THEOREMS ON SIMPLE GROUPS*

BY

H. F. BLICHFELDT

Introduction and Terminology.

§ 1. It is our purpose in this paper to state and prove a somewhat more precise theorem on simple groups than that given by Frobenius in his article Ueber auflösbare Gruppen. V.† This theorem of Frobenius we shall state in the following form: "Let H be a group whose order is divisible by $p^\lambda$, $p$ being a prime. If H is simple, then there is in H a substitution $T_1$ whose order is prime to $p$, which is commutative with some subgroup $Q$ of $H$ of order $p^n$ and not commutative with every subgroup of $Q$. In the contrary case, $H$ has an invariant subgroup of index $p^\lambda$, containing all the substitutions of $H$ whose orders are prime to $p$.”

The theorem which we shall here establish (divided for convenience into four parts, I, II, III, IV) defines the group $Q$ more explicitly, and the nature of the relation of $T_1$ to $Q$ in the most important case, namely, when $Q$ is a Sylow subgroup of $H$. Several applications are added in the form of corollaries.

The phraseology of ordinary group theory will be employed. The following abbreviations are used:

$A = B$ means “the groups (substitutions) $A$ and $B$ are identical”;
$A < B$ means “the group (substitution) $A$ is contained in the group $B$, though it is not identical with $B$.”

The letters $H$, $P$, $P_1$ and $T$ have the following significance throughout:
$H$ represents a group of order $p^\lambda n$, $p$ being a prime number not dividing $n$;
$P$ represents any given subgroup of $H$ of order $p^\lambda$;
$P_1$ represents any given subgroup of $P$ of order $p^{\lambda-1}$; and
$T$ is the general symbol for a substitution of $H$ whose order is prime to $p$.

Though it is contrary to general usage, we shall proceed from right to left in a succession of substitutions indicated. A function subjected to a substitution or a succession of such shall be written to the right of the substitutions indi-

---

*The present paper is an extension of two papers read before the San Francisco section, viz., A theorem concerning the Sylow subgroups of simple groups, September 29, 1906; and A theorem on simple groups, September 26, 1908.
†Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin, 1901, p. 1324.
H. F. BLICHFELDT:

Theorems and corollaries.

§ 2. Theorem I. Among the substitutions contained in $P$, but not in $P_1$, let $S$ be any one of those of lowest order. Then, if $H$ is simple, there are in $H$ a group $Q$ (either $= P$ or $< P$, containing $S$) and a substitution $T$, say $T_1$, of the following nature:

1°) If $Q = P$, this substitution $T_1$ is commutative with $P$ but not with $S$; more generally, the commutator $S^{-1}T_1^{-1}ST_1$ is not in $P_1$.

2°) If $Q < P$, then $T_1$ is commutative with $Q$, but not with every subgroup of $Q$ of index $p$.

Theorem II. If $Q < P$, there is a group $Q_1 = Q$ containing $S$, and there is a certain series of groups

$$Q_1, Q_2, Q_3, \ldots, Q_{\lambda-r+1} = P$$

of orders $p^r, p^{r+1}, p^{r+2}, \ldots, p^s$, respectively, each a subgroup of the one to the right of it, possessing the following property. Let $R_i$ be that group whose substitutions are common to all the subgroups of $Q_i$ of index $p$. Then, if $A_i$ be any substitution of $Q_i$ but not of $Q_{i-1}$, $i > 1$, the substitution

$$(SA_i)^pA_i^{-p},$$

though a substitution of $Q_{i-1}$, does not belong to $R_{i-1}$.

Corollary 1. Every substitution of $P$ commutative with $S$ must belong to $Q$. More generally, if $p > 2$, every substitution $A$ of $P$, such that the substitutions $A$ and $SAS^{-1}$ are commutative, must belong to $Q$. Hence, if $p > 2$, every abelian subgroup of $P$ which is transformed into itself by $S$, must belong to $Q$.

We prove this corollary from Theorem II by making use of the facts that $R_{i-1}$ is invariant in $Q_i$; that every commutator of $Q_{i-1}$ belongs to $R_{i-1}$; that the $p$th powers of the substitutions of $Q_{i-1}$ belong to $R_{i-1}$.

Theorem III.

a) If $Q_1 < P$, then the order $p^\lambda$ of $P$ is $\equiv p^{r+1}$, or is $\equiv p^{s^2}$, according as the order of $Q_1$ is $= p^{\lambda-1}$, or is $< p^{\lambda-1}$.

b) If the order of $P$ is $< p^{2p-1}$, then there is in $P$ some subgroup $P_1$ and substitution $S$ for which the corresponding group $Q = P$.

Corollary 2. The group $Q$ is certainly $= P$ in the cases where $P$

1°) is abelian \hspace{1cm} (Theorem II),

2°) or contains no substitutions of order $p^s$ \hspace{1cm} (Theorem II),

3°) or is of order $p^s$ at most \hspace{1cm} (Theorem III).
In any of these cases \( H \) will therefore contain a subgroup \( \mathcal{M} \) which contains \( P \) invariantly. Any one of the substitutions \( S \) of \( P \) (defined in Theorem I) is non-commutative with some substitution \( T \) of \( \mathcal{M} \).

