ON TRANSITIVE SIMPLE GROUPS OF DEGREE $3p^m$

To Richard Brauer on his sixtieth birthday

NOBORU ITO

Let $\Omega$ be the set of symbols $1, 2, \ldots, 3p$, where $p$ is an prime number greater than 3. Let $\mathfrak{G}$ be a transitive permutation group on $\Omega$, which is simple and in which the normalizer of a Sylow $p$-subgroup has order $2p$. Our purpose is to prove the following two theorems:

**Theorem 1.** If $\mathfrak{G}$ is primitive on $\Omega$, then $p = 5$ and $\mathfrak{G}$ is isomorphic to the alternating group $A_6$ of degree 6.

**Theorem 2.** If $\mathfrak{G}$ is imprimitive on $\Omega$, then $\mathfrak{G}$ is isomorphic to the linear fractional group $LF(2, 2^m)$ with $2^m + 1 = p$.

Our proof of Theorem 1 is fairly complicated. Theorem 1 implies that such a group $\mathfrak{G}$ cannot be doubly transitive. This fact will be proved in § 2. There the irreducible characters of dimension two of the symmetric group on $\Omega$ play an essential role as in our previous papers [14], [15]. We need also, however, recent result of Thompson [18] concerning groups of odd order. In § 3 we treat, roughly speaking, the almost doubly transitive case. There a result of Wielandt concerning the eigenvalues of intertwining matrices is very useful [21]. With the help of this theorem of Wielandt, some results of Brauer and Suzuki [4], [17] concerning groups whose Sylow 2-subgroups are dihedral groups of order either 4 or 8 respectively can be used. In § 4 we consider, roughly speaking, the strongly simply transitive case. For this case we need again some deep results.

Theorem II is a simple consequence of our previous result [14].

Finally, we want to emphasize that we need from beginning to end Brauer's $p$-block theory of irreducible characters.

Received September 5, 1961.

* This work was supported by the United States Army under Contract No. DA-ARO(D)-31-124-G 86 monitored by the Army Research Office.

1. Since \( \mathcal{G} \) is simple, the normalizer of a Sylow \( p \)-subgroup of \( \mathcal{G} \) is a dihedral group of order \( 2p \) by the splitting theorem of Burnside. Hence the principal \( p \)-block \( B_1(p) \) of irreducible characters of \( \mathcal{G} \) consists of two non-exceptional characters, the principal character \( \Delta \) and the other character \( X \), whose degree is congruent to \( \pm 1 \) modulo \( p \), and a family of \( \frac{1}{2}(p-1) \) \( p \)-conjugate exceptional characters \( C_i \) \( (i = 1, \ldots, \frac{1}{2}(p-1)) \). The equation

\[
\Delta(X) + \varepsilon X(X) - \varepsilon C_i(X) = 0
\]

holds for every \( p \)-regular element \( X \) of \( \mathcal{G} \) and for every \( i = 1, \ldots, \frac{1}{2}(p-1) \), where \( \varepsilon = \pm 1 \) according as the degree of \( X \) is congruent to \( \pm 1 \) modulo \( p \). Let \( P \) be an element of order \( p \). Then we have

\[
X(P) = \varepsilon
\]

and

\[
\frac{1}{2}(p-1) \sum_{i=1}^c C_i(P) = -\varepsilon.
\]

All the other irreducible characters \( D_j \) \( (j = 1, 2, \ldots) \) of \( \mathcal{G} \) belong to \( p \)-blocks of defect 0([3], §1).

We consider \( \mathcal{G} \) as usual as a linear group consisting of permutation matrices. Let \( \alpha \) be the character of \( \mathcal{G} \) in this sense. Then for every element \( X \) of \( \mathcal{G} \) \( \alpha(X) \) denotes the number of symbols of \( \Omega \) fixed by \( X \). Since \( \mathcal{G} \) is transitive on \( \Omega \), the decomposition of \( \alpha \) into its irreducible components is as follows:

\[
\alpha(X) = \Delta(X) + \varepsilon X(X) + c \sum C_i(X) + Y(X),
\]

where \( x \) and \( c \) are non-negative integers and \( Y \) is a linear combination of \( D_j \)'s with non-negative integers. All the \( C_i \)'s have the same coefficient \( c \), because they are algebraically conjugate to one another \( (i = 1, \ldots, \frac{1}{2}(p-1)) \).

2. Now we want to show that

\[
\varepsilon = -1, x = 1 \text{ and } c = 0 \text{ in (4).}
\]

In order to show this, let us assume at first that \( p > 5 \). Put \( X = P \) in (4). Then from (2), (3) and (4) we have
because $Y$ vanishes at $P$ by a theorem of Brauer-Nesbitt ([8], Theorem 1).
Put $X=1$ in (4). Then from (1) and (6) we have

(7) \[ 3p = 1 + xX(1) + (x+\varepsilon) \frac{1}{2} (p-1)(X(1)+\varepsilon) + Y(1). \]

Now assume that $\varepsilon = 1$. Then since $\mathcal{G}$ is simple and hence $X(1) \geq p+1$, we obtain from (7)

\[ 3p \geq 1 + \frac{1}{2} (p-1)(p+2), \]

which implies the contradiction $p \leq 5$. Hence $\varepsilon = -1$. Next assume that $x \geq 2$. Then since $\mathcal{G}$ is simple and hence $X(1) \geq p-1$, we obtain from (7)

\[ 3p \geq 1 + 2(p-1) + \frac{1}{2} (p-1)(p-2), \]

which implies the contradiction $p \leq 5$. Hence $x = 1$ and $c = 0$ by (6).

Now let us assume that $p = 5$. Though it is a little troublesome to handle with this case from the beginning, all the primitive groups of degree $l_5$ are known. There are 6 types of such groups. Among them only the group, which is isomorphic to $3\hat{16}$, appears here. Therefore it is easy to check the validity of (5) in this case.

Put $X = B$. Then (1), (2), (3) and (4) can be rewritten as follows:

(1.1) \[ A(X) + C_i(X) = B(X) \left( i = 1, 2, \ldots, \frac{1}{2} (p-1) \right). \]

(2.1) \[ B(P) = -1. \]

(3.1) \[ \sum_{i=1}^{\frac{1}{2}(p-1)} C_i(P) = 1. \]

(4.1) \[ \alpha(X) = A(X) + B(X) + Y(X). \]

3. Let $J$ be an involution in the normalizer of the Sylow $p$-subgroup $\langle P \rangle$ of $\mathcal{G}$. Let $g$ and $z$ denote the orders of $\mathcal{G}$ and the centralizer of $J$. Then applying the method of Brauer-Fowler ([7], (23)) we have

(8) \[ p = \frac{g}{z^2} \sum \frac{Z(J)^2 Z(P)}{Z(1)}, \]
where \( Z \) ranges over all the irreducible characters of \( \mathfrak{G} \). Since all the characters of defect 0 for \( p \) vanish at \( P \) by a theorem of Brauer-Nesbitt ([8], Theorem 1), (8) can be written as follows:

\[
\hat{p} = \frac{2^i}{g} \sum_{Z \in \mathfrak{h}} \frac{Z(J)^3 Z(P)}{Z(1)}.
\]

Let \( v p - 1 \) be the degree of \( B \). Then the following equation can be obtained from (9) using (1.1), (2.1) and (3.1):

\[
(v p - 1)(v p - 2)p^2 = g(v p - 1 - B(J))^2.
\]

There is just one class of conjugate involutions in \( \mathfrak{G} \). In fact let \( K \) be an involution which is not conjugate to \( J \). Then the method of Brauer-Fowler yields us \( B(K) = v p - 1 \), which contradicts the simplicity of \( \mathfrak{G} \).

Now since the centralizer of \( J \) contains a Sylow 2-subgroup of \( \mathfrak{G} \), the equation (10) tells us something about the order of a Sylow 2-subgroup of \( \mathfrak{G} \).

According to the degree of \( B \) we distinguish three cases, each of which is handled separately, since we see from (4.1) that \( v \) equals either 3 or 2 or 1.

\( \S \) 2. The case in which the degree of \( B \) is \( 3p - 1 \).

4. Let us assume that the degree of \( B \) equals \( 3p - 1 \). Then the equations (4.1) and (10) take the following forms:

\[
\alpha(X) = A(X) + B(X).
\]

\[
(3p - 1)(3p - 2)p^2 = g(3p - 1 - B(J))^2.
\]

The equation (4.2) tells us in particular that \( \mathfrak{G} \) is doubly transitive on \( \Omega \).

By a theorem of Brauer ([3], Lemma 3) we have

\[ B(J) = -2 \text{ or } 0 \text{ or } 2. \]

Since \( \alpha(J) \geq 0 \) the case \( B(J) = -2 \) does not occur by (4.2). Now assume that \( B(J) = 2. \) Then by (4.2) we have

\[
\alpha(J) = 3,
\]

and (10.1) can be read as follows:

\[
(3p - 1)(3p - 2)p^2 = 9(9 - 1)^2 g.
\]

Since \( \mathfrak{G} \) is doubly transitive, \( \mathfrak{G} \) contains an involution \( J \) with the cycle
structure (12) . . . . Let $\mathfrak{A}$ denote the subgroup of $\mathfrak{S}$ consisting of all the permutations of $\mathfrak{S}$ each of which fixes each of the symbols 1 and 2. Then $I$ is contained in the normalizer of $\mathfrak{A}$. Hence there exists a Sylow 2-subgroup $\mathfrak{H}$ of $\mathfrak{A}$, whose normalizer contains $I$. $\mathfrak{S} = \langle I \rangle$ is a Sylow 2-subgroup of $\mathfrak{S}$. In fact otherwise we must have $3p \equiv 1 \pmod{4}$. Then the equality (10.2) shows that $g$ must be odd, which is a contradiction. Since $I$ and $J$ are conjugate with each other, $I$ fixes by (11) just three symbols different from 1 and 2, say 3, 4 and 5 of $\mathfrak{O}$. Let $X$ be an element of $\mathfrak{A}$, which is commutative with $I$. Then since $a(X) \leq 3$ and is odd, $X$ must fix just one symbol, for instance 5, of the symbols 3, 4 and 5, and the cycle structure of $X$ is of the form (34)(5) . . . . Since every involution fixes just three symbols of $\mathfrak{O}$, $X$ must be an involution. Let $Y \neq X, Y$ be an element of $\mathfrak{A}$, which is commutative with $I$. Then $Y$ must fix, like $X$, just one symbol of 3, 4 and 5. If it is 3, $Y$ has the cycle structure (3)(45) . . . . Then $XY$ belongs to $\mathfrak{A}$ and has the cycle structure (354) . . . , which is a contradiction. The same holds for 4, too. Hence $Y$ must fix 5, and has the cycle structure (34)(5) . . . . Then $XY$ belongs to $\mathfrak{A}$ and fixes the symbols 1, 2, 3, 4 and 5. This implies that $XY = 1$, and since $X$ is an involution, $X = Y$, which contradicts our assumption on $Y$. Therefore the centralizer of $I$ in $\mathfrak{S}$ has order 4. Thus by a theorem of Suzuki ([18], Lemma 4) $\mathfrak{S}$ contains an element $L$ such that $\mathfrak{S} = \langle I, L \rangle$ and $ILI = L^{-1}2^{a-1}e$, where $2^a$ is the order of $\mathfrak{S}$ and $e$ equals either 1 or 0. Let $f$ be the exact exponent of 2 dividing $\frac{p}{2}$ - 1. Then we obtain from (10.2) the following equality:

$$a = 2f - 1.$$  

The simplicity of $\mathfrak{S}$ implies that $a$ is greater than 1. This implies by (12) that the order of $L$ is greater than 2. Now it is easy to see that the cycle structure of $L$ is of the form either $L = (1)(2)(i)R$ or $L = (12)(i)R$, where $i \neq 1, 2$ is a symbol of $\mathfrak{O}$ and $R$ consists of cycles of order $2^{a-1}$. In any case this shows that $\frac{p}{2} - 1$ is divisible by $2^{a-1}$, that is, $f \geq a - 1$. Hence we obtain from (12) that $a = 3$ and $\mathfrak{S}$ is a dihedral group of order 8.

