formula holds when $k_2 = k_1$. We assume that the relation holds for all values of $k_2 (\geqq k_1)$ up to, and including, $i - 1$. Every invariant operator of G_2 is in H, since otherwise G_2' would be simply isomorphic with H' and therefore $k_2 - 1 < k_1$. Hence every invariant operator of G_2 has all its $(k_1 - 1)$th commutators in G invariant. The subgroups of $G^{(k_1)}$ that correspond to G_1 and G_2 are therefore of classes $l_1 \leqq k_1$ and $l_2 \leqq i - 1$ respectively. Hence, by our supposition,

$$k^{(k_1)} \leqq \frac{k_1[2(i-1) - k_1] + k_1 + 2}{2}, \qquad k \leqq \frac{k_1(2i - k_1) + k_1 + 2}{2}.$$

That is, if the formula holds for $k_2 = i - 1$, it holds for the next greater value of k_2. This result can be formulated into

THEOREM VI. *If a group G, of order p^m (p a prime), contains two subgroups of order p^{m-1} and classes k_1 and $k_2 (\geqq k_1)$ respectively, then* $k \leqq \frac{1}{2}\{k_1(2k_2 - 1) + k_1 + 2\}$.

Let G be of order p^m and let D be the greatest common divisor of all its invariant subgroups of index p^2. Then D contains K_1 and P_2, the subgroup generated by the p^2th powers of the operators of G. If D is identity, then G is abelian and has no operator of order greater than p^2. Conversely, if G is abelian and has no operator of order greater than p^2, then D is identity. Moreover,* $D \equiv \{K_1, P_2\}$.

If D is the greatest common divisor of all the invariant subgroups of index $p^\alpha (\alpha > 1)$ and is of order p^γ, then $k \leqq \alpha + \gamma - 1$; for any such invariant subgroup gives a quotient group of class $l \leqq \alpha - 1$, and hence D contains the $(\alpha - 1)$th commutator subgroup.

PART II.

It is well known that the only substitutions of finite order permutable with every substitution of an irreducible linear homogeneous group of finite order are those which multiply each variable by the same number. Obviously then a necessary condition that a group be simply isomorphic with an irreducible group is that its central be cyclic.† This condition is also sufficient if the group is the direct product of groups of orders $p_1^{m_1}, p_2^{m_2}, \cdots, p_n^{m_n}$ respectively ($p_1, p_2, \cdots, p_n$ being distinct primes). In proving this statement we shall use the following notation:

* The proofs of these statements are similar to those given by DE SÉGUIER, loc. cit., p. 115, for the subgroups of index p. Cf. BAGNERA, Reale Accademia dei Lincei-Atti, Rendiconti, series 5, 1898, p. 63; Annali de Matematica, series 3, vol. 2 (1899), p. 264.

† The subgroup formed by the invariant operators of a group is called the *central* of the group. This term seems to have been used for the first time by DE SÉGUIER, loc. cit., but he gives no explicit definition of it.

H is the cyclic central of G of order $p_1^{a_1}p_2^{a_2}\cdots p_n^{a_n}$; $H^{(i)}$ $(i=1, 2, \cdots, n)$ is the subgroup of H of order p_i; G_i is the subgroup of G of order $p_i^{m_i}$. The number of systems of conjugate operations of G is r; the number of systems of conjugate operations of $G/H^{(i)}H^{(j)}H^{(k)}\cdots$ is $r_{ijk\ldots}$; the number of systems of conjugate operations of G_i is s_i; the number of systems of conjugate operations of $G_i/H^{(i)}$ is s_i'; the number of systems of conjugate operations of $G_i/H^{(i)}$ that (in $G/H^{(i)}$) correspond to operations of G that give no invariant commutators besides identity is t_i.

If now G were not simply isomorphic with an irreducible group, every irreducible representation of G would also be a representation of at least one of the quotient groups $G/H^{(i)}$. The number of distinct irreducible representations of any group (of finite order) is equal to the number of its systems of conjugate operations.* If, therefore, we show that

$$r > \sum_{k=1}^{n}(-1)^{k+1}r_{kS_n},$$

where r_{kS_n} denotes the sum of the ${}_kC_n$ r's with k subscripts, it follows that the group under consideration is simply isomorphic with an irreducible group.