In particular, if \( P \) fulfills both \( 1^o \) and \( 2^o \), then no one of its substitutions (except identity) is invariant in \( \mathcal{M} \).

Corollary 3. Let \( p \) be the lowest prime which divides the order of \( A \), and let it be given that the corresponding subgroup \( P \) is abelian.* Let a set of independent generating substitutions of \( P \) be constructed; then, if one of these generators be of order \( p^n \), there must be at least three generators of order \( p^n \) if \( p > 2 \); at least two if \( p = 2 \).

Hence, if \( p > 2 \), and if the order of \( P \) be \( \equiv p^8 \), then \( P \) must be of type \((1, 1, \ldots, 1)\) in every case, with the exception of the possibility \((2, 2, 2)\). Again, if \( p = 2 \), and the order of \( P \) be \( \equiv p^6 \), the only permissible types are the following: \((1, 1)\), \((1, 1, 1)\), \((1, 1, 1, 1)\), \((1, 1, 1, 1, 1)\), \((1, 1, 1, 1, 1, 1)\), \((2, 2)\), \((2, 2, 1, 1)\), \((2, 2, 2)\), \((3, 3)\).

To prove this corollary, let \( A_1, A_2, \ldots \) be the generators of order \( p^n \); \( B_1, B_2, \ldots \) the generators whose orders, \( p^{n_1}, p^{n_2}, \ldots \) are \( > p^n \). The group \( K \), generated by the substitutions \( B_1^{p^{n_1}-1}, B_2^{p^{n_2}-1}, \ldots, A_1^{p^{n_1}-1}, A_2^{p^{n_2}-1}, \ldots \), is a characteristic subgroup of \( P \).† Moreover, the group \( K' \), generated by \( B_1^{p^{n_1}-1}, B_2^{p^{n_2}-1}, \ldots \) (leaving out of \( K \) the generators \( A_1^{p^{n_1}-1}, \ldots \)), is a characteristic subgroup of \( P \). Let the factor-group \( K/K' \) be denoted by \( L \), and its generating substitutions by \( a_1, a_2, \ldots \), corresponding to \( A_1, A_2 \ldots \).

In applying Theorem I, \( 1^o \), let \( P_1 \) be that group generated by those generators of \( P \) whose orders are higher or lower than \( p^n \), and by \( A_1^{p^n}, A_2, \ldots \). Then we may put \( S = A_1 \), and we must have

\[
T_1^{-1} A_1 T_1 = A_1^x C, \quad x \equiv 1 \pmod{p},
\]

where \( C \) belongs to \( P_1 \).

Accordingly,

\[
T_1^{-1} A_1^{p^n} T_1 = (A_1^{p^n})^x C^{p^n}.
\]

Since \( T_1 \) is commutative with \( L \), we have correspondingly

\[
T_1^{-1} a_1 T_1 = a_1^x c,
\]

c belonging to that subgroup of \( L \) generated by \( a_2, \ldots \). Hence, if there were only two generators, \( a_1, a_2 \), in \( L \), then the order of \( T_1 \) would be a factor of \( p^n - 1 \). But this number is divisible by no prime \( > p \) except when \( p = 2 \).

*The more general case where \( P \) is not abelian, if it be only such that, for every \( P \) and \( S, Q = P \) (cf. Cor. 2), is embodied in this corollary when \( B_1, \ldots, A_1, \ldots \), instead of being the generators of \( P \), are the generators of the factor-group \( P/W \), \( W \) being the commutator subgroup of \( P \).

At the end of his paper on soluble groups, referred to in the introduction, Frobenius proves that every group of order \( p^kqr \) is soluble, if \( \lambda \leq 4 \); \( p, q, r \) being odd primes. Using his arguments in conjunction with Theorems I–III we find the

**Corollary 4.** Every group of order \( p^kqr \) is soluble, if \( \lambda \leq p^2 - 1 \); \( p, q, r \) being different odd primes.

**Theorem IV.** If the conditions as specified for a simple group \( H \) in Theorems I, II and III are not all fulfilled with reference to \( S \) and \( P \), then \( H \) has an invariant subgroup \( H_1 \) of index \( p \), which does not contain \( S \), but contains every substitution \( T \) of \( H \).

**Proof of the theorems.**

§ 3. Let \( P' \) be the largest subgroup of \( H \) whose substitutions are commutative with \( P \), and which, besides, transform \( S \) into itself or into \( S \times ( \text{a substitution of} \ P_1 ) \). This group \( P' \) is of order \( p^{n'} \), \( n' \) being a factor of \( n \). We shall prove that

A) The group \( P' \) contains an invariant subgroup \( P'_1 \) of order \( p^{\lambda - 1} \), to which \( S \) does not belong; further, no substitution of \( P \), not belonging to \( P' \), is of lower order than \( S \).