Let us consider the principal 2-block $B_1(2)$ of irreducible characters of $\mathfrak{S}$. By a theorem of Brauer-Tuan ([10], Corollary of Lemma 3) $B_1(2)$ contains at least either B or all of the $\mathfrak{G}$'s $(i = 1, \ldots, \frac{1}{2}(p - 1))$, because there is no element of order $2p$ from our assumptions. Assume that $B_1(2)$ does not contain
any $C_i$. Then by a theorem of Brauer-Tuan ([10], Lemma 3) we have the congruence

\[(13) \sum Z(1)Z(P) \equiv 0 \pmod{2^m},\]

where $Z$ ranges over all the irreducible characters of $\mathfrak{G}$ belonging simultaneously to $B_2(\ell)$ and $B_1(2)$. But the left hand side of (13) equals $1 + (3p-1)(-1) = -(3p-2)$, which is a contradiction. Hence $B_2(2)$ contains all the $C_i$'s. On the other hand $B_1(2)$ consists of five characters ([5], [17] and for a detailed presentation see [13]). Thus we have obtained the inequality $\frac{1}{2} (p + 1) \leq 5$, which implies that $p = 5$. Now again we have only to check six primitive groups of degree 15 and we see that there is no group with required properties. Therefore we must have that $B(J) = 0$ and by (4.2) that

\[(14) \alpha(J) = 1.\]

Furthermore (10.1) becomes the following form:

\[(10.3) (3p-2)px^2 = (3p-1)g.\]

(10.3) tells us in particular that the order of a Sylow 2-subgroup of $\mathfrak{G}$ equals the power of 2 dividing $3p-1$. Hence $B$ is a character of defect 0 for 2. In particular by a theorem of Brauer-Nesbitt ([8], Theorem 1) we have

\[(15) \alpha(X) = 1\]

for every 2-singular element $X$ of $\mathfrak{G}$.

5. Let $\mathfrak{S}$ denote the symmetric group on $\mathfrak{O}$. Let $X_1$ and $X_\ldots$ be irreducible characters of $\mathfrak{S}$ corresponding to the diagrams

\[\bullet \cdots \bullet \quad \text{and} \quad \bullet \cdots \bullet .\]

By a theorem of Frobenius (12) we have the formulae

\[(16) X_1(X) = \left(\alpha(X) - 1\right) - \beta(X)\]

and

\[(17) X_\ldots(X) = \frac{\alpha(X)(\alpha(X) - 3)}{2} + \beta(X),\]

where $X$ is an element of $\mathfrak{S}$ and $\beta(X)$ denotes the number of transpositions.
in the cycle structure of $X$.

Now since $\mathcal{G}$ is doubly transitive, we have ((11), p. 164)

\begin{equation}
\sum_{\lambda \in \mathcal{G}} \alpha(X) = g, \quad \sum_{\lambda \in \mathcal{G}} \alpha(X)^2 = 2g \quad \text{and} \quad \sum_{\lambda \in \mathcal{G}} \beta(X) = \frac{1}{2} g.
\end{equation}

Using (18) we obtain from (16) and (17)

\[ \sum_{\lambda \in \mathcal{G}} X_\lambda(X) = \sum_{\lambda \in \mathcal{G}} X_{\mathcal{G}}(X) = 0. \]

Hence by the reciprocity theorem of Frobenius $\Lambda$ does not appear as an irreducible component of $X_\lambda$ and $X_{\mathcal{G}}$ restricted to $\mathcal{G}$. Let

\begin{equation}
X_\lambda = bB + c \sum C_i + \sum a_j D_j
\end{equation}

and

\begin{equation}
X_{\mathcal{G}} = b'B + c' \sum C_i + \sum b_j D_j
\end{equation}

be the decompositions of $X_\lambda$ and $X_{\mathcal{G}}$ into irreducible characters of $\mathcal{G}$.

We want to show that

\begin{equation}
b = b' = c' = c - 1 \leq 1.
\end{equation}

To this end, we first compare the values of both sides of (19) and (20) at $P$. Then using (2.1), (3.1) and a theorem of Brauer-Nesbitt ([8], Theorem 1) we obtain from (16) and (17) the equalities $1 = -b + c$ and $0 = -b' + c'$.

Next let us observe the generalized character $(X_\lambda - X_{\mathcal{G}})B$. Then we have

\[
\sum_{\lambda \in \mathcal{G}} (X_\lambda(X) - X_{\mathcal{G}}(X))B(X) = \sum_{\lambda \in \mathcal{G}} (1 - 2\beta(X)) (\alpha(X) - 1) \quad \text{(by (4.2), (16), (17))}
\]

\[
= \sum_{\lambda \in \mathcal{G}} (-1 + \alpha(X) - 2\beta(X)) = 0 \quad \text{(by (15)).}
\]

This implies $b = b'$.

Let us assume that $b > 1$. Then we have that $b \geq 2$ and $c \geq 3$. Comparing the degrees of the characters on both sides of (19) we have that

\[
\frac{1}{2} (3p - 1)(3p - 2) \geq 2(3p - 1) + 3 \cdot \frac{1}{2} (p - 1)(3p - 2),
\]

which implies the contradiction $0 \geq p$. Therefore we must have that $1 \leq b$. 
Now we distinguish two subcases $b = 0$ and $b = 1$, though they can be treated rather similarly. In any case, we can use, roughly speaking, the same routine as in the previous paper [15].

6. At first we handle the subcase $b = 0$. Then the equations (19) and (20) are read as follows:

\[(19.1) \quad X_i = \sum C_i + \sum a_j D_j\]

and

\[(20.1) \quad X.. = \sum b_j D_j.\]

Since $B$ is orthogonal to $X_i + X..$ in this case, using (18) we obtain

\[(22) \quad \sum \alpha_i X_i = \gamma.\]

In particular $\mathfrak{G}$ is triply transitive on $\Omega$ [21].

Using (15), (18) and (22) we can calculate the norm of $X_i$ and $X..$ from (16), (17) and (19.1), (20.1) as follows:

\[(23) \quad \sum \frac{1}{2} (\alpha(X) - 1)(\alpha(X) - 2) - \beta(X)^2 \]
\[= \sum \frac{1}{4} \alpha(X)^4 + \sum \beta(X)^2 - 3 \]
\[= \frac{1}{2} (\rho - 1) + \sum a_j^2.\]

\[(24) \quad \sum \frac{1}{2} \alpha(X) (\alpha(X) - 3) + \beta(X) \]
\[= \sum \frac{1}{4} \alpha(X)^4 + \sum \beta(X)^2 - 4 \]
\[= \sum b_j.\]

Eliminating the expression $\sum \frac{1}{4} \alpha(X)^4 + \sum \beta(X)^2$ from (23) and (24) we have

\[(25) \quad \sum b_j = \frac{1}{2} (\rho - 3) + \sum a_j.\]

7. Let $e$ be the principal character of $\mathfrak{K}$ and $e^*$ be the character of $\mathfrak{G}$ induced by $e$. Since $\mathfrak{G}$ is doubly transitive, by a theorem of Frobenius [12] we have the following equation

\[e^* = A + 2B + X_i + X..\]
Substituting (19.1) and (20.1) into this equation, we have

\begin{equation}
(26) \quad e^* = A + 2B + \sum C_i + \sum (a_j + b_j)D_j.
\end{equation}

Let \( \Omega_2 \) denote the set of vectors \((x, y)\), where \( x \neq y \) and \( x, y \) belong to \( \Omega \). The basis of our proof rests on the following theorem ([22], 28.4, 29.2): the norm of \( e^* \) equals the number of domains of transitivity of \( \mathcal{R} \) on \( \Omega_2 \).

By (26) the norm of \( e^* \) equals

\[ 1 + 4 + \frac{1}{2} (p - 1) + \sum (a_j + b_j)^2. \]

Put \( T = \Omega - \{1, 2\} \). \( T_2 \) is the set of vectors \((x, y)\), where \( x \neq y \), and \( x, y \in T \). The vectors \((1, 2)\) and \((2, 1)\) themselves constitute domains of transitivity of \( \mathcal{R} \) and furthermore the vectors of forms \((i, T)\) and \((T, i)\) \((i = 1, 2)\) each constitute domains of transitivity of \( \mathcal{R} \). Therefore we see that the vectors of \( T_2 \) are divided into

\[ \frac{1}{2} (p - 3) + \sum (a_j + b_j)^2 \]

domains of transitivity of \( \mathcal{R} \). By (25) this number will be transformed into

\begin{equation}
(27) \quad p - 3 + 2 \sum a_j^2 + 2 \sum a_j b_j.
\end{equation}

Since \( \mathcal{G} \) is triply transitive on \( \Omega \) and hence \( \mathcal{R} \) is transitive on \( T \), every domain of transitivity of \( \mathcal{R} \) from \( T_2 \) contains a vector of the form \((3, x)\) with \( x (\neq 3) \in T \).

8. Let \( \mathcal{Q} \) denote the subgroup of \( \mathcal{G} \) consisting of all the permutations of \( \mathcal{G} \) each of which fixes each of the symbols 1, 2, 3. At first assume that \( \mathcal{Q} \) fixes no symbol from \( \Omega \) other than 1, 2 and 3. Then since the order of \( \mathcal{Q} \) is by (15) odd, every domain of transitivity of \( \mathcal{R} \) from \( T_2 \) contains at least three different vectors of the form \((3, x)\) with \( x \in T \). Then we see at once that there exist at most \( p - 1 \) domains of transitivity of \( \mathcal{R} \) from \( T_2 \). Then from (27) we have the following inequality

\begin{equation}
(28) \quad 1 \geq \sum a_j^2 + \sum a_j b_j.
\end{equation}

If all the \( a_j \)'s are zero, comparing the values at the identity element of both sides of (19.1) we have the contradiction.
\[
\frac{1}{2} (3p - 1)(3p - 2) = \frac{1}{2} (p - 1)(3p - 2).
\]

Hence (28) turns out to be an equality. This means that there exist just \( p - 1 \) domains of transitivity of \( \mathcal{R} \) from \( T_2 \) and every domain of transitivity of \( \mathcal{Z} \) from \( T - \{3\} \) has length 3. The latter fact implies that \( \mathcal{Z} \) is an elementary abelian 3-group. It is easy to check that the normalizer of \( \mathcal{Z} \) in \( \mathcal{R} \) coincides with \( \mathcal{Z} \). Therefore by the splitting theorem of Burnside \( \mathcal{R} \) contains the normal 3-complement \( \mathfrak{M} \) of order \( 3p - 2 \). Every element \( \neq 1 \) of \( \mathfrak{M} \) fixes just two symbols of \( \mathfrak{O} \), 1 and 2. Now let \( I \) be an involution of \( \mathfrak{O} \) with the cycle structure \( (2) (3) \ldots \). Then \( I \) normalizes \( \mathcal{R} \) and therefore \( \mathfrak{M} \). By (15) \( I \) fixes only the symbol 3 from \( \mathfrak{O} \). Hence \( I \) centralizes only the identity element of \( \mathfrak{M} \). Therefore \( \mathfrak{M} \) must be abelian. Under this circumstances we want to show that the order of \( \mathfrak{O} \) is smaller than \( 3p - 2 \).

Let \( \mathcal{Q} \) be a Sylow \( q \)-subgroup of \( \mathfrak{M} \) and let \( \mathfrak{Q}_Q \) be the centralizer of \( \mathcal{Q} \) in \( \mathfrak{M} \). Then the factor group \( \mathfrak{M}/\mathfrak{Q}_Q \) is isomorphic to an automorphism group of \( \mathcal{Q} \). Let \( q \) vary over all the prime divisors of \( 3p - 2 \). Then obviously \( \mathfrak{M} \) is isomorphic to a subgroup of the direct product of all the \( \mathfrak{M}/\mathfrak{Q}_Q \)'s. Therefore we have only to show that for every prime divisor \( q \) of \( 3p - 2 \) the order of \( \mathfrak{M}/\mathfrak{Q}_Q \) is smaller than that of \( \mathfrak{Q} \). Then the ordinary Frattini argument allows us to assume that \( \mathcal{Q} \) is elementary abelian (of order \( q^n \)). So we can assume that \( \mathfrak{M} \) is a subgroup of the general linear group \( GL(u, q) \). Moreover we can assume that \( \mathfrak{M} \) is irreducible in the prime field of characteristic \( q \). This implies that \( \mathfrak{O} \) is cyclic (of order 3). There remains nothing to prove.

