ON A CONJECTURE OF FROBENIUS

WALTER FEIT

1. Introduction. Let $G$ be a finite group of order $g$, where $g = qm$ with $(q, m) = 1$. Let $M$ denote the set of all elements of $G$ whose order divides $m$. Frobenius proved that the number of elements in $M$ is a multiple of $m$. He furthermore conjectured that if $M$ contains exactly $m$ elements, then it is a normal subgroup of $G$. The normality of $M$ in $G$ is obvious from the definition, the difficulty arises in trying to prove that $M$ is a group. Frobenius was able to prove the following special case of his conjecture.

Theorem 1.1. If $G$ contains a subgroup $Q$ of order $q$ with the properties:

(i) The normalizer of $Q$ in $G$ is $Q$.

(ii) The intersection of $Q$ with any subgroup conjugate to $Q$ is either $Q$ or the group $\{1\}$ consisting of the identity element of $G$ only.

Then there are exactly $m - 1$ elements not lying in any subgroup conjugate to $Q$, and these together with the identity element of $G$ form a normal subgroup of $G$.

It is not necessary in the above theorem to assume that $(m, q) = 1$, as this can easily be verified from the other hypotheses. One of the consequences of the theorems in this paper is Theorem 1.1 with hypothesis (I) replaced by the assumption that $M$ contains exactly $m$ elements.

Several attempts have been made to prove Theorem 1.1 without using character theory. Under the assumption that the group $Q$ is
solvable, this has been done. If we assume that the group \( \mathfrak{O} \) in Theorem 3.1 is solvable, then it is possible to prove that theorem without the use of characters. Enough information about the structure of the group \( \mathfrak{O} \) is given so that a theorem which Higman has proved without using character theory can be applied.

In §8, another special case of the conjecture is proved which is independent of the preceding results. The method used there does not involve the theory of characters in any way.

2. Prerequisite and notation. A subgroup \( \mathfrak{C} \) of \( \mathfrak{O} \) is called an elementary group if it is the direct product \( \mathfrak{A} \times \mathfrak{B} \) of a cyclic group \( \mathfrak{A} \) and a \( p \)-group \( \mathfrak{B} \), where \( p \) is a prime which does not divide the order of \( \mathfrak{A} \). It is important to note that the definition of \( \mathfrak{C} \) implies that \( \mathfrak{B} \) is in the centralizer of \( \mathfrak{A} \).

The main tool used in the proof of Theorem 3.1 is the following result due to R. Brauer.

**Theorem 2.1.** A complex-valued function \( \theta \) defined on the group \( \mathfrak{O} \) is an irreducible character of \( \mathfrak{O} \) if and only if \( \theta \) satisfies the following conditions:

1. \( \theta \) is a class function on \( \mathfrak{O} \).
2. For every elementary subgroup \( \mathfrak{C} \) of \( \mathfrak{O} \), the restriction of \( \theta \) to \( \mathfrak{C} \) is a character of \( \mathfrak{C} \).
3. \( \theta(1) \) is positive.
4. \( \sum \theta(G)\bar{\theta}(G) = 1 \), where \( G \) ranges over the group \( \mathfrak{O} \) in the summation, and \( \bar{\theta}(G) \) is the complex conjugate of \( \theta(G) \).

In the sequel, capital letters, \( A, B, \cdots \) will be used to denote group elements. If \( \mathfrak{A} \) is a subset of the group \( \mathfrak{O} \) then the symbol \( o(\mathfrak{A}) \) will denote the number of elements in the set \( \mathfrak{A} \). If \( \mathfrak{A} \) is a group, then of course \( o(\mathfrak{A}) \) is the order of \( \mathfrak{A} \). For any complex-valued function \( \theta \) defined on \( \mathfrak{A} \), \( \sum_{\mathfrak{A}} \theta(G) \) will mean that the summation ranges over all elements \( G \) in \( \mathfrak{A} \); if \( \mathfrak{B} \) is another subset of \( \mathfrak{O} \), \( \mathfrak{A} - \mathfrak{B} \) will stand for the set of all elements which are in \( \mathfrak{A} \) but not in \( \mathfrak{B} \); \( \mathfrak{B} \) need not be contained in \( \mathfrak{A} \). Finally if \( G \) is an element of \( \mathfrak{O} \), \( c(G) \) will denote the centralizer of \( G \) in \( \mathfrak{O} \) and \( e(G) \) will denote the order of this centralizer.