We write \( P' \) as a regular group in \( p^{n'} \) letters

\[ x_1, x_2, \ldots, x_{p^{n'}}. \]

The substitutions of \( P_1 \) will transform \( x_1 \) into \( p^{\lambda - 1} \) different letters, say

\[ x_1, x_2, \ldots, x_{p^{\lambda - 1}}. \]

The functions

\[ I_1 = x_1 + x_2 + \cdots + x_{p^{\lambda - 1}}, \quad S(I_1), \quad S^2(I_1), \quad \ldots, \quad S^{p-1}(I_1) \]

are all absolute invariants for the group \( P_1 \). Let \( \theta \) be a root different from 1, of the equation

\[ \theta^p - 1 = 0, \]

and let us consider the function

\[ I_2 = I_1 + \theta^{-1} S(I_1) + \theta^{-2} S^2(I_1) + \cdots + \theta^{-p+1} S^{p-1}(I_1). \]

It is not identically zero, no two of the functions (1) containing the same letter \( x_i \). It is an absolute invariant for the group \( P_1 \), and we have

\[ S(I_2) = \theta I_2. \]

We shall introduce the following abbreviations:

\( \zeta \) means a power of \( \theta \); and

*Loc. cit., p. 1329.*
\( \phi \) means a power of \( \theta \), different from 1.

Then if \( A \) is any substitution of \( P \),

\[
A(I_2) = \xi I_2, \quad S(I_2) = \phi I_2.
\]

§ 4. When the group \( P' \) is written symbolically in the form

\[
P' = P + B_2 P + B_3 P + \cdots + B_n P,
\]

the function

\[
I_3 = I_2 \cdot B_2(I_2) \cdot B_3(I_2) \cdots B_n(I_2)
\]

is seen to be a relative invariant for \( P' \). We find that

\[
S(I_3) = \theta^{n'} I_3 = \phi I_3.
\]

It follows that all the substitutions of \( P' \) for which \( I_3 \) is an absolute invariant form an invariant subgroup \( P'' \) of order \( p^{n'-1} \), not containing \( S \). This subgroup has a subgroup \( P_1' \) of order \( p^{n'-1} \), also invariant in \( P' \). The first part of (A), § 3, has thus been proved.

To prove the second part, we remark first that, as \( P \) is invariant in \( P' \), all the factors of \( I_3 \) are relative invariants for \( P \). Hence, if \( A \) be a substitution of \( P \) and not of \( P_1' \), the condition

\[
A(I_3) = \phi I_3
\]

necessitates that, for some factor \( B_i(I_2) \) of the right-hand member of (2), the relation shall subsist:

\[
AB_i(I_2) = \phi B_i(I_2).
\]

This gives

\[
B_i^{-1}AB_i(I_2) = \phi I_2.
\]

It follows that \( B_i^{-1}AB_i \), though a substitution of \( P \), does not belong to \( P_1' \). Hence its order is not lower than that of \( S \) (cf. Theorem I). Hence the order of \( A \) is not lower than that of \( S \).

§ 5. We shall now write \( H \) as a regular group in \( h = p^k \) letters, \( x_1, x_2, \ldots, x_h \). The substitutions of \( P'' \) will transform \( x_1 \) into \( p^{n'-1} \) letters, say \( x_1, x_2, \ldots, x_{p^{n'-1}} \). Let \( I = x_1 + x_2 + \cdots + x_{p^{n'-1}} \), and let us consider the function

\[
J = I + \theta^{-1} S(I) + \theta^{-2} S^2(I) + \cdots + \theta^{-p+1} S^{p-1}(I)
\]

which is not identically zero.

B) The group \( P' \) contains all the substitutions of \( H \) for which \( J \) is a relative invariant.

Let \( W \) transform \( x_a \) into \( x_a \), both occurring in \( J \). Since the letters involved in \( J \) form a transitive set for the group \( P' \), we can find a substitution in the latter, say \( V \), which also transforms \( x_a \) into \( x_a \). The substitution \( VW^{-1} \) will
therefore leave $x_\circ$ unchanged. Since $H$ is written in regular form, it follows that $W^{-1} W$ is identity. If $J$ be a relative invariant for $W$, and the order of $W$ be a power of $p$, then $W$ belongs to $P$.

§ 6. The substitutions of $H$ will transform $J$ into $n/n'$ expressions that do not differ by constant factors merely. The product $\pi$ of these factors will be a relative or absolute invariant for $H$. Evidently, $A(\pi) = \xi \pi$, $A$ being any substitution of $H$. If

$$S(\pi) = \phi \pi,$$

then $H$ contains an invariant subgroup $H_1$ of index $p$, consisting of all the substitutions $C$ for which

$$C(\pi) = \pi.$$

To this subgroup would belong every substitution $T$ of $H$. Accordingly, unless the group $H_1$ of Theorem IV exists, we must have

$$S(\pi) = \pi.$$  

§ 7. To examine the nature of the factors of $\pi$, let us write $H$ symbolically in the form

