ON THE NUMBER OF ELEMENTS OF A GROUP WHICH HAVE A POWER IN A GIVEN CONJUGATE SET*

BY LOUIS WEISNER

1. *Introduction.* A fundamental theorem on abstract groups is Frobenius' theorem: The number of elements in a group of order g whose nth powers belong to a given conjugate set is zero or a multiple of the greatest common divisor of g and n. In this paper, I will prove the following theorems, which are also concerned with the number of elements having a power in a given conjugate set.

THEOREM 1. *The number of elements of a group whose nth powers are in a given conjugate set is either zero, or a multiple of the number of elements in the conjugate set.*

THEOREM 2. *In a group of order g, the number of elements which have a power in a given conjugate set of elements of order n is a multiple of the greatest divisor of g that is prime to n.*

An interesting deduction from Theorem 2 is the following theorem.

THEOREM 3. *In a group of order g, the number of elements whose orders are multiples of n is either zero, or a multiple of the greatest divisor of g that is prime to n.*

2. *Proof of Theorem* 1. Let $t_1, t_2, \cdots, t_x$ be the elements of a group G which satisfy the equation $t^n = s_1$, and let the conjugates of s_1 under G be $s_1, s_2, \cdots, s_m$. There exist elements $u_1, u_2, \cdots, u_m$ in G such that

$$u_i^{-1} s u_i = s_i, \qquad (i = 1, 2, \cdots, m).$$

Since $t_a^n = s_1$,

$$(u_i^{-1} t_a u_i)^n = u_i^{-1} s u = s_i.$$

* Presented to the Society, February 28, 1925.

Hence there are exactly x elements of G whose nth powers are s_i. If $u_i^{-1}t_a u_i = u_k^{-1}t_b u_k$, then, raising both members to the nth power, we have

$$u_i^{-1}su_i = u_k^{-1}su_k,$$

or $s_i = s_k$, whence $i = k$. It follows that $t_a = t_b$, whence $a = b$.

The distinct elements of G whose nth powers are conjugate to s_1 are therefore

$$u_i^{-1}t_a u_i, \qquad \begin{pmatrix} a = 1, 2, \cdots, x \\ i = 1, 2, \cdots, m \end{pmatrix},$$

and their number is mx.

3. *Proof of Theorem* 2. Suppose, first, that the conjugate set consists of only one element s, which is therefore invariant under the group G. Let k be the greatest divisor of g that is prime to n; and let $t^a = s$.

CASE 1: *a prime to n*. If $aa' \equiv 1 \pmod{n}$, then $t = s^{a'}$. An element u of G of order m prime to n, being commutative with s, is commutative with t. Hence

$$(tu)^{xm} = s^{a'xm}u^{xm} = s,$$

where $xa'm \equiv 1 \pmod{n}$. *Hence s is a power of tu.*

By Frobenius' theorem, G contains λk (λ integral) elements whose orders divide k. Denote these elements by $u_1, \cdots, u_{\lambda k}$. We have just proved that the only elements of G satisfying the equation $t^a = s$, where a assumes all values prime n, are

$$(1) \qquad s^{c_\mu}u_z, \qquad \begin{pmatrix} \mu = 1, \cdots, \varphi(n) \\ z = 1, \cdots, k \end{pmatrix},$$

where $c_1, \cdots, c_{\varphi(n)}$ are the integers not greater than n and prime to n. These elements are distinct;* hence their number is a multiple of k.

CASE 2: *a not prime to n*. Let $a = n_1 b$, where b is the greatest divisor of a that is prime to n. We may write $t = t_1 t_2$,† where t_1 and t_2 are powers of t, and the order of t_2 is the greatest divisor of the order of t that is prime to n, while the order of t_1 is a multiple n_2 of n which is not divisible by a number prime to n (except

* W. Burnside, *Theory of Groups*, 1911, § 16.

† Burnside, loc. cit.

unity). If the order of t_2 is c, then the order of t is n_2c. Since $s = t^{n_1b} = t_1^{n_1b}t_2^{n_1b}$, we may write

$$(2) \qquad s^n = t_1^{nn_1b}t_2^{nn_1b} = 1,$$

whence

$$t_1^{nn_1b} = t_2^{nn_1b} = 1.$$

Hence c is a divisor of nn_1b and therefore of b. It follows from (2) that $s = t_1^{n_1b}$. If u, of order m prime to n, is commutative with t, and if $m'm \equiv 1 \pmod{n_2}$, then

$$(3) \qquad (t_1u)^{m'mm_1b} = t_1^{m'mn_1b}u^{m'mn_1b} = t_1^{n_1b} = s.$$

Hence s is a power of t_1u.

