ON THE ORDER OF GROUPS OF AUTOMORPHISMS*

BY

GARRETT BIRKHOFF AND PHILIP HALL

1. Introduction. Consider the following problem. Let $G$ be any group of finite order $g$, and let $A$ denote the group of the automorphisms of $G$. What can one infer about the order $a$ of $A$, simply from a knowledge of $g$: in other words, to what extent is $a$ a numerical function of $g$?

The main known result relating to this problem is due to Frobenius. It limits the orders of the individual elements of $A$ in terms of $g$, and hence tells which primes can be divisors of $a$.

The present paper is independent of the work of Frobenius, and presupposes only the theorems of Lagrange and Sylow. Its main result is the following

**Theorem 1.** Let $G$ be any group of finite order $g$. Let $\theta(g)$ denote the order of the group of the automorphisms of the elementary Abelian group of order $g$, and let $r$ denote the number of distinct prime factors of $g$. Then the order $a$ of the group $A$ of the automorphisms of $G$ is a divisor of $g^{r-1}\theta(g)$.

The function $\theta(g)$ is computed numerically from $g$ as follows. Write $g$ as the product $p_1^{n_1}p_2^{n_2}\cdots p_r^{n_r}$ of powers $p_i^{n_i}$ of distinct primes. Then

$$
\theta(p_k^{n_k}) = (p_k^{n_k} - 1)(p_k^{n_k} - p)\cdots (p_k^{n_k} - p^{n_k-1})
$$

$$
= p_k^{n_k(n_k-1)/2} \cdot (p_k^{2} - 1) \cdots (p_k^{n_k} - 1)
$$

and

$$
\theta(g) = \theta(p_1^{n_1})\theta(p_2^{n_2})\cdots \theta(p_r^{n_r}).
$$

For example, $\theta(12) = \theta(3)\theta(4) = 2 \cdot (3 \cdot 2) = 12$.

One can strengthen Theorem 1 in special cases, by

**Theorem 2.** If $G$ is solvable, then $a$ is a divisor of $g\theta(g)$.

**Theorem 3.** If $G$ is “hypercentral,” that is, the direct product of its Sylow subgroups, then $a$ is a divisor of $\theta(g)$.

2. Preliminary lemmas. The following two statements are immediate corollaries of Lagrange's and Sylow's Theorems, respectively:

---

* Presented to the Society, December 26, 1933; received by the editors August 20, 1935.
**Lemma 1.** Let $H$ be any group whose elements induce automorphisms homomorphically (i.e., many-one isomorphically) on a second group $G$. Then the index in $H$ of the subgroup "centralizing" $G$ (i.e., leaving every element of $G$ invariant) divides the order of the group of the automorphisms of $G$.

**Lemma 2.** Let $G$ be any group, and $r$ any positive integer. If the order of every prime-power subgroup of $G$ divides $r$, then the order of $G$ divides $r$.

As a further preliminary step, it is well to verify the somewhat less obvious

**Lemma 3.** Let $P$ be any group of prime-power order $p^n$, inducing substitutions homomorphically on $r = p^aq$ letters $x_1, \ldots, x_r$ [$p^a$ the highest power of $p$ dividing $r$]. Then there is a letter $x_k$ such that, if $S$ denotes the subgroup of substitutions of $P$ which omit $x_k$, the index of $S$ in $P$ divides $r$.

Let $S_i$ denote that subgroup of $P$ whose substitutions omit the letter $x_i$; by Lagrange's Theorem, the index of $S_i$ in $P$ is a power $p^{\beta(i)}$ of $p$. Hence the transitive system including $x_i$ contains exactly $p^{\beta(i)}$ letters. But the sum of the numbers of letters in the different transitive systems is not a multiple of $p^{a+1}$; hence $\beta(i) < \alpha$ for some $i = i_0$. Setting $S_i = S_{i_0}$, we have Lemma 3.