$$H = P' + PV_1 + PV_2 + \cdots + PV_{n-n'}.$$  

The group $P'$, operating upon $J$, will furnish just one of the factors of $\pi$, namely $J$. The $p$ substitutions represented by the symbol $PV_i$ will furnish, say, $p^{k_i}$ factors of $\pi$, whose product we shall indicate by $\pi_i$. Now, for $j \neq i$, one of the factors of $\pi_j$ may be equal, apart from a constant multiplier, to one of the factors of $\pi_i$. In such a case we find $\pi_j = \pi_i \times (a \text{ constant})$. We shall then agree to say that $\pi_j = 1$, if $j > i$. With this understanding we may write

$$\pi = J\pi_1\pi_2\cdots\pi_{n-n'}.$$  

Since $S(J) = \theta J$, $S(\pi_i) = \xi \pi_i$, it follows that, if (3) is to hold, there is at least one index $\rho$ such that

$$S(\pi_\rho) = \phi \pi_\rho.$$  

§ 8. First, let $\pi_\rho$ consist of a single factor. Then the alternative case $1^o$ of Theorem I is proved in the following manner. Let $V$ be one of the substitutions $PV_\rho$ of (4). Then we may suppose that

$$\pi_\rho = V(J).$$  

The function $\pi_\rho$ is here a relative invariant for $P$. Hence, $J$ is a relative invariant for $V^{-1}PV$. Hence, by $(B)$, § 5,

$$V^{-1}PV = P.$$
Now, since \( V \) does not belong to \( P' \), the group generated by \( V \) and \( P' \), though containing \( P \) invariantly, does not fulfill the other conditions imposed upon \( P' \) in § 3. Case 1\(*\) of Theorem I thus follows.

§ 9. Next, let \( \pi_p \) consist of more than one factor,

\[ \pi_p = y_1 y_2 \cdots y_{p^k}. \]

C) Then we shall prove that \( V \), one of the substitutions of the symbol \( PV_p \), transforms a certain subgroup \( Q_1 \) of \( P \), which contains \( S \) into itself or into another subgroup of \( P \). Moreover, \( V \) does not transform that subgroup of \( Q_1 \) which is also a subgroup of \( P'_1 \) into itself or into another subgroup of \( P'_1 \).

Substituting (6) in (5), it might happen that, for some index \( j \), we have \( S(y_j) \neq \xi y_j \). Then we may suppose that

\[ S(y_j) = y_{j+1}, \quad S(y_{j+1}) = y_{j+2}, \ldots, \quad S(y_{j+p'}) = \theta' y_j \quad (\theta'^p = 1). \]

Thus, if \( y_j = W(J) \), we get

\[ W^{-1}S^{p'}W(J) = \theta' J. \]

Hence (§ 5, B) \( W^{-1}S^{p'}W \leq P \).

This substitution, being of lower order than \( S \), must belong to \( P'_1 \) (§ 3, A). The function \( J \) is, however, an absolute invariant for \( P'' \) and therefore for \( P'_1 \) (cf. §§4, 5). Accordingly \( \theta' = 1 \).

§ 10. The \( p^k \) factors of \( \pi_p \) (6), permuted transitively by \( P \), fall into \( p \) sets of \( p^{k-1} \) factors each, forming imprimitive sets. Let the \( p \) products of the factors of these sets be indicated by

\[ a_1, a_2, \ldots, a_p; \quad a_1 a_2 \cdots a_p = \pi_p. \]

Substituting in (5), either we have

\[ S(a_i) = \xi a_i \quad (i = 1, 2, \ldots, p); \]

or we may put

\[ S(a_1) = a_2, \quad S(a_2) = a_3, \ldots, \quad S(a_p) = \varphi a_1. \]

The latter relations would, however, lead to an equation like (7), \( \theta' \neq 1 \), contrary to what was proved in § 9. Accordingly, (8) is true, and \( \xi = \varphi \) for some index \( i \), say \( i = 1 \):

\[ S(a_1) = \varphi a_1. \]

That subgroup of \( P \) for which \( a_1, a_2, \ldots, a_p \) are relative invariants shall be designated by \( Q_{\lambda-\nu} \), where \( \nu = \lambda - k \). Its order is \( p^{k-1} \).

The \( p^{k-1} \) factors of \( a_1 \) fall into \( p \) sets of imprimitivity for the group \( Q_{\lambda-\nu} \). The respective products shall be indicated by

\[ b_1, b_2, \ldots, b_2; \quad b_1 b_2 \cdots b_p = a_1. \]
We may assume that \( \mathcal{S}(b_i) = \phi b_i \). The factors \( b_1, b_2, \ldots, b_p \) are relative invariants for a group \( Q_{\lambda-v-1} < Q_{\lambda-v} \), of order \( p^{\lambda-2} \). Proceeding thus, we finally arrive at groups \( Q_3, Q_2, Q_1 \), of orders \( p^{v+2}, p^{v+1}, p^v \) respectively, having sets of relative invariants respectively designated by

\[
\begin{align*}
w_1, w_2, \ldots, w_p; & \quad v_1, v_2, \ldots, v_p; & \quad y_1, y_2, \ldots, y_p.
\end{align*}
\]

These invariants satisfy the relations

\[
w_1 = v_1 v_2 \cdots v_p; \quad v_1 = y_1 y_2 \cdots y_p.
\]

It will be noticed that \( \mathcal{S} \) belongs to all of these groups, and we have, corresponding to (9),

\[
\begin{align*}
\mathcal{S}(w_i) &= \phi w_i, \quad \mathcal{S}(v_i) = \phi v_i, \quad \mathcal{S}(y_i) = \phi y_i.
\end{align*}
\]

§ 11. Let \( y_1 = V(J) \), \( V \) being one of the \( p^v \) substitutions \( P V_p[(4), \S 7] \). Then \( J \) is a relative invariant for the group \( V^{-1} Q \), \( V \), which must therefore be a subgroup of \( P (\S 5) \). The first statement in (C), \S 9, is thus true.