Let n_3k_1 be the order of the normaliser N of t in G and let $g/n_3k_1 = n_4k_2$, where k_1 and k_2 are the greatest divisors of n_3k_1 and n_4k_2 respectively that are prime to n and hence to n_2. The number of elements of N whose orders are prime to n is of the form αk_1; denote these elements by

$$(4) \qquad u_1, \cdots, u_{\alpha k_1}.$$

It follows from (3) that s is a power of

$$(5) \qquad t_1u_1, \cdots, t_1u_{\alpha k_1}.$$

It is noteworthy that t_2 is in (4) and hence $t = t_1t_2$ is in (5). Let $t_1' = w^{-1}t_1w$ be a conjugate of t_1. Since s is invariant under G,

$$t_1'^{n_1b} = w^{-1}t_1^{n_1b}w = w^{-1}sw = s.$$

Now there are exactly αk_1 elements in G whose orders are prime to n and which are commutative with t_1'. Denoting these by $u_1', \cdots, u_{\alpha k_1}'$, it follows that s is a power of

$$(6) \qquad t_1'u_1', \cdots, t_1'u_{\alpha k_1}'.$$

Moreover, no element in (6) is equal to an element in (5).* There being n_4k_2 conjugates of t_1, we obtain $\alpha n_4k_1k_2$ elements of which s is a power. Observing that $k = k_1k_2$ is the greatest divisor of g prime to n, it follows that t_1 and its conjugates give rise in the manner described above to a

* Burnside, loc. cit.

multiple of k elements of which s is a power. These elements are evidently distinct from those obtained under Case 1.

If s is a power of τ and τ is not one of the elements already obtained, let $\tau = \tau_1\tau_2$, where the order of τ_2 is the greatest divisor of the order of τ that is prime to n. Then τ_1 and its conjugates give rise to a multiple of k elements of which s is a power. Let $\tau_1 v$ be one of these elements, and, if possible, let it be equal to an element in (5), say $\tau_1 v = t_1 u = v$. Since the order of u and the order of v are both equal to the greatest divisor of the order of w that is prime to n, we must have $\tau_1 = t_1$, $v = u$. This is not the case, and hence τ_1 and its conjugates give rise to a multiple of k new elements of which s is a power.

The theorem now follows under the assumption that s is invariant under G.

Suppose next that the conjugate set consists of powers of s, so that (s) is invariant under G. Denote the conjugates of s by

$$(7) \qquad s^{c_1}, \cdots, s^{c_r}, \qquad (c_1 = 1), (r > 1).$$

Let H, of order h, be the normaliser of s in G; and let k be the greatest divisor of h that is prime to n. The number of elements in H of which s is a power is a multiple of k, which we denote by λk. Since $c_1, \cdots, c_r$ are prime to n, $s^{c_1}, \cdots, s^{c_r}$ are powers of these same λk elements. Hence H contains exactly λk elements which have a power in (7). If t has a power in (7), so has t^{c_i} $(i = 1, 2, \cdots, r)$. Hence the number of elements of G which have powers in (7) is a multiple of r. The order of G is $g = rh$; for G/H is simply isomorphic with the group obtained by establishing an isomorphism of s with $s^{c_1}, \cdots, s^{c_r}$, and is of order r. The number of elements of G which have powers in (7) is a multiple of r and a multiple of k and is therefore a multiple of the greatest divisor of g that is prime to n.

Finally, suppose the conjugate set of elements does not consist of the powers of one of them. The elements in the conjugate set may be separated into subsets

$$
\begin{array}{llr}
(8_1) & s_1^{c_1}, \cdots, s_1^{c_r}, & (c_1 = 1), \\
(8_2) & s_2^{c_1}, \cdots, s_2^{c_r}, & (r \geqq 1), \\
 & \cdots\cdots\cdots\cdots\cdots\cdots & \\
(8_m) & s_m^{c_1}, \cdots, s_m^{c_r}, & (m > 1),
\end{array}
$$

such that any two elements in the same subset are powers of each other, whereas no element is a power of an element in another subset.

Let H_i, of order h, be the normaliser of (s_i), $(i = 1, \cdots, m)$. An element of G which has a power in (8_i) is commutative with the elements of (8_i) and hence is in H_i. Therefore H_i contains all the elements of G which have powers in (8_i). Since the elements of (8_i) form a complete set of conjugates under H_i, the number of elements of G which have powers in (8_i) is λk, where λ is an integer, and k is the greatest divisor of h that is prime to n. If t has a power in (8_i), t cannot have a power in (8_j), $(i \neq j)$. For if $t^x = s_i^c$ and $t^y = s_j^{c'}$, then t^x and t^y are of the same order n, so that each is a power of the other, whence $i = j$. It follows that the number of elements of G which have a power in (8) is $\lambda kg/h$, and this number is evidently a multiple of the greatest divisor of g that is prime to n.

4. *Proof of Theorem* 3. If the group G contains an element of order n, separate the elements of order n into complete sets of conjugates, which we denote by $C_1, \cdots, C_x$. Of these, we select a subset $C_1, \cdots, C_y$, such that no element in C_i has a power in C_j $(i \neq j)$, $(i, j = 1, \cdots, y)$. Every element of G whose order is a multiple of n has a power in one and only one of the sets $C_1, \cdots, C_y$; and the order of every element which has a power in one of these sets is a multiple of n. Since the number of elements of G which have a power in C_i is a multiple of the greatest divisor of g that is prime to n, it follows that the number of elements of G whose orders are multiples of n is a multiple of the greatest divisor of g that is prime to n.

UNIVERSITY OF ROCHESTER