4 See [4]. A stronger result is proved there. Instead of hypothesis (II), Grün assumed that \( \mathfrak{O} \) contains a normal subgroup \( \mathfrak{Q} \) such that \( \mathfrak{O}/\mathfrak{Q} \) is solvable and the intersection of \( \mathfrak{O} \) with any subgroup conjugate to \( \mathfrak{Q} \) is contained in \( \mathfrak{Q} \). He was then able to show that \( \mathfrak{O} \) contains a normal subgroup \( \mathfrak{B} \) with the properties that \( \mathfrak{B}/\mathfrak{B} \) is isomorphic to \( \mathfrak{O}/\mathfrak{Q} \) and \( \mathfrak{O}/\mathfrak{B} \) is isomorphic to \( \mathfrak{O}/\mathfrak{Q} \). This result is analogous to Theorem 3.2, although the methods used to prove it are entirely different.

6 See either [1, p. 371 and footnote 8 on that page] or see [5, p. 496].

6 See [1, p. 357].
3. Statement of the results. The main results of this paper are contained in the following two theorems.

**Theorem 3.1.** Let $G$ be a group of order $g = mq$, with $(m, q) = 1$. If $Q$ is any element of $G$ whose order divides $q$, suppose that the number of elements in $\mathcal{C}(Q)$ whose order divides $m$ is exactly $(m, c(Q))$. Furthermore, assume that $G$ contains a subgroup $\mathcal{Q}$ of order $q$ with the property that any element $Q$ of order dividing $q$ is conjugate to some element of $\mathcal{Q}$. Then the set $\mathcal{M}$ of all elements whose order divides $m$ is a normal subgroup of $G$.

**Theorem 3.2.** Let $G$ be a group of order $g = qm$, with $(q, m) = 1$. Suppose that the set $\mathcal{M}$ of all elements whose order divides $m$ contains exactly $m$ elements. Furthermore, assume that $G$ contains a subgroup $\mathcal{H}$ of order $h = qs$, with $(s, m/s) = 1$, and with the properties:

1. The group $\mathcal{H}$ contains a normal subgroup $\mathcal{Q}$ of order $s$.
2. The intersection of $\mathcal{H}$ with any group conjugate to $\mathcal{Q}$ is either $\mathcal{Q}$ or is contained in $\mathcal{Q}$.

Then $\mathcal{M}$ is a normal subgroup of $G$.

The conditions of both the above theorems are also necessary for $\mathcal{M}$ to be a normal subgroup of $G$. We shall prove this for Theorem 3.1 in §6. The converse of Theorem 3.2 is immediate, for if $\mathcal{M}$ is a normal subgroup of $G$, then we may choose $\mathcal{H}$ to be the group $G$. By letting $s = 1$ in Theorem 3.2 we get the above mentioned generalization of Theorem 1.1.

4. Some lemmas. The proof of Theorem 3.1 rests mainly on Theorem 2.1; however, before we are able to apply that result it is necessary to get some information about the structure of the group $G$ with which we are dealing. Accordingly we prove several lemmas which will be needed. Before doing this we introduce the following notation.

If $Q$ is an element of $G$, define the set $\mathcal{M}_Q$ to consist of all elements in $G$ whose with power is conjugate to $Q$. Let $h(Q) = g/c(Q)$ denote the number of elements of $G$ which are conjugate to $Q$. We shall also find it convenient to write $c(Q)$ as a product $c(Q) = m(Q)q(Q)$, where $m(Q)$ divides $m$ and $q(Q)$ divides $g$.

**Lemma 4.1.** If $G$ satisfies the hypotheses of Theorem 3.1, then

\[ o(\mathcal{M}_Q) = mq/q(Q). \]

---

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Proof. Any element $G$ in $\mathfrak{G}$ can be written in a unique way as a product $G = M_1 Q_1 = Q_1 M_1$, where $Q_1^m = 1 = M_1^m$. If furthermore $G^m = Q_1^m = Q$, then it is easily seen that $Q_1$ is a fixed element depending only on $Q$. Hence the correspondence $G = M_1 Q_1 \leftrightarrow M_1$ is one-to-one between the elements $G$ whose $m$th power is $Q$ and the elements $M_1$ in $C(Q)$ whose order divides $m$. Therefore it follows from the hypotheses of Theorem 3.1 that the number of elements whose $m$th power is $Q$ equals $m(Q)$, consequently the number of elements in $M_Q$ is $h(Q)m(Q) = mq/q(Q)$ as was to be shown.