Let \( l \) be the order of \( \mathfrak{O} \). Then there holds

\[
g = 3p(3p - 1)(3p - 2)l.
\]

Substituting this value of \( g \) into (10.3) we have

\[
z^2 = 3(3p - 1)^2l.
\]

Hence we can put

(29) \[
3l = m^2.
\]

On the other hand by the theorem of Sylow (for \( p \)) we have that \( m^2 \equiv 1 \pmod{p} \), which implies \( m \equiv \pm 1 \pmod{p} \). Since \( m \) is odd \( > 1 \) by (29), we obtain that \( m \geq 2p - 1 \). So we have the following inequality
ON TRANSITIVE SIMPLE GROUPS OF DEGREE 3

\[(2p - 1)^3 < 3(3p - 2),\]

which implies the contradiction \(p \leq 2\).

9. Therefore \(\mathcal{Q}\) must fix at least one symbol from \(\Omega\), say 4 different from 1, 2 and 3. Now we can assume, without loss of generality, that \(\mathcal{Q}\) fixes just \(i\) symbols, 1, 2, \ldots, \(i\) (\(i \geq 4\)) of \(\Omega\). Let \(N\mathcal{Q}\Omega\) denote the normalizer of \(\mathcal{Q}\) in \(\mathfrak{G}\). Put \(\Phi = \{1, 2, \ldots, i\}\). Then the factor group \(N\mathcal{Q}/\Omega\) is a triply transitive permutation group on \(\Phi\) ([22], 9.4). Clearly every permutation \(\neq 1\) of \(N\mathcal{Q}/\Omega\) fixes at most two symbols of \(\Phi\). Hence the order of \(N\mathcal{Q}/\Omega\) equals \(i(i - 1)(i - 2)\). The degree \(i\) must be odd by (15). Therefore using a theorem of Zassenhaus [24] we obtain that \(N\mathcal{Q}/\Omega\) is isomorphic to \(LF(2, 2^m)\) with \(2^m + 1 = i\).

In these circumstances let us assume at first that \(\mathcal{Q}\) has at least one domain of transitivity from \(T\) whose length is greater than 3. Now we can show that

\[(30)\]

\[i < \sqrt{p}.\]

To this end let \(\mathcal{V}\) be a domain of transitivity of \(\mathcal{Q}\) from \(T\) with length \(f > 3\). Let \(\mathcal{V}/\Omega\) be a Sylow 2-subgroup of \(N\mathcal{Q}/\Omega\). Then for any involution \(X\) of \(\mathcal{V}/\Omega\) have \(\mathcal{V} \cap \mathcal{V}^X = \emptyset\). In fact \(\mathcal{V}^x\) is again a domain of transitivity of \(\mathcal{Q}\) from \(T\). If \(\mathcal{V} \cap \mathcal{V}^x \neq \emptyset\), then we have \(\mathcal{V} = \mathcal{V}^x\). But this means that \(X\) fixes at least one symbol in \(\mathcal{V}\), because the length of \(\mathcal{V}\) is odd. This contradicts (15). Let \(\mathcal{V}^\ast\) be the set of all the different \(\mathcal{V}^X\) with any element \(X\) from \(N\mathcal{Q}\). Then we can consider \(N\mathcal{Q}/\Omega\) as a transitive permutation group on \(\mathcal{V}^\ast\). Let \(\mathcal{V}/\Omega\) be the subgroup of \(N\mathcal{Q}/\Omega\) consisting of all the elements of \(N\mathcal{Q}/\Omega\) each of which fixes \(\mathcal{V}\). Then the order of \(\mathcal{V}/\Omega\) is, as is shown above, odd. Then we see from a property of \(LF(2, 2^m)\) that \(\mathcal{V}/\Omega\) is cyclic of order at most \(2^m + 1\). Therefore \(\mathcal{V}^\ast\) contains at least \(f2^m(2^m - 1)\) symbols of \(T\). Thus we have obtained the following inequality

\[2^m + 1 + 5.2^m(2^m - 1) \leq 2^m + 1 + f2^m(2^m - 1) \leq 3p.\]

Let assume that \(i \geq \sqrt{p}\). Then we obtain from above the following inequality:

\[\sqrt{p} + 5(\sqrt{p} - 1)(\sqrt{p} - 2) \leq 3p,\]

which implies that

\[p + 5 \leq 7\sqrt{p}.\]
So we obtain that $p \leq 37$. Since $p \equiv -1 \pmod{4}$ by (15) we have only the following possibilities $p = 7; 11; 19; 31$. Furthermore $3p - 1$ must be divisible by 32, because $n$ is odd and bigger than 3. The last fact follows from the fact that any Sylow 3-subgroup of $\mathcal{Q}$ has index 3 in a Sylow 3-subgroup of $\mathcal{G}$. Then we see that only the case $p = 11$ is possible. But if $p = 11$, we must have that $\mathcal{Q} = 1$, which contradicts our assumption on $\mathcal{Q}$.

Let $j$ be the number of domains of transitivity of $\mathcal{Q}$ with length 3 from $T$. Then by a theorem of Bochert [1] we have that

$$i + 3j \leq 2p.$$  

Now there exist at most

$$i + j + \frac{3p - i - 3j}{5}$$

domains of transitivity of $\mathcal{R}$ from $T$. Here we notice that the number in (27) is not smaller than $p - 1$, because it is shown to be impossible in 8 that all the $a_j$'s are zero. Then we have the following inequality

$$4i + 2j + 5 \geq 2p,$$

which implies

$$10i + 2(i + 3j) + 15 \geq 6p.$$  

So by (30) and (31) we obtain the following inequality

$$10\sqrt{p} + 15 \geq 2p,$$

which implies that $p \leq 37$. This has already been shown above to be impossible.

Thus we can assume that all the domains of transitivity of $\mathcal{Q}$ from $T - \emptyset$ have length 3. Then we want to show that we are essentially in the same situation as in 8. At any rate $\mathcal{Q}$ is an elementary abelian 3-group. Let $I$ be an involution with the cycle structure (12) . . . . Let $g$ be a prime divisor of $3p - 2$ and $\mathcal{O}$ be a Sylow $q$-subgroup of $\mathcal{R}$ such that the normalizer of $\mathcal{O}$ contains $I$. Then we see as in 8 that $\mathcal{O}$ is abelian. Hence $\mathcal{R}$ is an $A$-group of odd order. Therefore by a theorem of Thompson [18] $\mathcal{R}$ is soluble. Let $\mathcal{M}$ be a Sylow 3-complement of $\mathcal{R}$ such that the normalizer of $\mathcal{M}$ contains $I$. Then we see again that $\mathcal{M}$ is abelian. Let $\mathcal{M}$ be the largest normal subgroup of $\mathcal{R}$ contained in $\mathcal{N}$. We want to see that $\mathcal{M} = \mathcal{M}$. Assume that $\mathcal{N} \neq \mathcal{M}$. Then let
us consider the centralizer of $\mathcal{M}$ in $\mathfrak{S}$. Since $\mathcal{M}$ is abelian, this has the form $\mathcal{M}Q'$ with $Q' \leq \mathfrak{S}$. If $Q' \neq 1$, then $Q'$ becomes a normal $3$-subgroup $\neq 1$ of $\mathfrak{S}$. This is a contradiction. So we have that $\mathfrak{S} = \mathcal{M}$. The rest is just the same as in 8. Therefore the subcase $b = 0$ cannot occur.

10. Next we consider the subcase $b = 1$. In this case the equations (19) and (20) take the following forms:

\[(19.2) \quad \mathbf{x}_i = \mathbf{b} + 2 \sum c_i + \sum a_j d_j\]

and

\[(20.2) \quad \mathbf{x}_.. = \mathbf{b} + \sum c_i + \sum b_j d_j.\]

Corresponding to (22), (23), (24) and (25) we have now

\[(22.1) \quad \sum_{x \in \mathfrak{S}} \alpha(x)^2 = 7g.\]

\[(23.1) \quad \sum_{x \in \mathfrak{S}} \left( \frac{1}{2} \alpha(x)(\alpha(x) - 1)(\alpha(x) - 2) - \beta(x) \right)^2 = \sum_{x \in \mathfrak{S}} \frac{1}{4} \alpha(x)^4 + \sum_{x \in \mathfrak{S}} \beta(x)^2 - 6 = 1 + 4 \cdot \frac{1}{2} (p - 1) + \sum a_j.\]

\[(24.1) \quad \sum_{x \in \mathfrak{S}} \left( \frac{1}{2} \alpha(x)(\alpha(x) - 3) + \beta(x) \right)^2 = \sum_{x \in \mathfrak{S}} \frac{1}{4} \alpha(x)^4 + \sum_{x \in \mathfrak{S}} \beta(x)^2 - 7 = 1 + \frac{1}{2} (p - 1) + \sum b_j.\]

\[(25.1) \quad \sum b_j = \frac{1}{2} (3p - 5) + \sum a_j.\]

Furthermore corresponding to (26) we have now

\[(26.1) \quad e^* = \mathbf{a} + 4 \mathbf{b} + 3 \sum c_i + \sum (a_j + b_j) d_j.\]

Hence the norm of $e^*$ equals

\[1 + 16 + 9 \cdot \frac{1}{2} (p - 1) + \sum (a_j + b_j)^2.\]

Let $\mathcal{H}$ denote the subgroup of $\mathfrak{S}$ consisting of all the permutations of $\mathfrak{S}$ each of which fixes the symbol $1$, and let $h$ be the order of $\mathcal{H}$. Let us consider
the norm of $\mathcal{B}$ restricted to $\mathfrak{H}$ and put
\[\sum_{X \in \mathfrak{H}} \mathcal{B}(X)^2 = \sum_{X \in \mathfrak{H}} (\alpha(X) - 1)^2 = ah.\]

The same equality holds for any conjugate subgroup of $\mathfrak{H}$ in $\mathfrak{G}$. Adding up (32) over all the conjugate subgroups of $\mathfrak{H}$ in $\mathfrak{G}$, we have
\[\sum_{X \in \mathfrak{G}} \alpha(X)(\alpha(X) - 1)^2 = ag.\]

By (18) and (22.1) we see that the left hand side of (33) equals $4g$. Thus we have proved that $a = 4$. Therefore by ([22], 28.4, 29.2) $\mathfrak{Q} - \{1, 2\}$ is divided into three domains of transitivity of $\mathfrak{R}$, say $T(i)$ $(i = 1, 2, 3)$. Let $t_i$ be the length of $T(i)$. Then we have
\[t_1 + t_2 + t_3 = 3p - 2.\]

By $T(i)_2$ is meant the set of vectors $(x, y)$, with $x \neq y$, $x, y \in T(i)$. Now the vectors $(1, 2)$ and $(2, 1)$ themselves constitute domains of transitivity of $\mathfrak{R}$ and furthermore the vectors of $(i, T(j))$ and $(T(j), i)$ $(i = 1, 2; j = 1, 2, 3)$ each constitute domains of transitivity of $\mathfrak{R}$ from $\mathfrak{Q}_2$. Therefore we see that the vectors of $T(i)_2$ and $(T(i), T(j))$ $(i, j = 1, 2, 3; i \neq j)$ are divided into
\[\frac{1}{2} \cdot 3(3p - 1) + \sum (a_j + b_j)^2\]
domains of transitivity of $\mathfrak{R}$ from $\mathfrak{Q}_2$. By (25.1) this number will be transformed into
\[6p - 4 + 2\sum a_j + 2\sum a_j b_j.\]

Let $n_k$ be a symbol of $T(k)$ and $\mathfrak{Q}_k$ be the subgroup of $\mathfrak{R}$ consisting of all the permutations of $\mathfrak{R}$ each of which fixes the symbol $n_k$ $(k = 1, 2, 3)$. Let $i_k$ and $j_k$ denote the numbers of domains of transitivity of $\mathfrak{Q}_k$ from $T(1) + T(2) + T(3)$ having lengths 1 and 3, respectively $(k = 1, 2, 3)$. Let us assume at first that for every $k = 1, 2, 3$, $\mathfrak{Q}_k$ has a domain of transitivity of length greater than 3 from $\mathfrak{Q}$. Then since $\mathfrak{Q}$ is doubly transitive, we have, by a theorem of Bochert [2], the following inequalities:
\[2p + \frac{2\sqrt{3}p}{3} \geq 2 + i_k + 3j_k \quad (k = 1, 2, 3)\]
Every domain of transitivity of $\mathfrak{R}$ from $T(1)_2$, $(T(1), T(2))$ and $(T(1), T(3))$
contains a vector of the form \((n_1, *)\). Hence there exist at most

\[(36) \quad i_1 - 1 + j_1 + \frac{3p - 2 - i_1 - 3j_1}{5}\]

domains of transitivity from \(T(1)_2\), \((T(1), T(2))\) and \((T(1), T(3))\). The same holds also for \(T(2)_2\), \((T(2), T(1))\), \((T(2), T(3))\) and \(T(3)_2\), \((T(3), T(1))\), \((T(3), T(2))\). Adding up three numbers of type \(36\) we see that there exist at most

\[(37) \quad \frac{9p - 21}{5} + \frac{4}{5}(i_1 + i_2 + i_3) + \frac{2}{5}(j_1 + j_2 + j_3)\]

domains of transitivity of \(S_e\) from \(T(k)_2\) and \((T(k), T(1))\) \((k, 1 = 1, 2, 3; k \neq 1)\).