**Lemma 4.** Let $G$ be any group of prime-power order $p^n$. Then the order $a$ of the group $A$ of the automorphisms of $G$ divides $\theta(p^n) = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$.

By Lemma 2, it is sufficient to prove the result for every subgroup $Q$ of $A$ of prime-power order $q^n$. But given $Q$, one can define $Q_1 > Q_2 > Q_3 > \cdots > Q_r = 1$ and $S_1 < S_2 < S_3 < \cdots < S_r = G$ recursively as follows:

1. $Q_1$ is the group $Q$.
2. Given $Q_k$, $S_k$ is the subgroup of the elements of $G$ "centralized" by $Q_k$ (i.e., invariant under every automorphism of $Q_k$).
3. Given $Q_k$ and $S_k$, $Q_{k+1}$ is a proper subgroup of $Q_k$ whose index in $Q_k$ divides the number of elements in $G - S_k$.

The only questionable point in the existence of these subgroups concerns the possibility of (3); this is ensured by Lemma 3.

Moreover multiplying together on one side the indices of the $Q_{k+1}$ in the $Q_k$, and on the other their multiples, the degrees of the $G - S_k$, one sees that $q^n$ divides the product of those factors $(p^n - p^i)$ corresponding to the orders

† A more delicate result implying this, but presupposing a study of the structure of groups of prime-power order, is given by P. Hall in *A contribution to the theory of groups of prime-power order*, Proceedings of the London Mathematical Society, vol. 36 (1933), p. 37.
of complexes $G-S_k$. Hence a fortiori $q^m$ divides $\theta(p^n)$, and the lemma is proved.

3. Proof of principal theorem. We are now in a position to prove Theorem 1.

Accordingly, let $G$ be any group of finite order $g$, let $g=p_1^{r_1}\cdots p_r^{r_n}$, let $\theta(g)$ denote the order of the group of the automorphisms of the elementary Abelian group of order $g$, and let $A$ (of order $a$) denote the group of the automorphisms of $G$.

By Sylow's Theorem, $G$ contains subgroups $S_i$ of orders $p_i^{r_i}$ [$i=1,\ldots,r$; $j=1,\ldots,s_i$]. By Sylow's Theorem also, $s_i$ is the index in $G$ of the "normalizer" of any $S_i$ (i.e., the set of elements $a\in G$ such that $aS_iS_i^{-1}=S_i$); hence, by Lagrange's Theorem and the fact that $S_i$ is contained in its own normalizer, $s_i$ divides $g/p_i^{r_i}$.

Again, the automorphisms of $G$ obviously permute the $S_i$ of given order $p_i^{r_i}$ homomorphically. Therefore, by iterated use of Lemma 3, any subgroup $Q$ of $A$ of prime-power order $q^m$ contains a subgroup $Q_1$ whose index in $Q$ divides the product $\prod_{i=1}^{r}(g/p_i^{r_i})=g^{r-1}$, and which normalizes at least one $S_i$ of each order $p_i^{r_i}$. But by Lemma 1 and iterated use of Lemma 4, $Q_1$ has a subgroup $Q^*$ whose index in $Q_1$ divides $\theta(g)$, and which "centralizes" $S_i$ [i.e., leaves every element of these subgroups of $G$ invariant].

But the $S_i$ generate $G$; hence $Q^*$ contains only the identity, and $q^m$ divides $g^{r-1}\theta(g)$.

Theorem 1 now follows from Lemma 2 and the fact that $Q$ was permitted to be an arbitrary group of prime-power order.

4. Special cases of solvable and hypercentral groups. The proofs of Theorems 2-3 are now immediate.

In fact, Theorem 3 is really a corollary of Lemma 4. For the Sylow subgroups of a hypercentral group are characteristic. Denoting them by $S_1,\ldots,S_r$, one sees immediately that the group of the automorphisms of $G$ is the direct product of the groups of the automorphisms of the $S_i$, making the theorem obvious.

