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

(SECOND PAPER)

By W. BURNSIDE.

[Received November 17th, 1904—Read December 8th, 1904.]

HAVING shown that all groups of order $p^\alpha q^\beta$ are soluble, the enquiry naturally suggests itself as to whether any general law can be laid down with respect to the orders of the self-conjugate sub-groups of such groups. I have here shown that, subject to certain specified exceptions when the order is even, a group of order $p^\alpha q^\beta$ $(p^\alpha > q^\beta)$ must have a characteristic sub-group of order p^a, where a satisfies the inequality $p^a > p^\alpha q^{-\beta}$. The exceptions are interesting, as emphasizing the marked distinction that may exist between groups of even and groups of odd order.

LEMMA.—If p, q are primes, and α, β positive integers, such that $p^\alpha > q^\beta$, then p^α cannot be a factor of

$$(q-1)(q^2-1)\dots(q^\beta-1)$$

unless (i.) p is 2 and q is of the form $1+2^{2^m}$, or (ii.) q is 2 and p is of the form 2^n-1.

Let m be the index to which q belongs (mod p), and let

$$q^m = 1+yp^x \quad (y \not\equiv 0, \text{ mod } p).$$

Then p will divide q^t-1 only when t is a multiple of m; and, if

$$t = kmp^s \quad (k \not\equiv 0, \text{ mod } p),$$

p^{x+s} is the highest power of p which divides q^t-1.

Let $$\gamma m \leqslant \beta < (\gamma+1)m,$$

so that the only terms in the product $\prod_1^\beta (q^t-1)$ which p divides are

$$(q^m-1),\ (q^{2m}-1),\ \dots,\ (q^{\gamma m}-1).$$

Further, let $$\gamma = a_0+a_1p+a_2p^2+\dots+a_rp^r,$$

where the a's are zeroes or positive integers less than p. Then, in the product $\prod_{t=1}^{t=\gamma}(q^{tm}-1)$ there are just

$$a_s+pa_{s+1}+\ldots+p^{r-s}a_r-(a_{s+1}+pa_{s+2}+\ldots+p^{r-s-1}a_r)$$

terms which are divisible by p^{x+s} and not by p^{x+s+1}. Hence, if p^d is the highest power of p which divides the product, then

$$d=\sum_{s=0}^{s=r}[a_s+pa_{s+1}+\ldots+p^{r-s}a_r-(a_{s+1}+pa_{s+2}+\ldots+p^{r-s-1}a_r)](x+s)$$

$$=\gamma x+\frac{\gamma-a_0-a_1-\ldots-a_r}{p-1}.$$

Now $$p^d<q^\beta$$

if $$p^{md/\beta}<1+yp^x$$

or $$p^{[1/(p-1)](m\gamma/\beta)}<(yp^{x[(\beta-m\gamma)/\beta]}+p^{-m\gamma x/\beta})\,p^{m\Sigma a_i/[\beta(p-1)]}.$$

Since $\beta\geqslant m\gamma$, the right-hand side is greater than y, and the left-hand side is not greater than $p^{1/(p-1)}$. But, if p and q are both odd primes, y cannot be less than 2, and $p^{1/(p-1)}<2$. Hence, when p and q are both odd, the highest power of p which divides $\prod_{i}^{\beta}(q^i-1)$ is less than q^β, and the same holds if either p or q is 2, and y is greater than unity.

It remains to consider the two cases in which either p or q is 2, and at the same time y is 1.

If p is 2, m is unity, and therefore, when y is unity, q is a prime of the form $1+2^{2^m}$. That this gives an exception to the lemma may be verified at once by considering a particular case. Thus

$$p=2,\quad q=5,\quad x=2,\quad y=1,\quad \beta=3$$

give $$d=7,$$

and, in fact, $2^7>5^3$.

If q is 2, and y is unity, then x must be unity,* and p is a prime

---

* That 2^n-1 cannot be a power, higher than the first, of an integer may be proved as follows:—

If $$2^n-1=p^x,$$

then $$2(2^{n-1}-1)=p^x-1=(p-1)(p^{x-1}+p^{x-2}+\ldots+1).$$

Hence x must be odd, since the second factor on the right is not divisible by 2. But, if x is odd,

$$2^n=p^x+1=(p+1)(p^{x-1}-p^{x-2}+\ldots+1).$$

Hence $p+1=2^\nu$ $(\nu\leqslant n)$, and $2^n-1=(2^\nu-1)^x$.