Let \( A \) be a substitution of \( Q_2 \), but not of \( Q_1 \). Then we may suppose that

\[
y_i = A^{-i+1}(y_1) \quad (i = 2, \ldots, p);
\]

and we get

\[
\begin{align*}
\phi &= \frac{\mathcal{S}(v_i)}{v_1} = \frac{\mathcal{S}(y_1) \cdot \mathcal{S}(y_2) \cdots}{y_1 \cdot y_2 \cdots} = \frac{S \cdot ASA^{-1} \cdot A^2SA^{-2} \cdots \cdot A^{p-1}SA^{-p+1}(y_1)}{y_1} \\
&= \frac{(SA)^p A^{-p}(y_1)}{y_1} = \frac{V^{-1}(SA)^p A^{-p} V(J)}{J}.
\end{align*}
\]

Now \((SA)^p A^{-p} < Q_1\), and is also contained in every subgroup of \( P \) of order \( p^{\lambda-1} \). It is therefore contained in \( P_1' \). For this group \( J \) is an absolute invariant. Therefore, if the second part of (C), \S 9, were not true, then (10) could not be true.

§ 12. We shall now prove case 2° of Theorem I. Let \( Q^{(0)} \) be any subgroup of \( P \) such that \( Q^{(0)} \cong Q_1 \), and let

\[
Q^{(0)}, Q^{(1)}, Q^{(2)}, \ldots, Q^{(m)} = P
\]

be that series of groups in which each member is the largest subgroup of \( P \) containing the one immediately to the left of it invariantly. If \( H \) contains a substitution \( T \) which is commutative with one of these groups, say \( Q^{(m)}, m > 0 \), without being commutative with \( Q^{(m-1)} \), then 2° of Theorem I is true; the group \( Q \) in the theorem representing a certain group \( > Q^{(m-1)} \) and \( \cong Q^{(m)} \). We shall therefore assume that every substitution \( P \) which is commutative with \( Q^{(m)} \) of (11), or of any similar series, is commutative also with \( Q^{(m-1)}, m > 0 \). Under
this assumption the following theorem by Frobenius holds: If $K$ represents
the greatest subgroup of $H$ in which $Q^{(n)}$ is invariant $(n > k \geq 0)$, then $Q^{(k+1)}$
is a Sylow subgroup of $K$. *

D) By means of this theorem we can prove that, if $V$ be the substitution
considered in §§ 9, 11, we may write

$$V = W_1 W_2 W_3 \cdots W_r,$$

where $W_1, W_2, \ldots, W_r$ are substitutions of $H$, respectively commutative with
the following members of a certain series of groups:

$$L_1 = Q_1, \quad L_2, \quad L_3, \quad \ldots, \quad L_r = P,$$

each a subgroup of those that follow.

§ 13. To prove (D), let $VPV^{-1} = M$. Then $M$ and $P$ have in common
the group $Q_1$, but no greater group. Let $Q'_1$ be the greatest subgroup of $P$
containing $Q_1$ invariantly, and $Q'_1$ the corresponding subgroup of $M$. The
groups $Q'_1$ and $Q''_1$ will generate a group $N$ in which $Q'_1$ is a Sylow subgroup
by Frobenius’s theorem, §12. There is therefore in $N$ a substitution $W_1$ such
that $Q_{1,1} = W_1^{-1} Q''_1 W_1 \subseteq Q'_1$, $Q_{1,1} > Q_1$. We have also $W_1^{-1} Q_1 W_1 = Q_1$.
Let now $(W_1^{-1} V) P (W_1^{-1} V)^{-1} = M_1$. Then $P$ and $M_1$ have in common a
subgroup, say $L_2, \subseteq Q_{1,1}$, and therefore $L_2 > Q_1$. If $L_2 = P$, then (D) is
proved, the series (12) consisting of the two terms $Q_1, P$; in this case we find

$$V = W_1 W_2,$$

where $W_2$ is a certain substitution of $H$ commutative with $P$.

If $L_2 < P$, let $L'_2$ be the largest subgroup of $P$ containing $L_2$ invariantly,
$L''_2$ the corresponding subgroup of $M_1$. The groups $L'_2$ and $L''_2$ generate a
group in which $L'_2$ is a Sylow subgroup, etc. Proceeding as above, the proof
of (D) may be completed without difficulty.