Now

$$\text{(I)} \qquad r - r_1 = \prod_{i=2}^{n} s_i t_1 (p_1 - 1),$$

$$\text{(II)} \qquad r_{kC_{n-1}} - r_{k+1C_n'} = \prod_{i=2}^{n}{}' s_i t_1 (p_1 - 1).$$

The first subscript in the left member denotes a particular combination of the subscripts $2, 3, \cdots, n$, while the second subscript is the same with the addition of 1; in the right member Π' indicates that in the product s_i' is to be placed for s_i whenever i occurs in both subscrips in the left member. If in equation (II) we take all possible subscripts for a given k, and add, we get

$$\text{(III)} \qquad r_{kS_{n-1}} - r_{k+1S_n'} = \sum \prod_{i=2}^{n'}{}' s_i t_1 (p_1 - 1).$$

From (I) and (III) we get

$$\text{(IV)} \qquad r - \sum_{k=1}^{n}(-1)^{k+1}r_{kS_n} = \prod_{i=2}^{n}(s_i - s_i')t_1(p_1 - 1) = \prod_{i=1}^{n} t_i(p_i - 1).$$

The right member of this equation is positive. Hence:

THEOREM I. *A necessary and sufficient condition that a group whose order is a power of a prime or a group which is the direct product of such*

* The most direct proof of this is that given by BURNSIDE, Acta Mathematica, vol. 28 (1904), p. 36. FROBENIUS and BURNSIDE had given indirect proofs before this.

groups be simply isomorphic with an irreducible linear homogeneous group is that its central be a cyclic group.

An irreducible abelian group operates upon only one variable. We consider now the number of variables operated upon by an irreducible non-abelian group. Let

$$S: \qquad x_i' = \omega_i x_i \qquad (i=1, 2, \cdots, n),$$

be the normal form of a non-invariant operation of an irreducible group G that gives at least one invariant commutator besides identity, and suppose that

$$\omega_1 = \omega_2 = \cdots = \omega_{\lambda_1} \neq \omega_{\lambda_1+1} = \omega_{\lambda_1+2} = \cdots = \omega_{\lambda_2} \neq \omega_{\lambda_2+1} = \cdots.$$

We select R so that $S^{-1}RS = RT$, where T is the invariant commutator of highest order given by S. Now T is of the form

$$x_i' = \omega x_i \qquad (i=1, 2, \cdots, n),$$

and therefore

$$\omega_i^{-1} \sum_{t=1}^{n} b_{it}\omega_t x_t = \sum_{s=1}^{n} b_{is}\omega x_s,$$

if

$$R: \qquad x_i' = \sum_{s=1}^{n} b_{is}x_s \qquad (i=1, 2, \cdots, n).$$

If $\omega_i^{-1}\omega_j \neq \omega$, then $b_{il} = 0$ when j and l are both between λ_{r-1} and $\lambda_r + 1$. But if $\omega_i^{-1}\omega_j = \omega$, b_{il} is not necessarily zero. Now $\omega_i^{-1}\omega_j$ will still equal ω if j takes any one of $\lambda_r - \lambda_{r-1}$ values, and i takes any one of, say, $\lambda_s - \lambda_{s-1}$, values. Since the determinant of R does not vanish, we must have $\lambda_r - \lambda_{r-1} = \lambda_s - \lambda_{s-1}$. If $\omega_j^{-1}\omega_k = \omega$, then $\lambda_s - \lambda_{s-1} = \lambda_t - \lambda_{t-1}$, and so on in a cycle until we get back to ω_i. The number of elements in this cycle equals the order of T, and the sum of the ω_i's composing the cycle is zero. Therefore

$$\sum_{i=1}^{n} \omega_i = 0.$$

If S corresponds to an invariant operator of G', then $\lambda_1 t = n$, where t is the order of* T.

---

*Since $R^{-1}SR = ST^{-1}$ and the characters of any two conjugate operations are the same, we have

$$\sum_{i=1}^{n} \omega_i = \omega^{-1} \sum_{i=1}^{n} \omega_i.$$

Therefore

$$\sum_{i=1}^{n} \omega_i = 0.$$

This is a much shorter proof than the one given above. The latter however has the advantage of showing also that the number of variables cannot be less than the number of invariant commutators.

Let N be the order of G and r the number of its systems of conjugate operations. If $\chi_k^i (k = 1, 2, \cdots, r)$ is the set of characters of G corresponding to the irreducible representation g_i, and if h_k is the number of operations in the kth conjugate set, then *

$$\sum_{k=1}^{r} h_k \chi_k^i \chi_k^{i'} = N.$$

If we take g_i as G itself, this can be put into the form

$$hn^2 + \sum' h_k \chi_k^i \chi_k^{i'} = N,$$

where the summation extends over all the conjugate sets that are composed of more than one operation. But χ_k^i and $\chi_k^{i'}$ are conjugate imaginaries and therefore $\chi_k^i \chi_k^{i'}$ is real and positive. If every non-invariant operation of G gives an invariant commutator besides identity, every term in this summation is zero. Hence:

THEOREM II. *The number of variables in an irreducible linear homogeneous group G is equal to the square root of the order of G', if every non-invariant operation of G gives an invariant commutator besides identity. The number of variables is less than this, but not less than the number of invariant commutators if G contains an operation the sum of whose multipliers is not zero.*

In particular, if G is an irreducible metabelian group of order N in n variables, then $n = \sqrt{N/h}$, where h is the order of the central of G.