Lemma 4.2. Under the hypotheses of Theorem 3.1, $\mathfrak{G}$ contains a subgroup $\mathfrak{Q}$ of order $q$ with the following properties:

(I) Any two elements of $\mathfrak{Q}$ which are conjugate in $\mathfrak{G}$ are also conjugate in $\mathfrak{Q}$.

(II) If $Q$ is in $\mathfrak{Q}$, then the order of $e(Q)\Pi Q$ is $q(Q)$.

Proof. Every element $G$ in $\mathfrak{G}$ belongs to precisely one of the sets $M_Q$, where $Q$ ranges over representatives of classes of elements conjugate in $\mathfrak{Q}$ whose order divides $q$. By assumption each such class contains an element which lies in $\mathfrak{Q}$, and we may pick this as the representative. Hence using equation (1) we get

\begin{equation}
q = \sum \frac{q}{q(Q)}
\end{equation}

where the summations in equations (2) and (3) range over the classes of elements in $\mathfrak{Q}$ which are conjugate in $\mathfrak{G}$.

It is easily seen that

\begin{equation}
\sigma(Q \cap Q) \leq (c(Q), q) = q(Q),
\end{equation}

or in other words

\begin{equation}
\sigma(Q) \geq \frac{q}{q(Q)},
\end{equation}

where the summation ranges over all classes of elements in $\mathfrak{Q}$ which are conjugate to $Q$ in $\mathfrak{Q}$. The class equation of $\mathfrak{Q}$ may be written as

\begin{equation}
q = \sum h Q(Q),
\end{equation}

where $h Q(Q)$ denotes the number of elements in $\mathfrak{Q}$ which are conjugate to $Q$ in $\mathfrak{Q}$. The class equation of $\mathfrak{Q}$ may be written as
are conjugate in \( \mathfrak{Q} \). Clearly the number of classes of elements in \( \mathfrak{Q} \) which are conjugate in \( \mathfrak{Q} \) is greater than or equal to the number of classes of elements in \( \mathfrak{Q} \) which are conjugate in \( \mathfrak{G} \). Hence on comparing equations (3) and (6) we see that there are at least as many terms in the sum in (6) as there are in the sum in (3). From equation (5) it follows that to any summand in (3) corresponds a summand in (6) which is at least as big. As the two sums both equal \( q \), we conclude that we must have the same number of terms in both the equations and corresponding terms must be equal. This proves both statements of the lemma.

5. The proof of Theorem 3.1. Suppose that the group \( \mathfrak{G} \) satisfies the assumptions of Theorem 3.1. Let \( Z \) be an irreducible representation of \( \mathfrak{Q} \), and let \( \rho \) denote the character of \( Z \). We now define the function \( \chi \) on the group \( \mathfrak{G} \) by

\[
(7) \quad \chi(G) = \rho(Q),
\]

where \( G = MQ = QM \), with \( M^m = 1 = Q^q \), and where \( Q \) is conjugate to \( Q_i \) which lies in \( \mathfrak{Q} \).

**Lemma 5.1.** The function \( \chi \) defined by equation (7) is a single-valued function whose domain of definition is all of \( \mathfrak{G} \).

**Proof.** As every element \( G \) can be written in the form \( G = MQ = QM \), with \( Q \) conjugate to an element of \( \mathfrak{Q} \), \( \chi \) is defined on the whole group \( \mathfrak{G} \).

Suppose that \( G = MQ = QM \) with \( Q \) conjugate to both \( Q_1 \) and \( Q_2 \) in \( \mathfrak{Q} \). Then \( Q_1 \) and \( Q_2 \) are conjugate in \( \mathfrak{G} \), and hence by Lemma 4.2, also in \( \mathfrak{Q} \). Therefore as \( \rho \) is a class function on \( \mathfrak{Q} \), \( \rho(Q_1) = \rho(Q_2) \) and \( \chi(G) \) is uniquely determined.

The last result that we now need before giving the proof of Theorem 3.1 is the following.

**Lemma 5.2.** The function \( \chi \) defined by equation (7) on the group \( \mathfrak{G} \) is an irreducible character of \( \mathfrak{G} \). The representation \( Z' \) of \( \mathfrak{G} \) with character \( \chi \) contains \( M \) in its kernel.