§ 14. To complete the proof of case 2° of Theorem I, let us consider the sub-
stitutions $W_1, W_2, \ldots, W_r$, respectively commutative with the groups of (12). If they were at the same time commutative with the corresponding subgroups of
$P'$, i.e., if $W_i$, which is commutative with $L_i$, is also commutative with that
subgroup ($L'_i$) of $L_i$ which is a subgroup of $P'$, then (C), § 9, would not be
true. For, the group

$$V^{-1} L_1^0 V = W_1^{-1} \{ \cdots [ W_2^{-1} (W_1^{-1} L_1^0 W_1) W_2 ] \cdots \} W_r$$

* Paper referred to in § 1, p. 1325, Lemma I. The above theorem is apparently more general
than that given by Frobenius, account being taken of the underlying assumptions as stated in
both places. The method of proof by Frobenius is valid for the case considered here.
would then be a subgroup of $P'_i$. Accordingly, for some subscript $i$, there
is a substitution, $W_i$, commutative with $L_i$, but not with $L'_i$.

Now if $G$ be the largest subgroup of $H$ in which $L_i$ is invariant, then $L'_i$
is a Sylow subgroup of $G$ (§§ 12, 13). Evidently, $L'_i$ is invariant in $L'_i$. Since
$L'_i$ is not invariant in $G$ ( $W_i$ belongs to $G$), it follows that there is a substi-
tution $T$ in $G$ which is not commutative with $L'_i$. The group $L_i$ takes the
place of $Q$ in Theorem I, 2°).

§ 15. To prove Theorem II, let

$$Q_1, Q_2, \ldots, Q_{\lambda-\nu}, P$$

be the series of groups arrived at in § 10. Let $A_{\lambda-\nu+1}$ be a substitution belong-
ing to $P$, but not to $Q_{\lambda-\nu}$. Then we may suppose that

$$a_i = A_{\lambda-\nu+1}^{-i+1}(a_1) \quad (i = 2, 3, \ldots, p).$$

We obtain

$$\phi = \frac{S(\pi_{\rho})}{\pi_{\rho}} = \frac{1}{a_1} \left [ S \cdot A_{\lambda-\nu+1}^{-1} A_{\lambda-\nu+1}^{-2} \cdots (a_1) \right ]$$

$$= \frac{1}{a_1} \left ( S A_{\lambda-\nu+1}^{-1} A_{\lambda-\nu+1}^{-2} \cdots (a_1) \right ).$$

The function $a_1$, being a relative invariant for $Q_{\lambda-\nu}$, is plainly an absolute
invariant for the group $R_{\lambda-\nu}$, whose substitutions are common to all the sub-
groups of $Q_{\lambda-\nu}$ of order $p^{\lambda-2}$. It follows that $(SA_{\lambda-\nu+1})pA_{\lambda-\nu+1}^{-p}$ does not
belong to $R_{\lambda-\nu}$.

Starting now with a substitution $A_{\lambda-\nu}$ belonging to $Q_{\lambda-\nu}$ but not to $Q_{\lambda-\nu+1}$, we
may suppose

$$b_i = A_{\lambda-\nu+1}^{-i+1}(b_1) \quad (i = 2, 3, \ldots, p).$$

Substituting in $\phi = S(a_1)/a_1$, we find that $(SA_{\lambda-\nu})pA_{\lambda-\nu}^{-p}$ does not belong to $R_{\lambda-\nu-1}$, etc.

The group $Q_1$ is $\equiv Q$ of Theorem I, 2°), by §§ 12–14.

§ 16. We proceed to prove Theorem III. Considering the groups $Q_1, Q_2, \ldots, P$
of § 10, let $A$ designate a substitution belonging to $Q_2$, but not to $Q_1$. We
will assume that $A$ permutes the letters $y_1, y_2, \ldots, y_p$ in the order

$$A: \quad (y_1 y_2 \cdots y_p),$$

and that

$$S(y_i) = \theta^{a_i}(y_i) \quad (i = 1, 2, \ldots, p).$$

Then, since $S(v_1) = \phi v_1,$

$$\alpha_1 + \alpha_2 + \cdots + \alpha_p \equiv 0 \pmod{p}.$$

We shall say that the constants $\theta^{a_1}, \theta^{a_2}, \ldots, \theta^{a_p}$ are the multipliers of $S$.  