If x is greater than unity, this gives

$$2^n=2^{\nu x}-x.2^{\nu(x-1)}+\ldots+x.2^\nu,$$

and therefore $x\equiv 0 \pmod 2$, in contradiction to the fact that x is odd.

of the form 2^m-1. In this case, if β be taken equal to $m\gamma+1$,

$$d = \gamma\frac{p}{p-1} - \frac{\Sigma a}{p-1},$$

and $$p^d > 2^\beta$$

if $$p^{\gamma[p(p-1)]} > 2^{1+m\gamma}p^{\Sigma a_i(p-1)},$$

or if $$p^{p(p-1)} > (1+p)\,2^{1/\gamma}p^{\Sigma a'[\gamma(p-1)]}.$$

Now $$p^{p(p-1)} > 1+p,$$

and therefore in this case, by taking γ (and therefore β) large enough, it can always be insured that $$p^d > 2^\beta.$$

This case, again, then gives an exception in which the lemma is not necessarily true.

COROLLARY.—If p and q are primes, the highest power of p which divides

$$\prod_{i=1}^{i=t}(q-1)(q^2-1)\ldots(q^{\gamma_i}-1)$$

is less than $q^{\sum_1^t \gamma_i}$, with the same exceptions.

Let G be a group of order $p^\alpha q^\beta$, where p and q are primes and $p^\alpha > q^\beta$, while p and q do not come under either of the above two exceptional cases. Since G is soluble, it must have a self-conjugate sub-group whose order is a power of either p or q. Suppose that H, of order p^α, is a self-conjugate sub-group of G, and that G contains no self-conjugate sub-group whose order is a greater power of p than p^α. Then either $p^\alpha > p^\alpha/q^\beta$ or the factor group G/H, of order $p^{\alpha-\alpha}q^\beta$, where $p^{\alpha-\alpha} > q^\beta$, has no self-conjugate sub-group whose order is a power of p.

We are led therefore to consider the case in which a group G of order $p^\alpha q^\beta$, where $p^\alpha > q^\beta$, has a self-conjugate sub-group whose order is a power of q. If this is the case, let K, of order q^b, be the greatest self-conjugate sub-group of G whose order does not contain p as a factor. Then G has a sub-group G' of order $p^\alpha q^b$, containing K self-conjugately; and every operation of a sub-group of order p^α in G' gives an isomorphism of K. Let $K, K_1, \ldots, K_n, 1$, of orders $q^b, q^{b_1}, \ldots, q^{b_n}, 1$, be a characteristic series of K. Every isomorphism of K, whose order is relatively prime to q, which transforms every operation of each of the factor-groups

$$K/K_1,\ K_1/K_2,\ \ldots,\ K_n,$$

into itself, is the identical isomorphism.*

* *Theory of Groups*, p. 249.

Now the order of the group of isomorphisms of K_i/K_{i+1} is

$$(q^{b_i-b_{i+1}}-1)(q^{b_i-b_{i+1}}-q)\dots(q^{b_i-b_{i+1}}-q^{b_i-b_{i+1}-1}).$$

Hence, the greatest power of p which can be the order of a group of isomorphisms of K cannot exceed the greatest power of p which divides

$$\prod_{i=0}^{i=n}(q-1)(q^2-1)\dots(q^{b_i-b_{i+1}}-1);$$

and, by the corollary to the lemma, the greatest power of p, say p^d, which divides this product is less than q^b. Hence, the isomorphisms of K, given by the operations of a sub-group of G' of order p^α, must be alike in sets of $p^{\alpha-d'}$, where $d' \leqslant d$; and every operation of some sub-group of order $p^{\alpha-d'}$ must give the identical isomorphism of K, *i.e.*, must be permutable with every operation of K. Now

$$p^{d'} \leqslant p^d < q^b < q^\beta,$$

and therefore there must be a sub-group of G, of order p^α, where $p^\alpha > p^\alpha/q^\beta$, every one of whose operations is permutable with every operation of K. Let a represent the greatest number for which this is true. The totality of the operations of G which are permutable with every operation of K constitute a self-conjugate sub-group I of G. The order of this sub-group is $p^a q^{b'+c}$, where $q^{b'}$ is the order of the sub-group L of K formed of its self-conjugate operations and $c \geqslant 0$. The greatest sub-group common to I and K is L. If I has a self-conjugate sub-group whose order is a power of q greater than $q^{b'}$, let it be L' of order $q^{b'+c_1}$, where c_1 is as great as possible. Then L' is a self-conjugate sub-group of G, and $\{K, L'\}$ is a self-conjugate sub-group of G whose order is a higher power of q than q^b. No such sub-group exists, since it was supposed above that q^b is the highest power of q which is the order of a self-conjugate sub-group. Hence I/L has no self-conjugate sub-group whose order is a power of q. It must therefore have a self-conjugate sub-group of maximum order p^{a_1}. This is necessarily a characteristic sub-group, and I therefore contains a characteristic sub-group of order $p^{a_1}q^{b'}$. This is the direct product of L and a group of order p^{a_1}; and the latter therefore is a self-conjugate sub-group of G.

Finally, then, G must in any case have a self-conjugate sub-group whose order is a power of p; and, since, when $p^{a_1} < p^\alpha/q^\beta$, the same reasoning may be applied to the factor group of order $p^{\alpha-a_1}q^\beta$, G must have a self-conjugate sub-group of order p^a, where $p^a > p^\alpha/q^\beta$.