**Proof.** After it is proved that \( \chi \) is an irreducible character of \( \mathfrak{G} \), the second part of the lemma is an immediate consequence of the fact that the kernel of a representation consists of all elements \( G \) with \( \chi(G) = \chi(1) \), where \( \chi \) is the character of the representation, as by the definition of \( \chi \), \( \chi(G) = \chi(1) \) for all \( G \) in \( \mathfrak{M} \). Hence it suffices to show that \( \chi \) is an irreducible character of \( \mathfrak{G} \). This will be done by showing that \( \chi \) satisfies conditions (I)-(IV) of Theorem 2.1.
Let $G_i = Q_iM_i = M_iQ_i$ with $Q_i^k = 1 = M_i^k$, $i = 1, 2$. If $G_1$ is conjugate to $G_2$ in $\mathfrak{G}$, then it is easily checked that $Q_1$ is conjugate to $Q_2$ in $\mathfrak{G}$ and therefore also in $\mathfrak{Q}$. Therefore $\rho(Q_1) = \rho(Q_2)$, and by the definition of $\chi$, $\chi(G_1) = \chi(G_2)$. This shows that $\chi$ is a class function on $\mathfrak{G}$, and thus satisfies condition (I) of Theorem 2.1.

To verify condition (II), that the restriction of $\chi$ to any elementary subgroup $\mathfrak{E}$ is a character, it is sufficient to show that the restriction of $\chi$ to some group conjugate to $\mathfrak{E}$ is a generalized character, because $\chi$ is a class function. Every elementary subgroup $\mathfrak{E}$ of $\mathfrak{G}$ may be written as a direct product

$$\mathfrak{E} = \mathfrak{A}_1 \times \mathfrak{A}_2 \times \mathfrak{P},$$

where $\mathfrak{A}_i$ is cyclic of order $a_i$, $i = 1, 2$, with $a_1$ dividing $q$ and $a_2$ dividing $m$, and where $\mathfrak{P}$ is a $p$-group for some prime $p$. We shall consider two cases depending on whether the prime $p$ divides $m$ or $q$.

If $p$ divides $m$, then by taking a subgroup conjugate to $\mathfrak{E}$ we may as well assume that $\mathfrak{A}_1$ is contained in $\mathfrak{Q}$. In this case it is easily seen that $\chi$ restricted to $\mathfrak{E}$ is simply the product of the character $\rho_0$ of $\mathfrak{A}_1$ with the trivial character of $\mathfrak{A}_2 \times \mathfrak{P}$, where $\rho_0$ is the restriction of $\rho$ to $\mathfrak{A}_1$. Hence in this case, $\chi$ restricted to $\mathfrak{E}$ is a character.

Now it is necessary to consider only the case that $p$ divides $q$. Let $Q$ be a generator of $\mathfrak{A}_1$, where we may once again assume that $Q$ lies in $\mathfrak{Q}$ by picking a subgroup conjugate to $\mathfrak{E}$. The group $\mathfrak{P}$ lies in $\mathfrak{E}(Q)$, hence $\mathfrak{P}$ lies in a Sylow $p$-group $\mathfrak{P}'$ of $\mathfrak{E}(Q)$. By Lemma 4.2 (II), $\mathfrak{Q} \cap \mathfrak{E}(Q)$ contains a Sylow subgroup $\mathfrak{P}'$ of $\mathfrak{E}(Q)$. Therefore there exists $G$ in $\mathfrak{E}(Q)$ such that $\mathfrak{P}' = G \mathfrak{P}' G^{-1}$. Consequently,

$$G \mathfrak{P} G^{-1} \subset \mathfrak{A}_1 \times \mathfrak{A}_2 \mathfrak{P}^{-1} \times \mathfrak{G} \mathfrak{P} \mathfrak{P}' \mathfrak{G}^{-1} = \mathfrak{A}_1 \times \mathfrak{A}_2 \mathfrak{P}^{-1} \times \mathfrak{P}' \mathfrak{P},$$

as $G$ in $\mathfrak{E}(Q)$ commutes with $\mathfrak{A}_1 = \{Q\}$. In other words, some subgroup conjugate to $\mathfrak{E}$ is of the form (8) with $\mathfrak{A}_1 \times \mathfrak{P}$ in $\mathfrak{Q}$. Now it follows immediately from the definition that $\chi$ is the product of the character $\rho_0$ of $\mathfrak{A}_1 \times \mathfrak{P}$ with the trivial character of $\mathfrak{A}_2$, where $\rho_0$ is the restriction of $\rho$ to $\mathfrak{A}_1 \times \mathfrak{P}$. Hence also in this case $\chi$ is a character on $\mathfrak{E}$. This completes the verification of condition (II).