Let \(J\) be an involution whose cycle structure has the form \((12) \ldots\). By \(14\) \(J\) fixes just one symbol, say \(\alpha_j\), of \(\Omega\). Without loss of generality we can assume that \(\alpha_j\) belongs to \(T(3)\) and \(\alpha_j = \alpha_3\). Since \(J\) belongs to the normalizer of \(K\), \(J\) transfers \(T(1)\) into one of \(T(i)\)'s. \((i = 1, 2, 3)\). If it is \(T(1)\), then since \(J\) does not fix any symbol of \(T\), the length of \(T(1)\) must be even, which is a contradiction. Moreover since \(J\) fixes the symbol \(\alpha_3\), \(J\) fixes \(T(3)\). Hence \(J\) interchanges \(T(1)\) with \(T(2)\). In particular we see that \(L_t\) and \(L_s\) are conjugate in the normalizer of \(K\) and that \(i_1 = i_2, j_1 = j_2\) and \(t_1 = t_2\).

Let \(\Phi_3\) be the set of all the symbols of \(T(1) + T(2) + T(3)\), each of which is fixed by all the permutations of \(\mathfrak{G}_3\).

In the first place, let us assume that \(\Phi_3\) is contained in \(T(3)\). We consider the normalizer \(Ns\mathfrak{G}_3\) of \(\mathfrak{G}_3\) in \(\mathfrak{G}\). Then by a theorem of Witt \([22], 9.4\) \(Ns\mathfrak{G}_3/\mathfrak{G}_3\) is doubly transitive on \(\Phi_3 \cup \{1, 2\}\). Furthermore since \(\mathfrak{G}\) is transitive on \(T(3)\), we see by a theorem of Jordan \([22], 3.6\) that \(Ns\mathfrak{G}_3 \cap \mathfrak{G}\) is transitive on \(\Phi_3\). Hence \(Ns\mathfrak{G}_3/\mathfrak{G}_3\) is triply transitive on \(\Phi_3 \cup \{1, 2\}\) and has the order \((i_3 + 2)(i_3 + 1)i_3\). Since \(i_3\) is odd, we obtain by a theorem of Zassenhaus \([24]\) that \(Ns\mathfrak{G}_3/\mathfrak{G}_3 \simeq LF(2, 2^m)\), where \(2^m = i_3 + 1\).

Now if \(i_3 \geq \sqrt{p}\), then we obtain as in \(9\), that \(p \leq 37\). Hence again by \(14\) we have only the following possibilities \(p = 7; 11; 19; 23; 31\). Here \(3p - 2\) cannot be a prime number. In fact, otherwise, since the degree of \(C_i\) equals \(3p - 2\), the order of \(\mathfrak{G}\) must be divisible by \(3p - 2\) by a well known theorem and this implies the triple transitivity of \(\mathfrak{G}\) contradicting our assumption \(b = 1\). So it remains only the following two possibilities \(p = 19; 31\). Furthermore if \(\mathfrak{G}_3\) has the domain of transitivity of length \(>5\), the same method as in \(9\) assures us that \(p < 19\). Hence we can assume that \(\mathfrak{G}_3\) does not possess any domain of
transitivity of length $> 5$. The order of $\Omega_3$ is therefore of the form $3^a 5^b$. If $p = 31$, then since the order of $\mathfrak{R}$ is, as is noticed above, divisible by 91, we have that $t_3 \equiv 0 \pmod{91}$. This contradicts (34), because $t_1 = t_2 \geq 1$. So we must have that $p = 19$. Let $k_3$ denote the number of domains of transitivity of $\Omega_3$ with length 5. Then we have the following equality: $2 + t_5 + 3 j_3 + 5 k_3 = 57$. The same method as in 9 shows us that $k_3 \geq t_5 (t_5 + 1)$. Hence we have that $t_5 + 5 t_5 (t_5 + 1) \leq 55$, whence follows that $t_5 \leq 3$. This contradicts our assumption that $t_5 \geq 19 > 4$.

Therefore we can assume that $t_5 < \sqrt{p}$. Then using this inequality we have from (27.1), (35) and (37) that

$$\frac{9p - 21}{5} + \frac{4}{5} \sqrt{p} + \frac{4}{5} \left(4p + \frac{4\sqrt{3}p}{3} - \frac{2}{5} \left(\frac{2p}{3} + \frac{2\sqrt{3}p}{9} - 2\right)\right) \geq 6p - 4.$$  

Then we have easily that $p < 19$. This is, as is already shown above, a contradiction.

Next let us assume that $\Phi_2$ is not contained in $\mathcal{T}_2$. Then without loss of generality we can assume that $\Phi_2$ contains a symbol of $T(1)$ and namely $\alpha_1$. Then $\Omega_3$ is contained in $\Omega_1$. Since we can choose the symbol $\alpha_2$ in such a way that the cycle structure of $J$ has the form $J = (12)(\alpha_2)(\alpha_1 \alpha_2) \ldots$, we can assume that $\Omega_3$ is also contained in $\Omega_2$. In particular we have that $t_2 \equiv 0 \pmod{t_1(= t_5)}$. In this case $\Phi_1$, $\Phi_3$ the sets of all the symbols of $T(1) + T(2) + T(3)$, each of which is fixed by all the permutations of $\Omega_1(\Omega_2)$, must be contained in $T(1) + T(2)$. Otherwise, for instance, if $\Phi_1$ is not contained in $T(1) + T(2)$, we obtain that $\Omega_1 \subseteq \Omega_3$ and $t_1 = t_2 = t_3$. The latter fact contradicts (34). In particular we have that $t_1 > t_3$. If $t_5 : t_3 > 3$, then we have from (34) that $t_1 < \frac{3p}{7} - \frac{2}{7}$. Now using the fact $\Phi_1 \cup \Phi_2 \subseteq T(1) + T(2)$ we obtain from (27.1), (35) and (37) the following inequality

$$\frac{9p - 21}{5} + \frac{4}{5} \left(\frac{12}{7} p - \frac{8}{7}\right) + \frac{4}{5} \left(2p + \frac{2\sqrt{3}p}{3} - \frac{2}{5} \left(\frac{2p}{3} + \frac{2\sqrt{3}p}{9} - 2\right)\right) \geq 6p - 4.$$  

This implies a contradiction that $p < 5$. Hence we must have that $t_3 = 3 t_5$. Then we have from (34) that $t_1 = \frac{3}{5} p - \frac{2}{5}$. Finally using again $\Phi_1 \cup \Phi_2 \leq T(1) + T(2)$ we obtain from (27.1), (35) and (37) the following inequality

$$\frac{9p - 21}{5} + \frac{4}{5} \left(\frac{12}{5} p - \frac{8}{5}\right) + \frac{4}{5} \left(2p + \frac{2\sqrt{3}p}{3} - \frac{2}{5} \left(\frac{2p}{3} + \frac{2\sqrt{3}p}{9} - 2\right)\right) \geq 6p - 4.$$
This implies a contradiction that $p < 7$.

Hence we can assume that at least one of $\mathbb{L}_k (k = 1, 2, 3)$, say $\mathbb{L}_1$, has only domains of transitivity with length either 1 or 3 from $\Omega$. Then $\mathbb{L}_1$ must be an elementary abelian 3-group. On the other hand, $\mathbb{S}$ possesses an irreducible character of degree $3p - 2$, for instance, $\mathbb{C}_1$. Therefore by a famous theorem $g$ and hence the order of $\mathbb{S}$ must be divisible by $3p - 2$. Hence finally $\mathbb{S}_1$ must be divisible by $3p - 2$. By (34) this is a contradiction.

Therefore the case in which the degree of $B$ is $3p - 1$ cannot occur.

§ 3. The case in which the degree of $B$ is $2p - 1$.

11. Now let us assume that the degree of $B$ equals $2p - 1$. Then the equations (4.1) and (10) read as follows:

\[(4.3) \quad \alpha(X) = \Lambda(X) + B(X) + D_1(X),\]

where $X$ is any element of $\mathbb{S}$ and the degree of $D_1$ equals $p$;

\[(10.4) \quad 2(p - 1)(2p - 1)x^2 = g(2p - 1 - B(J))^2.\]

By a theorem of Brauer ([3], Lemma 3) we have

$B(J) = 1$ or $-1$.

If $B(J) = -1$, then from (10.4) we obtain the following equality

\[(p - 1)(2p - 1)x^2 = 2pg,\]

which shows that $x$ is divisible by $p$. This is a contradiction. Hence we must have

\[(38) \quad B(J) = 1,\]

and (10.4) takes the following form:

\[(10.5) \quad p(2p - 1)x^2 = 2(p - 1)g.\]

(10.5) tells us in particular that the order of a Sylow 2-subgroup of $\mathbb{S}$ equals the power of 2 dividing $2(p - 1)$, say $2^{a+1}$. Therefore every character $\mathbb{C}_i$ becomes by (1.1) a character of 2-defect 0 \(\left\{ i = 1, \ldots, \frac{1}{2} (p - 1) \right\}$. 

We consider the representation $\mathbb{D}_1$ corresponding to $D_1$ and the matrix $\mathbb{D}_1(J)$ corresponding to $J$. Let us assume that $\mathbb{D}_1(J)$ possesses the eigenvalues 1 and $-1$ in the multiplicities $m$ and $n$ respectively. Then we have that
On the other hand, again by a theorem of Brauer ([3], Lemma 3) we have
\[(40)\quad D_1(J) = m - n = \epsilon,\]
where \(\epsilon\) is either 1 or \(-1\). From (39) and (40) we obtain that
\[(41)\quad n = \frac{1}{2} (p - \epsilon).\]

Now since \(\mathfrak{G}\) is simple, the determinant of \(\mathfrak{D}_1(J)\), \((-1)^n\), must be the unity, and hence \(n\) must be even. Here it may be convenient to distinguish two subcases, (I) \(p \equiv 1 \pmod{4}\) and (II) \(p \equiv -1 \pmod{4}\), though the second subcase will be eliminated rather promptly later. Then in the subcase (I) (41) and (40) imply that \(\epsilon = 1\) and \(D_1(J) = 1\). Hence by (38) and (4.3) we have that
\[(42)\quad \alpha(J) = 3.\]
In the subcase (II) (41) and (40) imply that \(\epsilon = -1\) and \(D_1(J) = -1\). Hence by (38) and (4.3) we have that
\[(43)\quad \alpha(J) = 1.\]

12. Now we are in a position to apply a method of Wielandt [21]. By (4.3), \(\mathfrak{G} - \{1\}\) is divided into two domains of transitivity of \(\mathfrak{G}\), say \(T(i)\) \((i = 1, 2)\) ([22], 28.4, 29.2). Let \(t_i\) be the length of \(T(i)\) and assume that \(t_1 \leq t_2\). Then we have
\[(44)\quad t_1 + t_2 = 3p - 1\]
and
\[(45)\quad t_1 \leq \frac{1}{2} (3p - 1) \leq t_2.\]