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
The substitution
\[ S' = S^{a_1} A^{-1} S^{a_2} A^{-2} S^{a_3} A^{-3} \cdots A^{-p+1} S^{a_p} A^{p-1}, \]
belonging to \( Q_1 \), will have the multipliers \( \theta, 1, 1, \ldots, 1 \), provided the congruences
\[
\begin{align*}
\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_p x_p & \equiv 1, \\
\alpha_2 x_1 + \alpha_3 x_2 + \cdots + \alpha_p x_p & \equiv 0, \\
& \quad \vdots \\
\alpha_p x_1 + \alpha_1 x_2 + \cdots + \alpha_{p-1} x_p & \equiv 0 \quad (\text{mod } p)
\end{align*}
\]
are satisfied. The necessary condition is that the determinant \( \Delta \) of the coefficients does not vanish (mod \( p \)). We find
\[ \Delta = (\alpha_1 + \theta \alpha_2 + \theta^2 \alpha_3 + \cdots)(\alpha_1 + \theta^2 \alpha_2 + \theta^4 \alpha_3 + \cdots) \cdots \\
\equiv \Delta^p \equiv (\alpha_1^p + \alpha_2^p + \alpha_3^p + \cdots)^p \equiv \alpha_1 + \alpha_2 + \alpha_3 + \cdots \equiv 0 \quad (\text{mod } p). \]
The substitutions \( S', A^{-1} S A, A^{-2} S A^2, \ldots \), all belonging to \( Q_1 \), are readily seen to generate a group of order \( p^p \) at least. The group \( Q_2 \) is accordingly of order \( p^{p+1} \) at least. Theorem III, \( \alpha \), is thus true when \( Q_2 = P \).

§17. Let \( Q_2 < P \). The functions \( v_1, v_2, \ldots, v_p \) (§10) contain \( p^2 \) factors \( y_1, y_2, \ldots \). We may assume that
\[ v_i = y_{(i-1)p+1} y_{(i-1)p+2} \cdots y_{ip} \quad (i = 1, 2, \ldots, p). \]
We shall say that the \( p \) factors of \( v_i \) constitute the set \( V_i \). The letter \( B \) shall designate a substitution belonging to \( Q_3 \) but not to \( Q_2 \). It permutes the letters \( v_1, v_2, \ldots, v_p \) in some such order as
\[ B: \quad (v_1 v_2 \cdots v_p). \]
Let \( R \) represent a substitution of the group \( Q_2 \). It has \( v_i \) for a relative invariant. We may assume that it permutes the members of the set \( V_i \) in the order \( y_{(i-1)p+1} y_{(i-1)p+2} \cdots y_{ip} \), or some power of this order,
\[ R: \quad (y_{(i-1)p+1} y_{(i-1)p+2} \cdots y_{ip})^n. \]
If \( n = p \), i. e., if the functions \( y_{(i-1)p+1}, \ldots \) are relative invariants for \( R \), we shall say that \( R \) is linear in \( V_i \). Otherwise we shall say that \( R \) is circular in \( V_i \). Thus, \( S \) is linear in \( V_1 \), and \( A \) is circular in \( V_1 \).

§18. Let us now suppose that \( R \) is linear in \( V_i \) and write
\[ R(y_{(i-1)p+j}) = \theta^{y_j} y_{(i-1)p+j} \quad (j = 1, 2, \ldots, p). \]
We shall say that $R$ is of rank $m$ in $V_i$ if $\beta_1 + \theta \beta_2 + \theta^2 \beta_3 + \cdots + \theta^{m-1} \beta_p$ is divisible by $(1 - \theta)^m$, but by no higher power of $1 - \theta$; $\beta_1, \beta_2, \ldots, \beta_p$ not being all equal (mod $p$). If $\beta_1 \equiv \beta_2 \equiv \cdots \equiv \beta_p \equiv 0$ (mod $p$), we shall say that $R$ is of rank $p - 1$; if $\beta_1 \equiv \beta_2 \equiv \cdots \equiv \beta_p \equiv 0$ (mod $p$), we shall say that $R$ is of rank $p$.

Let $A_i$ be any substitution contained in $Q_2$. Then $A_i R A_i^{-1} R^{-1}$ is linear in $V_i$. It is of rank $p$ if $A_i$ is linear in $V_i$; if $A_i$ is circular, the commutator in question is of rank $m + 1$ if $m < p$, and of rank $p$ if $m = p$.

§ 19. We can construct by the method of § 16, using $S$ and $B$, a substitution $S_1$, $< Q_2$, such that

$$S_1(v_1) = \theta v_1, \quad S_1(v_i) = v_i \quad (i = 2, 3, \ldots, p).$$

The following three cases may arise:

1. $S_1$ is linear in $V_1, V_2, \ldots, V_p$;
2. $S_1$ is circular in $V_1, V_2, \ldots, V_p$;
3. $S_1$ is partly linear and partly circular.

Consider case (1). The substitution $S_1$ is of rank 0 in $V_1$ and of rank $\geq 1$ in $V_2, V_3, \ldots, V_p$. The substitution $S_2 = A S_1 A^{-1} S_1^{-1}$ is of rank 1 in $V_1$ and of rank $\geq 2$ in $V_2, V_3, \ldots$. The substitution $S_3 = A S_2 A^{-1} S_2^{-1}$ is of rank 2 in $V_1$ and of rank $\geq 3$ in $V_2, V_3, \ldots$. Proceeding thus, we get a series of substitutions of which the last, $S_p = A S_{p-1} A^{-1} S_{p-1}^{-1}$, is of rank $p - 1$ in $V_1$ and of rank $p$ in $V_2, V_3, \ldots$.

The substitutions

$$S_p, \quad B S_p B^{-1}, \quad B^2 S_p B^{-2}, \ldots, \quad B^{p-1} S_p B^{-p+1}$$

will generate a group $Q'$ of order $p^p$ at least. This group does not contain $S_{p-1}$.