Condition (III) is trivially true, so it now only remains to show that $\chi$ satisfies condition (IV).

If $G_1$ and $G_2$ are any two elements in $\mathfrak{M}_Q$, then it was shown earlier that

$$G_i = Q'M_i = M_iQ'', \quad i = 1, 2,$$

with $Q'$ conjugate to $Q''$ and with $Q'^{q} = 1 = M_i^{q}$. Hence $\chi(G_1) = \chi(G_2) = \rho(Q')$. Therefore equation (1) implies
ON A CONJECTURE OF FROBENIUS

The last equality follows from the fact that \( Q \) and \( Q' \) are powers of each other as is easily seen. As \( \rho \) is an irreducible character of \( \Omega \), the orthogonality relations yield

\[
(12) \sum_{\Omega} h_{\Omega}(Q')\rho(Q')\overline{\rho(Q')} = q,
\]

where the prime on the summation means that the classes of \( \Omega \) rather than the elements of \( \Omega \) are summed over. By Lemma 4.2 the sum in (12) ranges over classes of elements of \( \Omega \) which are conjugate in \( \Theta \). Furthermore by the same lemma \( h_{\Omega}(Q) = q/q(Q) \). Upon combining equations (11) and (12) we now get

\[
(13) \sum_{\Omega} h(G)\chi(G)\overline{\chi(G)} = \sum_{\Omega} \left( \sum_{\Omega} h_{\Omega}(Q')\rho(Q')\overline{\rho(Q')} \right) = \sum_{\Omega} \frac{mq}{q(Q)}\rho(Q')\overline{\rho(Q')} \]

This shows that \( \chi \) satisfies condition (IV) and completes the proof of the lemma.

The proof of Theorem 3.1 is now very simple. Let \( \rho_1, \ldots, \rho_k \) be the set of all irreducible characters of \( \Omega \). Let the functions \( \chi_1, \ldots, \chi_k \) be defined by equation (7). It follows from Lemma 5.2 that there exist irreducible representations \( Z'_1, \ldots, Z'_k \) of \( \Theta \), each of which contains \( \mathbb{M} \) in its kernel, and with the property that the character of \( Z'_i \) is \( \chi_i \), for \( i = 1, \ldots, k \). Let \( \mathbb{M}_i \) be the kernel of \( Z'_i \). We define \( \mathbb{M}' \) by

\[
(14) \mathbb{M}' = \bigcap \mathbb{M}_i.
\]

By definition, \( \mathbb{M}' \) is a normal subgroup of \( \Theta \), and by Lemma 5.2, \( \mathbb{M} \) is contained in \( \mathbb{M}' \). To complete the proof it only remains to show that \( \mathbb{M}' \) is contained in \( \mathbb{M} \).

Let \( G \) be an element in \( \mathbb{M}' \), then \( G = QM \) where \( Q^n = 1 = M^n \), and \( QM = MQ \). By assumption \( Q \) is conjugate to an element \( Q_i \) of \( \Omega \), hence by the definition of \( \chi_i \), \( \chi_i(G) = \rho_i(Q_i) \) for \( i = 1, \ldots, k \). If \( Q_i \neq 1 \), then there is some character \( \rho_j \) of \( \Omega \) such that \( \rho_j(Q_i) \neq \rho_j(1) \), therefore \( \chi_i(G) \neq \chi_i(1) \) which implies that \( G \) is not in \( \mathbb{M}_i \) and therefore not in \( \mathbb{M}' \). Consequently \( Q_i = 1 \), hence \( Q = 1 \), and therefore \( G = M \), where \( M \) lies in \( \mathbb{M} \). This completes the proof of Theorem 3.1.

6. The converse of Theorem 3.1. Before proceeding with a proof of the converse of Theorem 3.1, we shall prove a result which is needed here and will also be used later.
Lemma 6.1. Let $\mathfrak{G}$ be a group of order $g = mq$, with $(m, q) = 1$. Suppose that $\mathfrak{G}$ contains a normal subgroup $\mathfrak{N}$ of order $m$. If $\mathfrak{Q}$ is any subgroup of $\mathfrak{G}$ of order $q$, and if $A$ is an element whose order divides $q$, then $A$ is conjugate to an element of $\mathfrak{Q}$.