If p^{a_1} is the greatest power of p that is the order of a self-conjugate sub-group of G, then G has a characteristic sub-group G_1 of

order p^{α_1}. Similarly, G/G_1, of order $p^{\alpha-\alpha_1}q^{\beta}$ has a characteristic sub-group of order q^{β_1}, where q^{β_1} is the greatest power of q which is the order of a self-conjugate sub-group of G/G_1. Thus G has a characteristic sub-group H_1, of order $p^{\alpha_1}q^{\beta_1}$. The system of characteristic sub-groups of orders p^{α_1}, $p^{\alpha_1}q^{\beta_1}$, $p^{\alpha_1+\alpha_2}q^{\beta_1}$, $p^{\alpha_1+\alpha_2}q^{\beta_1+\beta_2}$, ... and the indices $\alpha_1, \beta_1, \alpha_2, \beta_2, \ldots$ corresponding to them may be extended till G itself is arrived at.

When p and q are odd, or when, one of them being 2, the other is not of the form 2^n-1 or $2^{2^m}+1$, these indices are subject to a system of inequalities, materially limiting the extent of the system of characteristic sub-groups. It has already been proved that

$$p^{\alpha_1} > \frac{p^{\alpha}}{q^{\beta}} \qquad \text{and} \qquad q^{\beta_1} > \frac{q^{\beta}}{p^{\alpha-\alpha_1}}.$$

Now in G/G_1 there is a characteristic sub-group of order q^{β_1}, and no self-conjugate sub-group whose order is a power of p. Every operation of G/G_1 gives an isomorphism of the characteristic sub-group of order q^{β_1}, and, unless $p^{\alpha-\alpha_1} < q^{\beta_1}$, there will be a sub-group, whose order is a power of p, every one of whose operations is permutable with every operation of the characteristic sub-group. But this, as shown in the preceding paragraph, would involve that G/G_1 had a self-conjugate sub-group whose order was a power of p, which is not the case. Hence

$$q^{\beta_1} > p^{\alpha-\alpha_1},$$

and, taking this with $$q^{\beta_1} > \frac{q^{\beta}}{p^{\alpha-\alpha_1}},$$

it follows that $$\beta_1 > \tfrac{1}{2}\beta.$$

Similarly it may be shown that

$$\alpha_2 > \tfrac{1}{2}(\alpha-\alpha_1),$$

and generally that

$$\beta_{i+1} > \tfrac{1}{2}(\beta-\beta_1-\ldots-\beta_i), \qquad \alpha_{i+1} > \tfrac{1}{2}(\alpha-\alpha_1-\ldots-\alpha_i).$$

Again, since G/G_1 has a characteristic sub-group of order $p^{\alpha_2}q^{\beta_1}$ and no self-conjugate sub-group whose order is a power of p,

$$p^{\alpha_2} < q^{\beta_1}.$$

Similarly $$q^{\beta_2} < p^{\alpha_2},$$

and so on. Thus $\beta_1 > \beta_2 > \ldots$ and $\alpha_2 > \alpha_3 > \ldots$;

but it cannot be inferred that $\alpha_1 > \alpha_2$, since G may have a self-conjugate sub-group whose order is a power of q.

It is not without interest to show how these results lend themselves to

the discussion of possible types of groups when the order is given. As a very simple illustration, I take the case of a group of order $3^8 . 5^2$. Here

$$3^5 < \frac{3^8}{5^2} < 3^6;$$

so that there must be characteristic sub-groups of order 3^i and $3^i 5^2$, i being not less than 6. The factor group of order $5^2 3^{8-i}$ must be such that in it no operation whose order is a power of 3 gives the identical isomorphism of the group of order 5^2. Hence i must be either 7 or 8. If i is 7, the group of order 5^2 is non-cyclic, and the factor group of order $5^2 . 3$ has no self-conjugate sub-group of order 5. Hence the characteristic sub-group, of order $3^7 . 5^2$, can have no sub-group, characteristic within itself, of order 5. But, if there were 3^4 sub-groups of order 5^2, there would be such a sub-group of order 5. Hence the group must either contain 5^2 sub-groups of order 3^8, with a self-conjugate sub-group of order $3^7 . 5^2$, which is a direct product; or it must contain a self-conjugate sub-group of order 3^8. To push the discussion further would be foreign to the subject of this paper.

Finally it should be remarked that for the two exceptional cases noted in the statement, the theorems proved above are not necessarily true. Thus, although 2^{11} is greater than 5^4, a group of order $2^{11} . 5^4$ may have no self-conjugate sub-group whose order is a power of 2. In fact, an Abelian group of order 5^4, whose operations are all of order 5, admits a group of isomorphisms of order 2^{11}. Similarly a group of order $2^{21} . 7^8$, though 7^8 is greater than 2^{21}, may have no self-conjugate sub-group whose order is a power of 7.