We define matrices \(V(T(i))\) as follows: put \(V(T(i)) = (v_{k,l})\). Then \(v_{k,l} = 1\), if there exist an element \(X\) of \(\mathfrak{G}\) and a symbol \(n\) of \(T(i)\) such that \(X(1) = 1\) and \(X(n) = k\) hold, and \(v_{k,l} = 0\) otherwise. \(V(T(i))\) is commutative with every matrix of \(G\), which is as usual considered as a linear group consisting of permutation matrices. By the definition of \(V(T(i))\) we have
\[(46)\quad E + V(T(1)) + V(T(2)) = W = \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ \vdots & \vdots & \ddots \\ 1 & \cdots & 1 \end{pmatrix}.\]
where $E$ is the unit matrix of degree $3p$. Let us bring $G$ into the completely reduced form. Then by the lemma of Schur $V(T(i))$ and $W$ become diagonal matrices. Without loss of generality we can assume that the diagonal form of $V(T(i))$ is

$$
\begin{bmatrix}
  z(i, 1) \\
  z(i, 2) \\
  \vdots \\
  z(i, 2) \\
  z(i, 3) \\
  \vdots \\
  2p-1 \\
  z(i, 3)
\end{bmatrix}
$$

Now as in [21] we obtain the following:

\begin{enumerate}
  \item[(i)] $z(i, j)$ is a rational integer ($i = 1, 2; j = 1, 2, 3$), and $z(i, 1) = t_i$, $z(i, 2) = t_i$, and $z(i, 3) = t_i$ ($i = 1, 2$).
  \item[(ii)] $z(i, 1) + p z(i, 2) + (2p - 1) z(i, 3) = 0$.
  \item[(iii)] $z(i, 1)^2 + p z(i, 2)^2 + (2p - 1) z(i, 3)^2 = 3p t_i$.
\end{enumerate}

Furthermore since $W$ possesses the eigenvalues $3p$ and 0 in the multiplicities 1 and $3p - 1$ respectively, by (46) we have the following equalities:

\begin{equation}
(48) \quad z(1, i) + z(2, i) = -1 \quad (i = 2, 3).
\end{equation}

From (i) and (ii) we derive at once that

\begin{equation}
(49) \quad z(i, 3) \equiv t_i \mod p.
\end{equation}

Moreover we obtain from (iii) that

$$z(i, 3)^2 \leq \frac{3pt_i}{2p - 1} < p^2.$$

In fact assume that

$$t_i = \frac{(2p - 1)p}{3}$$

But we have that $\frac{p(2p - 1)}{3} \geq 3p$ for $p \geq 5$, which contradicts (44).

Hence we have that
From (47) (i), (49), (50) and (45) we have that
\[-p < t_1 - z(1, 3) < \frac{1}{2} (5p - 1) < 3p\]
and
\[\frac{1}{2} (p - 1) < t_2 - z(2, 3) < 4p.\]
Therefore we have
\[(51) \quad t_1 - z(1, 3) = \text{either } p \text{ or } 2p,\]
and
\[(52) \quad t_2 - z(2, 3) = \text{either } p \text{ or } 2p \text{ or } 3p.\]

Among different combinations of (51) and (52) only the following two cases are possible by (48): Case (A) \( t_1 - z(1, 3) = p \) and \( t_2 - z(2, 3) = 2p \); Case (B) \( t_1 - z(1, 3) = 2p \) and \( t_2 - z(2, 3) = p \).

At first let us consider Case (A). Then we have from (47) (ii) the following equalities:
\[(53) \quad z(1, 2) = 2p - 1 - 2t_1 \text{ and } z(2, 2) = 2(2p - 1) - 2t_2.\]
Substituting (51), (52) and (53) into (47) (iii) we obtain
\[(54) \quad 6t_1^2 - 3(8p - 3)t_1 + (2p - 1)(3p - 1) = 0\]
and
\[(55) \quad 6t_2^2 - 3(8p - 3)t_2 + 4(2p - 1)(3p - 1) = 0.\]
Similarly in Case (B) we have the following equations:
\[(56) \quad 6t_1^2 - 3(8p - 3)t_1 + 4(2p - 1)(3p - 1) = 0\]
and
\[(57) \quad 6t_2^2 - 3(4p - 1)t_2 + (2p - 1)(3p - 1) = 0.\]
Now we can show that Case (B) cannot occur. To this end let us consider the quadratic form \(Q(T)\) in \(T\), which is the left hand side of (57). \(Q(T)\) takes its minimum value at \(\frac{1}{4} (4p - 1)\). By (45) we have that \(Q(t_2)\)
\[ Q\left(\frac{1}{2}(3p - 1)\right) \] is a simple calculation shows that \( Q\left(\frac{1}{2}(3p - 1)\right) > 0 \). This contradicts (57).

The equation (55) tells us that \( t_1 \) is divisible by 8. Since \( t_1 \) is the length of a domain of transitivity of \( \mathbb{G} \), \( t_1 \) is a divisor of the order of \( \mathbb{G} \), and hence of \( g \). Therefore \( g \) must be divisible by 8.

Now let us assume that the subcase (II) in 11 does occur. Then we have from (43) that \( \frac{1}{2}(3p - 1) \) must be even, because \( \mathbb{G} \) is simple and contains no odd permutation. This implies, however, by (10.5) that \( g \) cannot be divisible by 8. This is a contradiction.

Now by (42) we see that \( 3p - 1 \equiv 0 \pmod{4} \). Hence the equations (54) and (55) tells us that the exact powers of 2 dividing \( t_1 \) and \( t_2 \) are 2 and 8 respectively.

13. Let \( \mathbb{T} \) be a Sylow 2-subgroup of \( \mathbb{G} \), which is contained in \( \mathbb{G} \). Since \( \frac{1}{2}t_1 \) is odd, \( T(1) \) contains a domain of transitivity \( T_{\mathbb{G}} \) of \( \mathbb{G} \) with length 2. Without loss of generality we can put \( T_{\mathbb{G}} = \{2, 3\} \). Let \( \mathbb{X}_1 \) denote the subgroup of \( \mathbb{G} \) consisting of all the permutations of \( \mathbb{G} \) each of which fixes each of the symbols 2 and 3. Then \( \mathbb{X}_1 \) has index 2 with respect to \( \mathbb{G} \). Let us consider \( \mathbb{X}_1 \) as a permutation group on \( T(2) \). Then by (42) \( \mathbb{X}_1 \) must be semi-regular on \( T(2) \). In particular we have that \( t_2 \equiv 0 \pmod{2^a} \). This implies, together with the fact remarked at the end of 12, that \( 8 \equiv 0 \pmod{2^a} \). Therefore the order of \( \mathbb{T} \) equals either 8 or 16.

Now we want to show that \( \mathbb{T} \) contains a cyclic normal subgroup of index 2. At any rate \( \mathbb{T} \) contains an element \( X \) with the cycle structure \( (1)(23) \ldots \). Assume that there exists such an element \( X \) with order greater than 2, say \( 2^b \) \((b \geq 2)\). Let \( (1)(23)Y \) be the cycle structure of \( X \). Then by (42) \( Y \) consists of cycles of order \( 2^b \). Since \( \mathbb{T} \) contains no odd permutation, the number \( 3(p - 1)/2^b \) must be odd. This implies that \( b = a \). So we can assume that every element \( X \) with the cycle structure \( (1)(23) \ldots \) is an involution. At any rate we have the decomposition \( \mathbb{T} = \mathbb{X}_1 < X > \) with \( \mathbb{X}_1 \cap <X> = 1 \). By (42) \( X \) fixes just two symbols of \( \mathbb{T} \), which are different from 1, 2 and 3, say 4 and 5. Let us consider the centralizer \( Z_{\mathbb{T}}X \) of \( X \) in \( \mathbb{T} \). Then since by (42) every element \( Y \neq 1 \) of \( \mathbb{X}_1 \) fixes no symbol of \( \mathbb{T} \), which is different from 1, 2 and 3, we see that the order of \( Z_{\mathbb{T}}X \) equals four. Hence by a theorem of Suzuki
Moreover an ordinary transfer argument (see for example [19]) assures us that \( \mathcal{G} \) cannot be abelian. Therefore if \( \mathcal{G} \) is of order 8, we see, using a theorem of Brauer-Suzuki [9], that \( \mathcal{G} \) is a dihedral group.

Our next aim is to show that the order of \( \mathcal{G} \) cannot be 16. Let us assume that the order of \( \mathcal{G} \) is 16. Let us consider \( \mathcal{G} \) on \( T(2) \). Then \( \mathcal{G} \) cannot be semi-regular on \( T(2) \). In fact, otherwise, we have the congruence \( t_2 \equiv 0 \pmod{16} \), which implies the contradiction \( 8 \equiv 0 \pmod{16} \). Hence there exists a symbol of \( T(2) \), say 4, and an element \( B \neq 1 \) of \( \mathcal{G} \) such that \( B \) fixes 4. Let \( \mathcal{T}_2 \) denote the subgroup of \( \mathcal{G} \) consisting of all the permutations of \( \mathcal{G} \) each of which fixes the symbol 4. Then since \( t_2 \) is even, \( \mathcal{T}_2 \) fixes at least, and by (42) just, one more symbol of \( T(2) \), say 5. Moreover by (42) we have \( \mathcal{T}_1 \cap \mathcal{T}_2 = 1 \), which implies that the order of \( \mathcal{T}_2 \) equals 2. Hence \( B \) generates \( \mathcal{T}_2 \). \( B \) has the cycle structure \((1)(23)(4)(5) \ldots \). Let \( A \) be an element of \( \mathcal{G} \) of order 8. Then the cycle structure of \( A \) must have the form \((1)(23)A^4\), where \( A^4 \) consists of cycles of order 8. In fact, otherwise, it must have the form \((1)(2)(3)A^4\), which contradicts the simplicity of \( \mathcal{G} \), because \( (p-1)/8 \) is odd. Let us assume that \( \mathcal{G} \) is not a dihedral group. Then by a theorem of Suzuki ([16], Lemma 4) we have that \( BAB = A^3 \). Then \( \mathcal{G} \) contains just two classes of involutions, namely the class of \( A^4 \) and that of \( B \). Let \( z_1 \) and \( z_2 \) denote the orders of centralizers of \( A^4 \) and \( B \) in \( \mathcal{G} \) respectively. Let \( g(2) \) and \( h(2) \) denote the numbers of involutions in \( \mathcal{G} \) and in \( \mathcal{G} \) respectively. Then by (42) we have the following equality

\[
g/z = g(2) = ph(2) = p(h/z_1 + h/z_2),
\]

which implies the equality

\[(58) \quad 3/z = 1/z_1 + 1/z_2.
\]

If the centralizer \( ZsA^4 \) of \( A^4 \) in \( \mathcal{G} \) contains an element with the cycle structure \((123) \ldots \), we have \( z = 3z_1 \). Then (58) implies that \( 1/z_2 = 0 \), which is a contradiction. \( ZsA^4 \) contains \( B \). Hence if \( ZsA^4 \) contains no element with the cycle structure \((123) \ldots \), then we have \( z = z_1 \). Then (58) implies that \( z_1 = 2z_2 \). But the indices of the centralizers of involutions in \( \mathcal{G} \) with respect to \( \mathcal{G} \) are either 1 or 4. This contradicts that \( z_1 = 2z_2 \). Thus \( \mathcal{G} \) must be a dihedral group of order 16.
Let us consider $\mathfrak{H}$ on $T(2)$. Then since $B$ (or $A$) is odd on $T(2)$, $\mathfrak{H}$ contains a normal subgroup $\mathfrak{H}^*$ of index 2, which consists of even permutations of $\mathfrak{H}$ on $T(2)$. A Sylow 2-subgroup $E \cap \mathfrak{H}^*$ of $\mathfrak{H}^*$ is generated by $A^t$ and $AB$. $A^t$ and $AB$ are not conjugate in $\mathfrak{H}^*$. Then since $E \cap \mathfrak{H}^*$ is a dihedral group of order 8, an ordinary transfer argument assures us that $\mathfrak{H}^*$ contains a normal subgroup of index 2. Then since $\mathfrak{H}$ contains a normal subgroup of index 4, $\mathfrak{H}$ contains the normal Sylow 2-complement $\mathfrak{H}_0$ (for instance see [13], Lemma 8).