Proof. As the order of $\mathfrak{Q}$ equals the order of $\mathfrak{G}/\mathfrak{N}$ and as $(m, q) = 1$, the correspondence $G \to \mathfrak{G}/\mathfrak{N}$ is an isomorphism between $\mathfrak{Q}$ and $\mathfrak{G}/\mathfrak{N}$. Therefore there is some element of $\mathfrak{Q}$ in every coset of $\mathfrak{N}$ in $\mathfrak{G}$. Let $Q$ be the element of $\mathfrak{Q}$ in $A\mathfrak{N}$. If $(A\mathfrak{N})^a = A^a\mathfrak{N} = \mathfrak{N}$, then $A^a$ lies in $\mathfrak{N}$, as the order of $A$ is relatively prime to $m$, this implies that $A^a = 1$. Conversely, if $A^a = 1$, clearly $(A\mathfrak{N})^a = \mathfrak{N}$. Therefore the order of $Q$ equals the order $a$ of $A$, because $Q$ has the same order as $Q\mathfrak{N} = A\mathfrak{N}$ in $\mathfrak{G}/\mathfrak{N}$. Let $A$ be the cyclic group generated by $A$, and let $\mathfrak{S} = A\mathfrak{N}$. As $\mathfrak{N}$ is normal in $\mathfrak{G}$, $\mathfrak{S}$ is a group, furthermore $Q$ lies in $\mathfrak{S}$. By a theorem of Zassenhaus, $A$ is conjugate in $\mathfrak{S}$ to the cyclic group generated by $Q$. Hence in particular $A$ is conjugate in $\mathfrak{G}$ to some power of $Q$ as was to be proved.

The converse of Theorem 3.1 can now be proved.

Theorem 6.1. Let $\mathfrak{G}$ be a group of order $g = mq$, with $(m, q) = 1$. Suppose that $\mathfrak{G}$ contains a normal subgroup $\mathfrak{N}$ of order $m$. Then there exists a subgroup $\mathfrak{Q}$ of $\mathfrak{G}$ of order $q$ with the properties:

(I) Every element in $\mathfrak{G}$ whose order divides $q$ is conjugate to an element of $\mathfrak{Q}$.

(II) If $Q$ is in $\mathfrak{Q}$, then the number of elements in $\mathfrak{G}(Q)$ whose orders divide $m$ is exactly $(m, c(Q))$.

Proof. The existence of $\mathfrak{Q}$ follows from a theorem of Schur. Condition (I) is simply a restatement of Lemma 6.1. Condition (II) is an immediate consequence of the fact that $\mathfrak{N} \cap \mathfrak{C}(Q)$ is a normal subgroup of $\mathfrak{C}(Q)$ and consequently contains all elements of $\mathfrak{C}(Q)$ whose order divides $m$. Clearly the order of $\mathfrak{N} \cap \mathfrak{C}(Q)$ is precisely $(m, c(Q))$.

7. The proof of Theorem 3.2. In this section it will be shown that if a group $\mathfrak{G}$ satisfies the assumptions of Theorem 3.2, then $\mathfrak{G}$ also satisfies the assumptions of Theorem 3.1. The proof is broken up into several lemmas.

Let $\mathfrak{R}$ denote the normalizer of $\mathfrak{S}$, where $\mathfrak{S}$ is defined in Theorem 3.2. Let the order of $\mathfrak{R}$ be $n = ht = qst$.

Lemma 7.1. Under the hypotheses of Theorem 3.2, every element of $\mathfrak{G} - \mathfrak{N}$ is in the normalizer of a subgroup of $\mathfrak{G}$ which is conjugate to $\mathfrak{S}$.

* See [7, p. 143].
* See [7, p. 143].
Proof. If \( G \) is in \( \mathcal{G} - \mathcal{M} \), there is a prime \( p \) which divides \( q \) and also the order of \( G \), hence some power \( P \) of \( G \) has order \( p \). The element \( G \) commutes with \( P \). In other words, there is an element \( P \) in \( \mathcal{G} \) of order \( p \) with the property

\[
P = G^{-1}PG.
\]

The element \( P \) is in some Sylow \( p \)-group \( \Psi' \) of \( \mathcal{G} \). If \( \Psi \) is a Sylow \( p \)-group of \( \mathcal{G} \), then it is also a Sylow \( p \)-group of \( \mathcal{G} \) and therefore conjugate to \( \Psi' \). Thus there exists an element \( K \) of \( \mathcal{G} \), such that

\[
P \in \Psi' = K\Psi K^{-1} \subset K\mathcal{G}K^{-1} = \mathcal{G}'.
\]