To prove Theorem 2, suppose that $G$ is solvable, and use the stronger known result,† analogous to Sylow's Theorem, that $G$ contains subgroups of every index $p_i^{r_i}$. Now in the proof of Theorem 1 presented in §3, if $q$ does not divide $g$, it is numerically evident that $q^m$ divides $\theta(g)$. Hence, by Lemma 2, it is sufficient to show that if $q$ divides $g$, then $q^m$ divides $g\theta(g)$.

† More particularly, the part that states that the inner automorphisms of $G$ are transitive on the Sylow subgroups of any fixed order.

But to say that \( q \) divides \( g \) is evidently to say that \( q = p_k \) for suitable \( k \); without loss of generality, we can assume \( k = 1 \). In this case \( Q \) normalizes some Sylow subgroup \( S \) of \( G \) of order \( p_1^{\alpha_1} \); this follows from Lemma 3 and the fact that the number of Sylow subgroups of order \( p_1^{\alpha_1} \), being a divisor of \( p_2^{\alpha_2} \cdots p_r^{\alpha_r} \), is not divisible by \( q \). Moreover \( Q \) has a subgroup \( Q_1 \) whose index in \( Q \) divides \( q^{\alpha_1} \) [and hence \( g \)] which “normalizes” (i.e., leaves invariant) a subgroup \( H \) of order \( p_2^{\alpha_2} \cdots p_r^{\alpha_r} \) (and index \( p_1^{\alpha_1} \)) in \( G \); this follows from Lemma 3 and the fact that by Hall’s Theorem cited above, the number of such subgroups \( H \) is a divisor of \( p_1^{\alpha_1} \).

Finally, by Lemmas 1 and 4, the index in \( Q_1 \) of the subgroup \( Q_2 \) “centralizing” \( S \) divides \( \theta(q^{\alpha_1}) \). And by induction on \( g \), the index in \( Q_2 \) of the subgroup \( Q^* \) “centralizing” \( H \) divides \( \theta(p_1^{\alpha_1} \cdots p_r^{\alpha_r}) \theta(p_2^{\alpha_2} \cdots p_r^{\alpha_r}) \), or, since it is by Lagrange’s Theorem a power of \( q = p_1 \) and relatively prime to \( p_2^{\alpha_2} \cdots p_r^{\alpha_r} \), it divides \( \theta(p_2^{\alpha_2} \cdots p_r^{\alpha_r}) \). But \( S \) and \( H \), if only by Lagrange’s Theorem, generate \( G \); hence \( Q^* = 1 \). Combining, one sees that if \( q \) divides \( g \), then \( q^m \) divides \( g \theta(p_1^{\alpha_1}) \theta(p_2^{\alpha_2} \cdots p_r^{\alpha_r}) \), that is, \( g \theta(g) \). But this is just what we wished to prove.

5. Possible improvement of results. It is natural to ask what likelihood there is of improving the results expressed in Theorems 1-3.

It is well known that the least upper bound to the possible values of \( a \) for fixed \( g \) is at least \( \theta(g) \); this is shown by the elementary Abelian group of order \( g \). Consequently Theorem 3 is a best possible result. Moreover in general \( \theta(g) \) is not a common multiple for the possible values of \( a \), as is shown by the dihedral group of order six and many other groups of similar structure.

On the other hand, there is no known example of a group for which \( a \) fails to divide \( g \theta(g) \); this suggests the possibility of replacing \( g^{r-1} \theta(g) \) in Theorem 1 by \( g \theta(g) \), and omitting Theorem 2 altogether.

This leaves the determination of lower bounds and common divisors of \( a \) in terms of \( g \) unattempted. The cyclic groups of order \( g \) should throw considerable light on this more trivial question.

Also, the case in which \( G \) is simple would probably repay study.

Harvard University, Cambridge, Mass.

King’s College, Cambridge, England.