Let $\mathfrak{F}_1$ denote the subgroup of $\mathfrak{H}$ consisting of all the permutations of $\mathfrak{H}$ each of which fixes the symbol 2. Similarly let $\mathfrak{F}_2$ denote the subgroup of $\mathfrak{H}$ corresponding to 4 instead of 2. Moreover let $\mathfrak{H}'(2)$ denote the 2-commutator subgroup of $\mathfrak{H}$. Then since $\mathfrak{H}$ is 2-nilpotent, the index of $\mathfrak{H}'(2)$ in $\mathfrak{H}$ equals 4. It is easy to see that the indices of $\mathfrak{H}'(2)\mathfrak{F}_i$ with respect to $\mathfrak{H}$ are equal to 2 ($i = 1, 2$). Therefore $\mathfrak{H}$ is divided into 5 domains of transitivity of $\mathfrak{H}'(2)$. Then we have the following equation: $\sum_{H \in \mathfrak{H}'(2)} \alpha(H) = 5 h_1^t$, where $H$ ranges over all the elements of $\mathfrak{H}'(2)$ and $h_1^t$ is the order of $\mathfrak{H}'(2)$. Obviously $\sum_{H \in \mathfrak{H}'(2)} \lambda(H) = h_2^t$.

Furthermore since $C_i$ is a character of 2-defect 0 ($i = 1, 2, \ldots, \frac{h - 1}{2}$), we have by (1.1) $B(S) = 1$ for every 2-singular element $S$ of $\mathfrak{H}$. Then since every element $H$ outside $\mathfrak{H}'(2)$ is 2-singular, we have that $\sum_{H \in \mathfrak{H}'(2)} B(H) = h_2^t$. Therefore using (4.3) we obtain the following equation

$\sum_{H \in \mathfrak{H}'(2)} D_i(H) = 3 h_1^t$.

Let $e$ and $f_1$ be the principal characters of $\mathfrak{H}'(2)$ and $\mathfrak{H}$ respectively. Let $f_i$ ($i = 2, 3, 4$) be the linear characters of $\mathfrak{H}$ containing $\mathfrak{H}'(2)$ in their kernels and different from $f_1$. They can be indexed so that the following character table hold.

<table>
<thead>
<tr>
<th></th>
<th>$A^t$</th>
<th>$B$</th>
<th>$AB$</th>
<th>$A$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$f_2$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$f_3$</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$f_4$</td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>1</td>
</tr>
</tbody>
</table>

Let $e^*$ and $f_i^*$ be the characters of $\mathfrak{H}$ induced by $e$ and $f_i$ ($i = 1, 2, 3, 4$). Then we have the equations:
Furthermore by the reciprocity theorem of Frobenius we have from (59) the following equation:

\[ e^* = A + B + 3D_1 + \sum_{s=1}^{p-1} d_s D_s, \]

where \( D_s \) ranges some irreducible characters of \( G \) of \( p \)-defect 0. (We assume that \( d_s > 0 \)). From these equations we have the following equation:

\[ f_1^* + f_2^* + f_3^* = 2D_1 + \sum_{s=1}^{p-1} d_s D_s. \]

No \( f_k^* \) \((k = 2, 3, 4)\) has the form : \( f_k^* = 2D_1 + \cdots \). In fact, otherwise, we have that \( f_k^* = 2D_1 + D_2 \), where the degree of \( D_2 \) equals \( p \). Then we must have, as is shown in 11, that \( D_2(J) = 1 \) for every involution \( J \) of \( G \), and therefore that \( f_k^*(J) = 3 \). Let \( X_i \) be a permutation of \( G \) which transfers the symbol 1 to \( i (i = 1, 2, \ldots, 3p) \). Then we have a decomposition of \( G \) into the cosets of \( X_i : G = \sum_{i=1}^{3p} G X_i \). Now from the definition of induced characters we have that \( f_k^*(J) = f_k^*(B) = f_k(B) + f_k(X_1BX_1) + f_k(X_2^{-1}BX_2) \), which is less than 3 if \( k = 3 \) or 4, and that \( f_k^*(J) = f_k^*(AB) = f_k(AB) + \cdots \), which is less than 3 if \( k = 2 \). Anyway this is a contradiction.

Therefore either \( f_1^* \) or \( f_2^* \) takes the form : \( f_1^* = D_1 + \cdots \left(l = 2 \text{ or } 3\right) \).

Since \( f_1^* \) cannot be decomposed into characters of degree \( p \) from the same reason as above, we have that \( f_1^* = D_1 + D_2 \), where the degree of \( D_2 \) equals \( 2p \). Using again a theorem of Brauer [3], Lemma 3, we have that \( D_2(J) = 2 \) or \( -2 \) for every involution \( J \) of \( G \). The case \( D_2(J) = 0 \) can be eliminated from the simplicity of \( G \). Since \( f_1^*(J) < 3 \) we must have here that \( D_2(J) = -2 \), and therefore that \( f_1^*(J) = -1 \). Now from the definition of induced characters and from the fact that \( A^i, B \) and \( AB \) are conjugate with each other, we have that \( f_1^*(J) = f_1^*(A^i) = f_i(A^i) + f_i(B) + \cdots \), which is not less than 1 if \( l = 2 \) and that \( f_1^*(J) = f_1^*(A^i) = f_i(A^i) + f_i(AB) + \cdots \), which is not less than 1 if \( l = 3 \). This is a contradiction.

14. Since \( G \) is a dihedral group of order 8, there exists an involution \( B \) of \( G \) such that the cycle structure of \( B \) has the form \((1, 2, \ldots, 3) \). Let \( A \)
be an element of $\Xi$ with order 4. Then since $\frac{1}{4} \cdot 3(p-1)$ is odd, the cycle structure of $A$ has the form $(1), (23)A^*$, where $A^*$ consists of cycles of order 4.

Now we are in a position to use in full some excellent results of Brauer and Suzuki concerning the groups which satisfy the following two conditions:

(i) Their Sylow 2-subgroups are dihedral groups of order either 8 or 4. (ii) They contain no normal subgroup of index 2 ([4], [17] and [13]).

Our group $\mathfrak{G}$ with a dihedral Sylow 2-subgroup of order 8 certainly satisfies these two conditions. Hence the principal 2-block of irreducible characters of $\mathfrak{G}$ consists of five characters $A$ and $X_i$ ($i = 1, 2, 3, 4$), whose degrees satisfy the following equalities:

\[(60) \quad X_4(1) = \varepsilon + X_4(1) = X_i(1) + \varepsilon'X_4(1),\]

where $\varepsilon$ and $\varepsilon'$ equal either 1 or $-1$. Since every $C_i$ is a character of defect 0 for 2, we have $C_i \equiv X_i$. Then it is easy to see from (60) that $X_1 = B$, $\varepsilon = 1$ and $\varepsilon' = 1$.

Put $z = 8y$. Let $ZsA$, $ZsA^2$, $ZsB$, $ZsAB$ and $Zs\Xi$ be the centralizers of $A$, $A^2$, $B$, $AB$ and $\Xi$ in $\mathfrak{G}$. Furthermore we denote by $2l$, $4lu$, $4lu_1$ and $4lu_2$ the orders of $Zs\Xi$, $ZsA \cap ZsA^2$, $ZsB \cap ZsA^2$ and $ZsAB \cap ZsA^2$. Then the first formula of Suzuki concerning the order of $\mathfrak{G}$ is as follows:

\[(61) \quad g = \frac{32y^2(u_1 + u_2)^3p(2p - 1)}{(p-1)^2}.\]

Now we want to show by means of a contradiction that $\mathfrak{G}$ contains a normal subgroup of index 2. So let us assume that $\mathfrak{G}$ contains no normal subgroup of index 2. Then since $\mathfrak{G}$ also satisfies the above two conditions, we have the equality analogous to (61). It is clear from our choice of the elements $A$ and $B$ that $Zs\Xi$, $ZsA \cap ZsA^2$, $ZsB \cap ZsA^2$ and $ZsAB \cap ZsA^2$ are contained in $\mathfrak{G}$. Let $8y'$ be the order of $ZsA^2 \cap \mathfrak{G}$ and let $X_i'$ be the irreducible character of $\mathfrak{G}$ corresponding to $X_i = B$ of $\mathfrak{G}$. Then the first formula of Suzuki for $\mathfrak{G}$ is as follows:

\[(62) \quad \frac{g}{3p} = \frac{64y'u^2(u_1 + u_2)^3X_i'(1)(X_i'(1) + \varepsilon')}{(X_i'(1) - \varepsilon')^2}.\]

where $\varepsilon'$ equals $\pm 1$. Furthermore all the involutions in $\mathfrak{G}$ are conjugate to one another. Hence corresponding to (58) we have here that $y = 3y'$. Then
we obtain from (61) and (62) the following equality:

\[
\frac{X_i(1)(X_i'(1) + \epsilon')}{(X_i'(1) - \epsilon')^2} = \frac{2p - 1}{2(p-1)^3}.
\]

(63) implies at once that \( \epsilon' = -1 \). Furthermore it is easy to check that the right-hand side of (63) is smaller than \( \frac{1}{2} \) and that the left-hand side of (63) is greater than \( \frac{1}{2} \). In the latter case we use the congruence \( X_i(1) \equiv \epsilon' \pmod{8} \) due to Brauer and Suzuki. This is a required contradiction. Hence \( \mathcal{O} \) contains a normal subgroup \( \mathfrak{N}^* \) of index 2.

Then we want to show that \( \mathfrak{N}^* \) contains no normal subgroup of index 2. Assume that \( \mathfrak{N}^* \) contains a normal subgroup of index 2. Then \( \mathfrak{O} \) is 2-nilpotent. Let \( \mathfrak{O}'(2) \) denote the 2-commutator subgroup of \( \mathfrak{O} \). Then the index of \( \mathfrak{O}'(2) \) in \( \mathfrak{O} \) equals 4. It is easy to see that \( \mathfrak{O} \) is divided into either 5 or 7 domains of transitivity of \( \mathfrak{O}'(2) \). But if \( \mathfrak{O} \) is divided into 5 domains of transitivity of \( \mathfrak{H}'(2) \), we obtain the same contradiction as at the end of 13. So let us assume that \( \mathfrak{O} \) is divided into 7 domains of transitivity of \( \mathfrak{O}'(2) \). Then it follows that \( \mathfrak{S} \) is semi-regular on \( T(2) \). Anyway we can use the same notation as in 13. (Instead of \( A^i \) there we must consider here \( A^2 \)). Then we have the equations:

\[
e^* = A + B + 5D_1 + \sum_{\lambda \neq 1} d_\lambda D_\lambda
\]

and

\[
f_i^* + f^*_s + f^*_t = 4D_1 + \sum_{\lambda \neq 1} d_\lambda D_\lambda.
\]

Then some \( f_k^* \) \( (k = 2, 3, 4) \) must have the form: \( f_k^* = 3D_1 \) or \( f_k^* = 2D_1 + \cdots \), which gives us a contradiction as in 13. Thus \( \mathfrak{N}^* \) contains no normal subgroup of index 2.

Now the group \( \mathfrak{N}^* \) with an elementary abelian Sylow 2-subgroup of order 4 satisfies the two conditions at the beginning of this section. The principal 2-block of irreducible characters of \( \mathfrak{N}^* \) consists of four characters \( X_i^* \) \( (i = 0, 1, 2, 3) \), where \( X_0^* \) is the principal character of \( \mathfrak{N}^* \). Let \( 4l^* \) be the order of the centralizer \( Zs_{\mathfrak{O}}(\mathfrak{S} \cap \mathfrak{O}^*) \) in \( \mathfrak{S} \cap \mathfrak{O}^* \) and let \( u^* \) be the index of \( Zs_{\mathfrak{O}}(\mathfrak{S} \cap \mathfrak{O}^*) \) in \( ZsA^2 \cap \mathfrak{O}^* \). Then we have the following formula of Brauer concerning the order of \( \mathfrak{N}^* \):

\[
\frac{g}{6p} = \frac{32u^*l^*X_i^*(1)X_i^*(1)}{(X_i^*(1) + \delta_i)(X_i^*(1) + \delta_i)(X_i^*(1) + \delta_i)}.
\]
ON TRANSITIVE SIMPLE GROUPS OF DEGREE 3

where \( \delta_i \) equals \( 1 \).