Equations (15) and (16) imply that

\[
P = G^{-1}PG \in \mathcal{G}' \cap G^{-1}\mathcal{G}'G.
\]

The hypotheses of Theorem 3.2 state that if \( \mathcal{G}' \) is distinct from \( G^{-1}\mathcal{G}'G \), then the intersection of the two groups has order dividing \( s \), and thus cannot contain the element \( P \) of order \( p \). Therefore \( \mathcal{G}' \) and \( G^{-1}\mathcal{G}'G \) cannot be distinct. This implies that \( G \) is in the normalizer of \( \mathcal{G}' \), where \( \mathcal{G}' \) is conjugate to \( \mathcal{G} \).

Lemma 7.2. Under the hypotheses of Theorem 3.2, the number of elements in \( \mathcal{N} \cap \mathcal{M} \) is exactly \( st \), and these elements form a normal subgroup \( \mathcal{U} \) of \( \mathcal{N} \). The intersection of \( \mathcal{N} \) with any subgroup conjugate to \( \mathcal{N} \) contains only elements of \( \mathcal{M} \).

Proof. The number of elements in \( \mathcal{N} \cap \mathcal{M} \) is a nonzero multiple\(^{10} \) of \( st \), hence greater than or equal to \( st \), therefore

\[
o(\mathcal{N} - \mathcal{M}) \leq qst - st.
\]

The number of groups conjugate to \( \mathcal{N} \) is at most \( g/qst \). It follows from Lemma 7.1 that every element of \( \mathcal{G} - \mathcal{M} \) is in one of the subgroups conjugate to \( \mathcal{N} \). This yields

\[
o(\mathcal{G} - \mathcal{M}) \leq \frac{g}{qst} (qst - st) = \frac{g}{q} = g - m.
\]

By hypothesis, the number of elements in \( \mathcal{G} - \mathcal{M} \) is exactly \( g - m \). Hence we must have equality in (18), and no element in (19) can be counted more than once. That is to say, the intersection of \( \mathcal{N} \) with any subgroup conjugate to \( \mathcal{N} \) can contain only elements of \( \mathcal{M} \).

It only remains now to show that the \( st \) elements in \( \mathcal{N} \), whose order divides \( st \), form a normal subgroup of \( \mathcal{N} \).

\(^{10} \)See footnote 2.
The group $\mathcal{N}$ contains the normal subgroup $\mathcal{H}$ of order $h = qs$. It follows from the choice of $s$ that $(qs, t) = 1$. Schur's Theorem applied to the group $\mathcal{N}$ states that $\mathcal{N}$ contains a subgroup $\mathcal{T}$ of order $t$. It is easily seen that the subgroup $\mathcal{S}$ of $\mathcal{H}$ of order $s$ is normal in $\mathcal{N}$, hence $\mathcal{U} = \mathcal{S}\mathcal{T}$ is a group. The order of $\mathcal{U}$ clearly equals $st$. As $\mathcal{N}$ contains exactly $st$ elements of order dividing $st$, they must all lie in $\mathcal{U}$, and therefore $\mathcal{U}$ is a normal subgroup of $\mathcal{N}$.

We can now complete the proof of Theorem 3.2. Condition (1) of that theorem and Schur's Theorem yield the existence of a subgroup $\mathcal{Q}$ of $\mathcal{H}$, and therefore of $\mathcal{G}$, of order $q$. If $G$ is an element of $\mathcal{C}(Q)$, where $Q$ lies in $\mathcal{Q}$, then $Q$ is in $\mathcal{S}\cap G^{-1}\mathcal{S}G$ and the same argument that was used in Lemma 7.1 implies that $\mathcal{S} = G^{-1}\mathcal{S}G$, consequently $G$ lies in $\mathcal{H}$, or in other words,

$$\mathcal{C}(Q) \subseteq \mathcal{N}.$$ 

By Lemma 7.2, $\mathcal{M} \cap \mathcal{N}$ is a normal subgroup of $\mathcal{N}$, consequently $\mathcal{C}(Q) \cap \mathcal{M}$ is a normal subgroup of $\mathcal{C}(Q)$. From this it easily follows that the number of elements in $\mathcal{C}(Q) \cap \mathcal{M}$ is exactly $(c(Q), m)$.