The substitutions

$$S_{p-1}, \quad B S_{p-1} B^{-1}, \quad B^2 S_{p-1} B^{-2}, \ldots, \quad B^{p-1} S_{p-1} B^{-p+1}$$

and the group $Q'$ will generate a group $Q''$ of order $p^{2p}$ at least, etc. Finally, we have a group $Q^{(p)}$, of order $\geq p^{2p}$, linear in $V_1, V_2, \ldots, V_p$, which group with $A$ and $B$ generate a group of order $\geq p^{3p+2}$.

§ 20. Consider case (2). Constructing the substitutions

$$R_1 = B S_1 B^{-1}, \quad R_2 = S_1 R_1 S_1^{-1} R_1^{-1},$$

we find that $R_2$ is linear in $V_1, V_2, \ldots, V_p$, of rank 1 in $V_1$ and $V_2$ and of rank $\geq 2$ in $V_3, V_4, \ldots, V_p$.

Now, $S$ is linear in $V_1$ (§ 17). It cannot be linear in all the sets
$V_2$, $V_3$, \ldots, or $S_i$ would be linear throughout. Hence there is a substitution, $W = BRSB^{-2}$, which is circular in $V_1$ and linear in $V_2$. Then the substitution $R_3 = WR_2W^{-1}R_2^{-1}$ is linear in all the sets $V_1$, $V_2$, \ldots. It is of rank 2 in $V_1$ and of rank 3 in the remaining sets. Proceeding as in §19, we construct a group $Q^{(p-2)}$ of order $\geq p^{(p-2)p}$, linear throughout, a subgroup in the group generated by $A$, $B$ and $R_3$. This group $Q^{(p-2)}$ and the substitutions $R_2$, $BR_2B^{-1}$, $B^2R_2B^{-2}$, \ldots generate a group $Q^{(p-1)}$ of order $\geq p^{p^2-p-1}$, linear throughout. This group and the substitutions $S_i$, $BS_iB^{-1}$, $B^2S_iB^{-2}$, \ldots generate a group $\cong Q_2$, of order $\geq p^{p^2-1}$. Accordingly, the order of $Q_3$ is $\geq p^{p^2}$.

The same processes, with slight variations, will dispose of case (3). Theorem III, $\alpha$, will be found true.

§ 21. In proving Theorem III, $\beta$, we may assume that $Q_2 = P$.

There is a substitution $S' < Q_2$, but not $< Q_1$, which can take the place of $S$ in Theorem I, $Q_i$ being substituted for $P_1$ in the theorem, and a corresponding group $Q$ taking the place of $Q_i$ in Theorems II and III, $\alpha$. If $P = Q$, Theorem III, $\beta$) is true. If $P > Q'$, then there exists a set of functions

$V'_1$: \quad $y'_1$, $y'_2$, \ldots, $y'_p$,

corresponding to the set $V$ defined in §17. These functions are permuted transitively by $P$; otherwise the order of this group would be $\geq p^{p^2}$ [Theorem III, $\alpha$]. We will look upon $P$ as transforming simultaneously the two sets $V_1$ and $V'_1$, making use of the results of §16.

We may evidently assume $S' = A$ of § 16. Then $A$ is linear and of rank 0 in $V'_1$, and is circular in $V_1$.

There must be a substitution $A'$ which is circular in $V'_1$. We can evidently find an integer $n$ such that the substitution $A'A^n$ is linear in $V_1$. Again, such numbers $m$ and $k$ can be found that the substitution

$$R = (A'A^n)^kS^m$$

is linear and of rank 0 in $V_1$ and is circular in $V'_1$.

The substitutions $A$ and $R$ will now generate a group of order $\geq p^{2p-1}$. To prove this, we construct first $R_1 = ARA^{-1}R^{-1}$, which is linear and of rank 1 in both $V_1$ and $V'_1$; then the substitutions

$$R_2 = ARA^{-1}R_1^{-1}, \quad R_3 = ARA^{-1}R_2^{-1}, \ldots,$$

which are all linear, of rank $p$ in $V'_1$, and of ranks 2, 3, \ldots, respectively, in $V_1$; finally, we construct the substitutions

$$W_2 = RRA_1R_1^{-1}, \quad W_3 = RWR_2R_1^{-1}W_2^{-1}, \quad W_4 = RWR_3R_1^{-1}W_3^{-1}, \ldots,$$

all linear, of rank $p$ in $V_1$, and of ranks 2, 3, 4, \ldots, respectively, in $V'_1$.  

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
The substitutions $R_1, R_2, R_3, \ldots; W_2, W_3, \ldots$ will generate a group of order $\geq p^{2p-3}$, linear in $V_i$ and $V'_i$. Again this group together with $A$ and $R$ will generate a group of order $\geq p^{2p-1}$.

§ 22. Theorem IV is proved as follows. The invariant subgroup $H_1$ exists unless the condition $S(\tau) = \tau$ is satisfied (cf. § 6). But Theorems I, II and III were true in consequence of this condition.