ON GROUPS OF ORDER $p^\alpha q^\beta$

By W. BURNSIDE.

[Received and Read January 14th, 1904.]

IT may be convenient to the reader to summarize the results hitherto obtained with regard to groups of order $p^\alpha q^\beta$ other than those relating to particular values of p, q, α, and β. If m is the index to which p belongs, mod. q, the first result arrived at was that, if $\alpha \leqslant m$, the group is soluble.*

In my book on the *Theory of Groups* (1897) I extended this result, showing that, if $\alpha < 2m$, the group is soluble. In the same place I proved that, if the sub-groups of orders p^α and q^β are both Abelian, the group is soluble; and that all groups of order $p^\alpha q^2$ are soluble.

Of the last result another proof was given by Jordan (*Liouville's Journal*, Ser. 5, Vol. IV., 1898). Finally, in a memoir "Uber Gruppen der Ordnung $p^\alpha q^\beta$" (*Acta Mathematica*, Vol. XXVI., p. 189, 1902), Herr Frobenius has shown that when $\alpha \leqslant 2m$ the group is soluble, and also that when the group contains only p^m sub-groups of order q^β it is soluble.

In the present paper I have attacked the question of the solubility of a group of order $p^\alpha q^\beta$ by a consideration of certain properties of the group-characteristics of such a group; and I have succeeded in showing that all groups of order $p^\alpha q^\beta$ are soluble.

The first section of the paper is concerned with a property of the characteristics of certain operations in an irreducible group of linear substitutions in p^m variables, where p is prime; and it has bearings on other questions beside those with which the remainder of the paper is concerned.

My paper "On Group-Characteristics" (*Proc. London Math. Soc.*, Vol. XXXIII., p. 146) is referred to by the initials G.-C.

1. From the relations (G.-C., p. 151),

$$h_i h_j \chi_i \chi_j = \chi_1 \sum_k c_{ijk} h_k \chi_k,$$

---

* Frobenius, *Berliner Sitzungsberichte* (1895), p. 190; and Burnside, *Proc. London Math. Soc.*, Vol. XXVI. (1895), p. 209.

for a given suffix i and each suffix j in turn, by eliminating the ratios of the quantities $h_j\chi_j$, there results

$$\begin{vmatrix} c_{i11}-\dfrac{h_i\chi_i}{\chi_1}, & c_{i12}, & \dots, & c_{i1r} \\ c_{i21}, & c_{i22}-\dfrac{h_i\chi_i}{\chi_1}, & \dots, & c_{i2r} \\ \dots & \dots & \dots & \dots \\ c_{ir1}, & c_{ir2}, & \dots, & c_{irr}-\dfrac{h_i\chi_i}{\chi_1} \end{vmatrix} = 0.$$

Hence, since the c's are positive integers or zeros, $h_i\chi_i/\chi_1$ is an algebraic integer.*

Suppose that χ_1 is the power of a prime, p^m, so that the order of the group is divisible by p^m. Let p^a be the highest power of p which divides the order of the group, and let P be a self-conjugate operation of a sub-group of order p^a. Then h_P is relatively prime to p, and χ_P is the sum of p^m powers of ω, if ω is a primitive p^a-th root of unity, p^a being the order of P.

From $h_P\chi_P/\chi_1$ form the $p^{a-1}(p-1)$ conjugate expressions obtained on replacing ω by each primitive p^a-th root of unity. The elementary symmetric functions of these expressions will be algebraic integers, and, since they are rational, they must be rational integers. Now h_P and p^m (or χ_1) are relatively prime. Hence the elementary symmetric functions of χ_P/χ_1 and its conjugates are rational integers; and therefore χ_P/χ_1 is an algebraic integer. From this it follows at once that either (i) χ_P must be zero, or (ii) the p^m powers of ω, whose sum make up χ_P, must all be the same. In fact, if χ_P is not zero, (mod. χ_P)/χ_1 is (from its graphical representation) a proper fraction, except when $\chi_P = p^m\omega^x$, where x is some integer. But, if (mod. χ_P)/χ_1 is a proper fraction, so also is the product Π (mod. χ_P)/χ_1 formed from all the conjugates, and this is the same as $\Pi\,\chi_P/\chi_1$, which has been proved to be an integer. The result thus proved may be stated as the following:—