To complete the proof of Theorem 3.2 it is now sufficient to show that every element $Q$ of $\mathcal{Q}$ whose order divides $q$ is conjugate to an element of $\mathcal{Q}$. By Lemma 7.1, $Q$ lies in some group conjugate to $\mathcal{N}$ hence by a change of notation we may assume $Q$ lies in $\mathcal{N}$. As $\mathcal{S}$ is a normal subgroup of $\mathcal{N}$ whose index is relatively prime to $q$, $Q$ must lie in $\mathcal{S}$. By assumption $\mathcal{S}$ contains a normal subgroup $\mathcal{S}$ of index $q$ and therefore by Lemma 6.1, $Q$ is conjugate to an element of $\mathcal{Q}$ as was to be shown.

8. The case that $\mathcal{Q}$ is a cyclic $p$-group. There is another case in which the conjecture can be proved, namely when $q$ is the power of a prime $p$, and when the Sylow $p$-group $\mathcal{P}$ is cyclic. We shall say that an element $G$ in $\mathcal{G}$ is $p$-regular if the order of $G$ is relatively prime to $p$; if $G$ is not $p$-regular then it is said to be $p$-singular.

**Theorem 8.1.** Let $\mathcal{G}$ be a group of order $p^am$, with $p$ not dividing $m$. If the set $\mathcal{M}$ of $p$-regular elements of $\mathcal{G}$ contains exactly $m$ elements, and if the Sylow $p$-group $\mathcal{P}$ of $\mathcal{G}$ is cyclic, then $\mathcal{M}$ is a normal subgroup of $\mathcal{G}$.

**Proof.** Let $\mathcal{A}$ be the unique subgroup of $\mathcal{P}$ of order $p$. As all the $p$-Sylow groups of $\mathcal{G}$ are conjugate and as each group of order $p$ is characteristic in any Sylow group in which it is contained, all groups of order $p$ are conjugate in $\mathcal{G}$. Every $p$-singular element of $\mathcal{G}$ must

---

11 See footnote 9.
12 See footnote 9.
ON A CONJECTURE OF FROBENIUS

... commute with some element of order $p$, namely a suitable power of itself. Therefore every $p$-singular element of $\mathfrak{G}$ lies in the centralizer of some group which is conjugate to $\mathfrak{H}$. Let $\mathcal{C}$ denote the centralizer of $\mathfrak{H}$, and $\mathfrak{N}$ the normalizer of $\mathfrak{H}$, and let their orders be respectively $c$ and $n$. The Sylow group $\mathfrak{V}$ is contained in $\mathcal{C}$, which in turn is contained in $\mathfrak{N}$. Hence $c = np^c_1$, $n = np^n_1$ where $c_1$ divides $n_1$.

The number of $p$-regular elements in any group conjugate to $\mathcal{C}$ is a multiple of $c_1$, thus we get

$$\text{(21)} \quad o(\mathcal{C} - \mathfrak{M}) \leq p^c_1 - c_1. \tag{21}$$

Any element in the normalizer of $\mathfrak{H}$ must be in the normalizer of $\mathcal{C}$, therefore the number of groups conjugate to $\mathcal{C}$ is at most $g/p^n_1$, using equation (21) now leads to

$$g - m = o(\mathfrak{M} - \mathcal{C}) \leq \frac{g}{p^n_1} \left(p^c_1 - c_1\right) = (g - m) \frac{c_1}{n_1} \leq g - m. \tag{22}$$

Equation (22) shows that $c_1 = n_1$, and hence that $\mathcal{C} = \mathfrak{N}$. As $\mathfrak{H}$ is a characteristic subgroup of $\mathfrak{V}$, any element in the normalizer of $\mathfrak{V}$ is also in $\mathfrak{N}$. Therefore the normalizer of $\mathfrak{V}$ is contained in $\mathfrak{N} = \mathcal{C}$. As $\mathfrak{H}$ is in the center of $\mathcal{C}$, $\mathfrak{H}$ must be in the center of the normalizer of $\mathfrak{V}$. This implies, by a well-known theorem, that there is a normal subgroup of $\mathfrak{G}$ whose index is $p$. It is clear that such a subgroup will again satisfy the hypotheses of Theorem 8.1, and the argument can be repeated. After a finite number of such steps we shall arrive at a subgroup of order $m$; this must necessarily be $\mathfrak{M}$ and the theorem is established.

**Bibliography**


**Cornell University**

---

\^ See [7, p. 143].