Further we need the second formula of Suzuki concerning the order of \( \hat{G} \), which is, using the facts \( X_i = B \), \( \varepsilon = 1 \) and \( \varepsilon' = 1 \) in (60), stated as follows:

\[
g = \frac{128 u y^2 (2p - 1)p}{l(p-1)^2}.
\]

From (61) and (66) we obtain the equality

\[
y = \frac{1}{4} l u (u_1 + u_2)^2.
\]

On the other hand, it is easy to see that \( ZsA^2 \) contains a normal Sylow 2-complement \( \mathbb{Z} \). Let us consider \( \mathbb{E}/\langle A^2 \rangle \) as usual as an operator group of \( \mathbb{Z} \). Then among the orders of subgroups which consist of all the elements of \( \mathbb{Z} \) each of which is fixed by \( A\langle A^2 \rangle \), \( B\langle A^2 \rangle \), \( A\langle A^2 \rangle \) and \( \mathbb{E}/\langle A^2 \rangle \) respectively, there holds the following identity of Brauer-Wielandt ([23]), (1.1)):

\[
y - l uu_1 u_2.
\]

From (67) and (68) we obtain at once that

\[
u_1 = u_2.
\]

Since \( \hat{G} \) contains a normal subgroup of index 2, there are more than one class of involutions in \( \hat{G} \). Therefore the same considerations which led us to (58) yield here that \( ZsA^2 \) is contained in \( \hat{G} \). Now since every 2-regular element of \( \hat{G} \) is contained in \( \hat{G}^* \), we have together with (69) the following

\[
l^* = l u_1,
\]

and

\[
y = l u_1 u^*.
\]

Now using (68), (69), (70) and (71) we obtain from (65) and (66) the following equality:

\[
\frac{2(2p - 1)}{(p-1)^2} = \frac{3 X_1^*(1) X_1^*(1) X_1^*(1)}{(X_1^*(1) + \delta_1)(X_1^*(1) + \delta_2)(X_1^*(1) + \delta_3)}.
\]

Obviously the right-hand side of (72) is not smaller than 3/8. Therefore we have the following inequality

\[0 \geq 3 p^2 - 38 p + 19.\]
This implies that \( p \leq 11. \) Since \( p \equiv 1 \pmod{4}, \) we can conclude that \( p = 5. \) Thus again we have only to check six primitive groups of degree 15 and will find that only the group isomorphic to \( \mathfrak{H}_6 \) satisfies our requirements. It may be convenient to refer to some data: \( p = 5; t_1 = 6, t_2 = 8; z(1, 2) = -3, z(2, 2) = 2, z(1, 3) = 1, z(2, 3) = -2; y = u = u_1 = u_2 = 1 = 1; X^*_t(1) = 3, X^*_t(1) = X^*_s(1) = 1, \delta_1 = 1, \delta_2 = 1. \)

§ 4. The case in which the degree of \( \mathfrak{B} \) is \( p - 1. \)

15. Now let us consider the case in which the degree of \( \mathfrak{B} \) equals \( p - 1. \) Then (4.1) takes one of the following forms:

\[
\begin{align*}
\alpha(X) &= A(X) + B(X) + D_1(X), \\
\alpha(X) &= A(X) + B(X) + D_1(X) + D_2(X),
\end{align*}
\]

where \( D_1 \) is an irreducible character of \( \mathfrak{G} \) with degree \( 2p; \)

\[
\begin{align*}
\alpha(X) &= A(X) + B(X) + D_1(X) + D_2(X),
\end{align*}
\]

where \( D_1 \) and \( D_2 \) are different irreducible characters of \( \mathfrak{G} \) with degree \( p; \)

\[
\begin{align*}
\alpha(X) &= A(X) + B(X) + 2D_1(X),
\end{align*}
\]

where \( D_1 \) is an irreducible character of \( \mathfrak{G} \) with degree \( p. \) Moreover (10) becomes the following form:

\[
(p - 2)(p - 1)p^2 = g(p - 1 - B(J))^2.
\]

By a theorem of Brauer ([3], Lemma 3) we have that \( B(J) = 0. \) Therefore we obtain from (10.6) the following

\[
(10.7) \quad (p - 2)p^2 = g(p - 1).
\]

(10.7) tells us in particular that the order of a Sylow 2-subgroup of \( \mathfrak{G} \) equals the power of 2 dividing \( p - 1, \) say \( 2^a. \) Therefore \( B \) becomes a character of defect 0 for 2. Hence as in 4 by a theorem of Brauer-Tuan ([10], Corollary of Lemma 3) we see that every \( C_i \) belongs to the principal 2-block \( B_1(2) \) of irreducible characters of \( \mathfrak{G} (i = 1, \ldots, \frac{1}{2} (p - 1)). \)

Assume that \( a = 2. \) Then by a theorem of Brauer-Feit ([6], Theorem 1) \( B_1(2) \) contains at most 5 characters. Therefore we have the inequality \( 5 \geq \frac{1}{2} (p + 1), \) which implies that \( p = 5. \) So we have only to consider again 6 types of primitive groups of degree 15. It is easy to check that there is no group among them with required properties. Therefore we can assume that
ON TRANSITIVE SIMPLE GROUPS OF DEGREE $3p$

Since $p \equiv 1 \pmod{4}$, we obtain, as in (39)-(41), that $D_i(J) = 2$ in Case (4.4); $D_i(J) = 1$ ($i = 1, 2$) in Case (4.5) and $D_i(J) = 1$ in Case (4.6). Hence we have

$$\alpha(J) = 3.$$  \hspace{1cm} (73)

16. First of all we want to deal with Case (4.4). Then by (4.4) $\ Omega - \{1\}$ is divided into two domains of transitivity of $\mathfrak{O}$, say $T(i)$ ($i = 1, 2$) ([22], 28.4, 29.2). Let $t_i$ be the length of $T(i)$ ($i = 1, 2$). Then we have

$$t_1 + t_2 = 3p - 1.$$  \hspace{1cm} (44.1)

We see at once from (44.1) that $t_1$ and $t_2$ are simultaneously even or simultaneously odd. Assume that $t_1$ and $t_2$ are odd. Let $x \neq 1$ be any symbol of $\mathfrak{O}$ and let $\mathfrak{R}$ denote the subgroup of $\mathfrak{O}$ consisting of all the permutations of $\mathfrak{O}$ each of which fixes each of the symbols 1 and $x$ of $\mathfrak{O}$. Then it follows from our assumption that $\mathfrak{R}$ contains a Sylow 2-subgroup of $\mathfrak{O}$. Hence $\mathfrak{O}$ cannot contain an involution whose cycle structure has the form $(1x) \ldots$. Since $x \neq 1$ is an arbitrary symbol of $\mathfrak{O}$, every involution must fix the symbol 1 of $\mathfrak{O}$, which contradicts the simplicity of $\mathfrak{O}$. Therefore $t_1$ and $t_2$ are even.

Since $p \equiv 1 \pmod{4}$, we see by (44.1) that either $t_1$ or $t_2$ is semi-odd, say $t_1$. Let $\mathfrak{S}$ be a Sylow 2-subgroup of $\mathfrak{O}$, which is contained in $\mathfrak{R}$. Let us consider $\mathfrak{S}$ as a permutation group on $T(1)$. Then $T(1)$ contains a domain of transitivity of $\mathfrak{S}$ with length 2, say $\{2, 3\}$. Let $X$ be any element of $\mathfrak{S}$ whose cycle structure has the form $(1), (23) \ldots$. Assume that the order of $X$ is $2^b$ with $b > 1$. Then we see by (73) that the cycle structure of $X$ has the form $(1)(23)Y$, where $Y$ consists of cycles of order $2^b$. Since $\mathfrak{O}$ is simple and $X$ must be even, $3(p - 1)/2^b$ must be odd. This implies that $b = a$ and hence that $\mathfrak{S}$ is cyclic. This is a contradiction. Thus $X$ must be an involution. By (73) $X$ fixes just two symbols of $\mathfrak{O} - \{1\}$, say 4 and 5. Now let $\mathfrak{I}$ denote the subgroup of $\mathfrak{O}$ consisting of all the permutations of $\mathfrak{O}$ each of which fixes the symbol 2. Then the index of $\mathfrak{I}$ in $\mathfrak{O}$ equals $2$. Let us consider the centralizer of $X$ in $\mathfrak{I}$. Then since by (73) every element $\neq 1$ of $\mathfrak{I}$ does not fix the symbol 4, the centralizer of $X$ in $\mathfrak{I}$ has order 2. Therefore by a theorem of Suzuki ([16], Lemma 4) $\mathfrak{S}$ contains an element $Z$ such that $\mathfrak{S} = \langle X \rangle \langle Z \rangle$. Since $XZ$ is an involution, we have $XZX = Z^{-1}$. Therefore $\mathfrak{S}$ is a dihedral...
group of order \(2^a\) with \(a \geq 3\).

Let \(B_1(2)\) be the principal 2-block of irreducible characters of \(\mathcal{O}\). Then using a method of Suzuki ([13], (42)-(43)) we see that \(B_1(2)\) contains two irreducible characters \(X_1\) and \(X_4\) whose degrees satisfy the equality
\[
1 + \delta_i X_1(1) = \delta_i X_4(1),
\]
where \(\delta_i\) equals \(\pm 1\). We see at once from (74) that either \(X_1\) or \(X_4\) must be equal to some \(C_i\). But since \(B\) is a character of defect 0 for 2, (74) gives us a contradiction. This contradiction shows that Case (4.4) does not occur.

17. Next let us consider Case (4.6). Then by (4.6) \(\Omega - \{1\}\) is divided into five domains of transitivity of \(\mathcal{O}\), say \(T(i) (i = 1, \ldots, 5)\) ([22], 28.4, 29.2). Let \(t_i\) be the length of \(T(i) (i = 1, \ldots, 5)\). Then we have
\[
t_1 + t_2 + t_3 + t_4 + t_5 = 3p - 1.
\]
We see from (44.2) and (73) that either every \(t_i\) is even or just two of them, say \(t_1\) and \(t_4\), are odd. Assume that the former case occurs. Then the method in 16 can be applied and we obtain a contradiction. Therefore we can assume that the latter case occurs.

Then \(\mathcal{O}\) fixes at least one symbol, say 2, of \(T(1)\) and at least one symbol, say 3, of \(T(2)\). By (73) every element \(\neq 1\) of \(\mathcal{O}\) fixes only the symbols 1, 2 and 3. Let \(X\) be an element of \(\mathcal{O}\) whose cycle structure has the form \((21 \ldots) \ldots\). Then \(X^{-1} \mathcal{O} X\) fixes the symbol 1 and is contained in \(\mathcal{O}\). Therefore by Sylow's theorem there exists an element \(Y\) of \(\mathcal{O}\) such that \(Y^{-1} \mathcal{O} Y = X^{-1} \mathcal{O} X\). Then \(YX^{-1} = Z\) is contained in the normalizer \(N_\mathcal{O} \mathcal{O}\) of \(\mathcal{O}\) in \(\mathcal{O}\) and has the cycle structure \((12 \ldots) \ldots\). Since \(\mathcal{O}\) fixes only the symbols 1, 2 and 3, the cycle structure of \(Z\) must have the form \((123) \ldots\). Assume that there exists an involution \(W\) in \(\mathcal{O}\) which is commutative with \(Z\). Then since the cycle structure of \(WZ\) has the form \((123) \ldots\), we have by (73) that \(\alpha(WZ) = 0\). Moreover since \(WZ\) is 2-singular, we have by a theorem of Brauer-Nesbitt ([8], Theorem 1) that \(B(WZ) = 0\). Therefore we obtain from (4.6) that \(D_i(WZ) = -\frac{1}{2}\). But since \(D_i(WZ)\) must be an integer, this is a contradiction. Thus there is no such an involution.