Theorem I.—If a group G of order $p^a s$ (s relatively prime to p) can be represented as an irreducible group of linear substitutions in p^m variables, then a self-conjugate operation P of a sub-group of order p^a of G has for its characteristic in this representation either zero or $p^m\omega$, where ω is a root of unity. In the latter case the substitution corresponding to P in the irreducible group is a self-conjugate substitution, and G has a self-conjugate sub-group containing P.

* This result is given by Herr Frobenius.

If P, of order p^a, is a self-conjugate operation of a sub-group of order p^a of G, so also are $P^p, P^{p^2}, \ldots, P^{p^{a-1}}$. The characteristic of each of these operations is therefore either zero or p^m times a root of unity. If each of them is zero, so that no one of them is a self-conjugate operation of the irreducible group in p^m variables, the p^m roots of unity which make up χ_P must clearly be the different p^a-th roots of unity, each repeated p^{m-a} times. This is only possible when $a \leqslant m$; and, if $a > m$, the p^{a-m}-th power of P must be a self-conjugate operation of the irreducible group.

Consider in particular an irreducible group g of linear substitutions in p variables, and let p^a be the highest power of p which divides the order of g. If a sub-group of g of order p^a is not Abelian, it must be irreducible and will necessarily contain self-conjugate operations which are self-conjugate operations of g. If the sub-group of order p^a is Abelian, and if $a > 1$, the characteristics of all of its operations cannot be zero,* and therefore some must be self-conjugate operations of g. Hence:

Theorem II.—An irreducible group of linear substitutions in a prime number of variables p must either (i) contain self-conjugate operations whose orders are powers of p, or (ii) have no sub-group of order p^2.

2. Consider a group G of order $p^a q^\beta$. Let H and K be sub-groups of G of orders p^a and q^β respectively, and let P be a self-conjugate operation of H, and Q a self-conjugate operation of K, other than identity.

All the operations conjugate to P are obtained on transforming P by all the operations of K, or of any sub-group conjugate to K; and all those conjugate to Q on transforming Q by the operations of H. Hence, if PQ be transformed by any operation of H, it becomes PQ_j, where Q_j may be any one of the operations conjugate to Q; and, if PQ_j be transformed by any operation of the sub-group conjugate to K which contains Q_j self-conjugately, it becomes P_iQ_j, where P_i may be any one of the operations conjugate to P.

Hence the set of operations formed by multiplying any one of the operations of the conjugate set to which P belongs (say the i-th set) by any one of the operations of the conjugate set to which Q belongs (say the j-th set) all belong to one and the same conjugate set (say the k-th).

---

* Thus, if $x_1' = x_1, \quad x_2' = \omega x_2, \quad \ldots, \quad x_p' = \omega^{p-1} x_p$

and $x_1' = \omega_1 x_1, \quad x_2' = \omega_2 x_2, \quad \ldots, \quad x_p' = \omega_p x_p$

be two of its operations, say P and P', of order p, P' not being a power of P, then at least one of the operations $P^x P'$ $(x = 0, 1, 2, \ldots, p-1)$ has a characteristic different from zero. The case in which the group contains operations of order p^2 comes under the head considered immediately above.