Since the number of variables in an irreducible group of order p^m is greater than, or equal to, the order of its $(k-1)$th commutator subgroup, it follows that, if the central of G is cyclic, the order of G' must be greater than, or equal to, $p^{2\beta}$, where p^β is the order of the $(k-1)$th commutator subgroup. If G' is of order $p^{2\beta}$, every non-invariant operation of the irreducible group that is simply isomorphic with G must have the sum of its multipliers equal to zero.

THEOREM III. *If the central, H, of a group G, of order p^m (p an odd prime), is cyclic and of order p^h, then $m - h$ must be even when K is cyclic.*†

For if $m - h$ is odd, G must contain a non-invariant operation R that gives no invariant commutator besides identity. Now R must give some commutators besides identity. Suppose that it gives a commutator S in the $(k-i)$th commutator subgroup, but none in any higher commutator group; say $R^{-1}AR = AS$. If S^{p^γ} is the first power of S that is contained in the $(k-i+1)$th commutator subgroup, then, provided K is cyclic, $R^{-1}A^{p^\gamma}R = A^{p^\gamma}S_1$, where S_1 is contained

* FROBENIUS, Berliner Sitzungsberichte, 1896, II, p. 1359; BURNSIDE, Proceedings of the London Mathematical Society, vol. 33 (1900), p. 154; series 2, vol. 1 (1903), p. 123.

† For a special case, see Transactions of the American Mathematical Society, vol. 3 (1902), p. 342.

in the $(k-i+1)$th commutator subgroup and is distinct from identity.* But this contradicts the hypothesis. The theorem is therefore proved.

Let H_i be the ith central† of G. We shall denote its order by p^{h_i}. If K is cyclic, the subgroup of G that corresponds to the invariant operations of $G^{(j)}$ of order $p^{2\alpha+1}$, or less (α an integer), cannot be cyclic. If it were cyclic, we could denote by $\bar{H}_j$ the subgroup of H_j of order‡ $p^{h_{j-1}+2\alpha+1}$. This would be invariant in G and the commutator subgroup of $G/\bar{H}_j$ would be cyclic, as would also its central. But the order of its first cogredient would be $p^{m-h_j-2\alpha-1}$, which would be an odd power of p, since p^{m-h_j}, being the order of the first cogredient of G/H_{j-1}, would be an even power of p.

If the subgroup of G that corresponds to the invariant operations of $G^{(j)}$ of order $p^{2\alpha}$, or less, were cyclic, then the subgroup corresponding to the invariant operations of $G^{(j)}$ of order $p^{2\alpha-1}$, or less, would be cyclic, and this has just been seen to be impossible. Hence *if K is cyclic, no central except the first can be cyclic.*

Professor BURNSIDE has discussed irreducible groups in a prime number of variables with reference to their solubility.§ We shall here consider such groups, of order p^m, with reference to their classes.

Let G be such a group. It is non-abelian and K_{k-1} is of order p. If $k=2$, G' is of order p^2. If $k>2$, G contains a commutator, S, that corresponds to an invariant commutator of G' of order p. Therefore S has just p conjugates and is invariant in a subgroup, G_1, of G of order p^{m-1}. This subgroup is reducible and therefore abelian, and it contains K. Suppose that A is so chosen that $G \equiv \{G_1, A\}$. Then A^p is invariant in G and A has $p^{m-\alpha-1}$ conjugates. The order of K is therefore at least $p^{m-\alpha-1}$. If the order of K were greater than this the commutator subgroup of G' would be of order greater than $p^{m-\alpha-2}$. But this is impossible. Therefore the order of K is $p^{m-\alpha-1}$. The order of K_2 is $p^{m-\alpha-2}$ and, in general, the order of $K_i (i=1, 2, \cdots, k)$ is $p^{m-\alpha-i}$. Hence $k=m-\alpha$, and the p^rth power of every operator of G is invariant if‖ $r(p-1) \geqq m-\alpha-1$.

CORNELL UNIVERSITY,
March, 1905.

---

*If $p=2$, S_1 may be identity. This is the case in the groups of order 2^4 and class 3. The theorem is not true in the case of these groups.

†See DE SÉGUIER, loc. cit., p. 87.

‡In order that this may be applicable when $j=1$, we agree that h_0 shall be zero.

§Acta Mathematica, vol. 27 (1903), p. 217.

‖Bulletin of the American Mathematical Society, vol. 10 (1904) p. 347.