This is represented by the equation (G.-C., p. 148)

$$C_i C_j = c_{ijk} C_k,$$

involving the relations

$$h_i h_j = c_{ijk} h_k, \qquad c_{ijl} = 0 \quad (l \neq k).$$

If χ_i, χ_j, χ_k are the characteristics of the three sets in any irreducible representation of G, the relation (G.-C., p. 151)

$$h_i h_j' \chi_i \chi_j = \chi_1 \sum_s c_{ijs} h_s \chi_s\,.$$

reduces to

$$h_i h\, \chi_i \chi_j = c_{ijk} h_k \chi_1 \chi_k,$$

i.e.,

$$\chi_i \chi_j = \chi_1 \chi_k.$$

3. In every irreducible representation of G, χ_1 is a factor of the order of G (G.-C., p. 156), and must therefore be either unity, a power of p, a power of q, or a product of powers of p and q. For the identical representation χ_1 is unity, and (G.-C., p. 153)

$$\sum_t (\chi_1^t)^2 = p^\alpha q^\beta,$$

where the sum is extended to the r distinct irreducible representations of G. Hence every χ_1, except the first, cannot be divisible by p, nor can every one be divisible by q. It follows that either (i) other χ_1's besides the first must be unity, in which case the group can be represented as a cyclical group, and is therefore composite, or (ii) some χ_1's must be powers of p and others powers of q.

Consider an irreducible representation of G in which χ_1 is a power of p, say p^m. In this representation χ_i, the characteristic of the operation P considered in § 2 is either zero or $p^m\omega$, where ω is a p^c-th root of unity. In the former case χ_k, the characteristic of PQ, is, by the final equation of § 2, zero. In the latter case the substitution corresponding to P is a self-conjugate substitution of the irreducible representation of G in p^m variables, and G itself is composite. Similarly, in any irreducible representation of G in q^n variables, either χ_k is zero or G is composite.

Suppose now, if possible, that G has no representation, except the identical one, for which χ_1 is unity, and that χ_k is zero for every irreducible representation of G in which χ_1 is either a power of p or a power of q. Then the relation (G.-C., p. 153)

$$\sum_i \chi_1^i \chi_k^i = 0$$

becomes

$$1 + \sum_i{}' \chi_1^i \chi_k^i = 0,$$

where Σ' is limited to those representations for which χ_1 is divisible by pq. Since each χ_k is an algebraic integer, this equation may be written in the form $1/pq+a=0$, a being an algebraic integer; and no such equation is true.

Hence either χ_1 must be unity for some representation other than the identical one, or χ_k must be different from zero in some representations in which χ_1 is a power of p or a power of q. In either case G must be composite; and, since the same reasoning applies to the factor groups and the sub-groups of G, G must be soluble. Hence:—

Theorem III.—Every group whose order is of the form $p^\alpha q^\beta$ is soluble.

ADDITION TO THE PRECEDING PAPER. *February 9th*, 1904.

Since the above was communicated to the Society I have arrived at a materially simpler manner of establishing a rather more general result.

Suppose that in a group G of finite order the number of operations which constitute one conjugate set (say the i-th) is the power of a prime, so that $h_i = p^a$. If χ_i is the corresponding characteristic in an irreducible representation of G, then $h_i\chi_i/\chi_1$ is an algebraic integer; and therefore, if h_i and χ_1 are relatively prime, *i.e.*, if χ_1 is not divisible by p, χ_i/χ_1 is an algebraic integer. Hence, as above, either χ_i is zero or $\chi_i = \chi_1\omega$, where ω is a root of unity. In the latter case every operation of the i-th conjugate set is a self-conjugate substitution in the irreducible representation under consideration and G is therefore composite.

Now consider the relation $\sum\limits_s \chi_1^s\chi_i^s = 0,$

where the summation extends to the r distinct irreducible representations of G. If no χ_1, except the first, is unity, and if χ_i is zero whenever χ_1 is not divisible by p, this equation is of the form $1+pa=0$, where a is an algebraic integer, which is impossible. Hence either (i) some χ_1, other than the first, is unity, in which case G is isomorphic with a cyclical group, or (ii) some χ_i is equal to $\chi_1\omega$, in which case G has a self-conjugate sub-group containing the i-th set. In either case G is composite. Hence:—

Theorem.—If in a group of finite order the number of operations in any one conjugate set is the power of a prime, the group is composite.

From this the previous result follows immediately. For in a group of order $p^\alpha q^\beta$ there are necessarily conjugate sets, the numbers of operations in which are powers of primes. In fact the self-conjugate operations of a sub-group of order p^α (or q^β) belong to such sets.