Let \(V\) be a central involution in \(\mathcal{O}\). Then the above argument implies that \(V\) and \(Z^{-1} VZ\) are not conjugate in \(\mathcal{O}\). Thus there exist more than one class
ON TRANSITIVE SIMPLE GROUPS OF DEGREE 3

of involutions in \( \mathcal{D} \). Assume that \( t_1 = 1 \). Then the normalizer \( Ns \mathcal{D} \) of \( \mathcal{D} \) in \( \mathfrak{G} \) contains an element whose cycle structure has the form \((21 \ldots) \ldots\) and is bigger than \( \mathcal{D} \). Then by the primitivity of \( \mathfrak{G} \) we must have \( \mathfrak{G} = Ns \mathcal{D} \), which implies by the simplicity of \( \mathfrak{G} \) that \( \mathcal{D} = 1 \). Then the order of \( \mathfrak{G} \) equals \( 3p \), which contradicts the simplicity of \( \mathfrak{G} \). Thus we have that \( t_1 > 1 \). Now \( T(1) \) contains at least one symbol, say \( 4 \), different from \( 2 \). Since \( T(1) \) is a domain of transitivity of \( \mathcal{D} \), there exists a Sylow 2-subgroup \( \mathcal{E}^* \) of \( \mathcal{D} \) such that \( \mathcal{E}^* \) fixes the symbols \( 1, 4 \) and \( x \), where \( x \) is a symbol of \( T(2) \). Let \( U \) be an involution in \( \mathcal{E}^* \), which is not conjugate to \( V \). Then by a theorem of Brauer-Fowler ([7], Lemma (3 A)) there must exist an involution \( I \) of \( \mathcal{D} \) which is commutative with \( U \) and \( V \). Since every permutation \( \neq 1 \) of a Sylow 2-subgroup of \( \mathcal{D} \) fixes the same symbols, this implies that \( I \) must fix at least four symbols \( 1, 2, 3 \) and \( 4 \) contradicting (73). This contradiction shows that Case (4.6) does not occur.

18. Finally let us consider Case (4.5). Then by (4.5) \( \mathfrak{G} - \{1\} \) is divided into three domains of transitivity of \( \mathcal{D} \), say \( T(i) \) \((i = 1, 2, 3)\) ([25], 28.4, 29.2). Let \( t_i \) be the length of \( T(i) \) \((i = 1, 2, 3)\). Then we have

\[
(44.3) \quad t_1 + t_2 + t_3 = 3p - 1.
\]

We see from (44.3) that either every \( t_i \) is even or just two of them, say \( t_1 \) and \( t_2 \), are odd. Assume that the former case occurs. Then the method in 16 can be applied and we obtain a contradiction. Therefore we can assume that the latter case occurs.

If there exist more than one class of involutions in \( \mathcal{D} \), then the method in 17 can be applied and we obtain a contradiction. Therefore we can assume that all the involutions in \( \mathcal{D} \) are conjugate one another in \( \mathcal{D} \).

Now it follows from the argument in 17 that there exist in \( \mathfrak{G} \) an involution \( W \) and a 3-element \( Z \), which satisfy the following two conditions: (i) \( W \) and \( Z \) are commutative with each other. (ii) \( W \) and \( Z \) have the cycle structures \((1)(2)(3) \ldots\) and \((123) \ldots\) respectively.

Next let us consider the matrices \( V(T(i)) \) \((i = 1, 2, 3)\) as in 12. Without loss of generality we can assume that the diagonal form of \( V(T(i)) \) is
Then as in [21] we obtain the following:

$$z(i, j)$$ is an algebraic integer ($$i = 1, 2, 3; j = 1, 2, 3, 4$$). In particular, $$z(i, 1)$$ and $$z(i, 2)$$ are rational integers ($$i = 1, 2, 3$$). Furthermore we have that $$z(i, 1) = t_i$$ and $$z(i, j) = t_i$$ ($$i = 1, 2, 3; j = 2, 3, 4$$).

$$(i)$$ $$z(i, 1) + (p - 1)z(i, 2) + pz(i, 3) + pz(i, 4) = 0.$$

$$(ii)$$ $$z(i, 1)^2 + (p - 1)z(i, 2)^2 + p|z(i, 3)|^2 + p|z(i, 4)|^2 = 3pt_i.$$

Let us assume that $$D_1$$ and $$D_2$$ are rational characters. Then using a method of Wielandt ([22], p. 82) we see that every $$z(i, j)$$ is a rational integer. We consider (47.1) for $$i = 1$$. Then since from our assumptions $$t_1$$ is odd, we have from (ii) that $$z(1, 3) + z(1, 4) \equiv 1 \pmod{2}$$ and from (iii) that $$z(1, 3)^2 + z(1, 4)^2 \equiv 0 \pmod{2}$$. This is a contradiction. Now by (4.5) we see that $$D_3$$ (and only $$D_2$$) is an algebraically conjugate character of $$D_1$$.

Here let us consider the element $$WZ$$. Assume that $$D_1(WZ)$$ is rational. Then since $$D_1$$ and $$D_2$$ are algebraically conjugate, we have that $$D_1(WZ) = D_2(WZ)$$. On the other hand, since the cycle structure of $$WZ$$ has the form (123)... we have by (73) that $$\alpha(WZ) = 0$$. Moreover since $$WZ$$ is 2-singular and $$B$$ has 2-defect 0, we have by a theorem of Brauer-Nesbitt ([8], Theorem 1) that $$B(WZ) = 0$$. Therefore by (4.5) we have that $$D_1(WZ) = -\frac{1}{2}$$. Since $$D_1(WZ)$$ must be an integer, this is a contradiction.

Let the order of $$Z$$ be $$3^e$$. Then $$D_1(WZ)$$ belongs to the field of the $$3^e$$-th roots of unity over the rational number field $$Q$$. But this field is a cyclic field
over \( \mathbb{Q} \) and \( D_i(WZ) \) has degree two over \( \mathbb{Q} \), \( D_i(WZ) \) belongs to the field of the cubic roots of unity over \( \mathbb{Q} \): \( \mathbb{Q}(\omega) \) with \( \omega^3 = 1, \omega \neq 1 \). Furthermore since \( D_i \) and \( D_j \) are algebraically conjugate only with each other, we see that the field of \( D_i \) over \( \mathbb{Q} \), namely the field generated by all the numbers \( D_i(X) \), where \( X \) ranges over all the elements of \( \mathfrak{S} \), is \( \mathbb{Q}(\omega) \) \((i = 1, 2)\). Then again using the method of Wielandt ([25], p. 82) we see that all the \( z(i, j) \)'s belong to \( \mathbb{Q}(\omega) \) and that \( z(i, 3) \) and \( z(i, 4) \) are complex-conjugate numbers \((i = 1, 2, 3)\). The latter fact follows from the complex conjugacy of \( D_i \) and \( D_j \).

Now the numbers 1 and \( \frac{1}{2}(1 + \sqrt{3}i) \) constitute an integral basis of \( \mathbb{Q}(\omega) \). Therefore we can put

\[
(75) \quad z(i, 3) = \frac{1}{2}(n_i + m_i\sqrt{3}i) \text{ and } z(i, 4) = \frac{1}{2}(n_i - m_i\sqrt{3}i),
\]

where \( n_i \) and \( m_i \) are rational integers \((i = 1, 2, 3)\).

Choose a Sylow 2-subgroup \( \mathfrak{S} \) of \( \mathfrak{G} \) as in 17. Then by (73) \( \mathfrak{S} \) is semi-regular on \( T(1) - \{2\}, T(2) - \{3\} \) and \( T(3) \). Hence we have the congruences:

\[
(76) \quad t_i \equiv 1 \pmod{2^a} \text{ \((i = 1, 2)\)} \text{ and } t_3 \equiv 0 \pmod{2^a}.
\]

Furthermore we see as in 17 that

\[
(77) \quad t_i > 1 \text{ \((i = 1, 2, 3)\)}.
\]

Now we obtain from (47.1) (ii) and (75) the following congruences:

\[
(78) \quad n_i \equiv -1 \pmod{2^a} \text{ \((i = 1, 2)\)} \text{ and } n_3 \equiv 0 \pmod{2^a}.
\]

Therefore we can put

\[
(79) \quad n_i = A_i 2^a - 1 \text{ \((i = 1, 2)\)} \text{ and } n_3 = A_3 2^a,
\]

where \( A_i \) is a rational integer \((i = 1, 2, 3)\).

At any rate we have by a theorem of Brauer-Feit ([6], Theorem 1) the following inequality:

\[
\frac{1}{2}(p + 1) \leq 2^{2a - 3},
\]

which implies in particular that

\[
(80) \quad 2^{2a} \geq 2p.
\]

Now we want to show that (1) \( t_i \geq p + 2 \text{ \((i = 1, 2)\)} \) and (2) \( t_3 \geq p - 1 \), which
yield us a contradiction \( t_i + t_4 + t_5 \geq 3p + 3 \) to (44.3). We deal only (1), because (2) can be dealt with quite similarly as (1). At first let us assume that \(|A_i| \geq 3\) or \(A_i = -2\). Then we have from (78) and (79) that

\[
n_i^1 = A_i 2^{2a} - A_i 2^{a+1} + 1 > 8p.
\]

Assume that \(A_i = 2\). Then we have similarly that

\[
n_i^1 = 2^{2a+1} - 2^{a+2} + 1 > \frac{1}{2} \cdot 7 \cdot 2^{2a} > 7p.
\]

Hence if \(|A_i| \geq 2\), then we have from (47.1) (iii), (75) and (78) that

\[
t_i > (|z(i, 3)|^2 + |z(i, 4)|^2)/3 > n_i^1/6 > 7p/6 > p + 2.
\]

Now we can assume that \(|A_i| \leq 1\). If \(A_i = 0\), then we have by (47.1) (ii) that

\[
t_i = p - (p - 1)z(i, 2),
\]

which implies by (77) that \(t_i \geq p\). But \(t_i\) cannot be equal to \(p\), because \(t_i\) is a divisor of the order of \(\mathfrak{d}\). Since \(t_i\) is odd, thus we have that \(t_i \geq p + 2\). If \(A_i = 1\), then we have by (47.1) (ii) that

\[
t_i = -(p - 1)z(i, 2) - p(2^a - 1).
\]

Let us consider a linear form \(L(X) = (p - 1)X - p(2^a - 1)\) in \(X\) on the domain of rational integers. \(L(X)\) attains its least positive value \(p - 2^a\) at \(X = 2^a\). The next least positive value of \(L(X)\) is certainly not smaller than \(p\). So let us assume that \(t_i = p - 2^a\) and \(z(i, 2) = 2^a\). Then we have by (76) and (77) that \(p > 2^{a+1}\). But since \(2^a\) is an exact power of \(2\) dividing \(p - 1\), we have that \(p \geq 3 \cdot 2^a\). Then we have further that \((2^a - 1)^2 \geq 4p/3\). Then finally we have by (47.1) (iii) and (79) that
\[ t_i \geq ((t_1^2 + (p-1)2^{a+1} + \frac{1}{2}p(2^a - 1)^3)/3p \]
\[ > 4p/27 + 2p/3 - 2/3 + 2p/9 \]
\[ > 28p/27 - 2/3 \]
\[ > p. \]

The case of \( A_i = -1 \) can be handled quite similarly.

§ 5. Proof of Theorem 2.

Let \( \mathcal{G} \) denote the subgroup of \( \mathcal{G} \) consisting of all the permutations of \( \mathcal{G} \) each of which fixes the symbol 1 of \( \Omega \). Since \( \mathcal{G} \) is imprimitive on \( \Omega \) and since \( \mathcal{G} \) is simple, \( \mathcal{G} \) contains a subgroup \( \mathcal{M} \) of index \( p \) containing \( \mathcal{G} \). Hence by a previous result [14] \( \mathcal{G} \) is isomorphic to a linear fractional group \( LF(2, 2^m) \) with \( p = 2^m + 1 \) (\( m \geq 2 \)), and \( \mathcal{M} \) becomes the normalizer of a Sylow 2-subgroup of \( \mathcal{G} \). Conversely let us consider any \( LF(2, 2^m) \) such that \( p = 2^m + 1 \) is a prime number greater than 3. Let \( \mathcal{M} \) be the normalizer of a Sylow 2-subgroup of \( LF(2, 2^m) \). Then since \( m \) is even, the order of \( \mathcal{M} \) is divisible by 3. Hence \( \mathcal{M} \) contains a (uniquely determined) subgroup of index 3, because the factor group of \( \mathcal{M} \) by its Sylow 2-subgroup is cyclic. Therefore such an \( LF(2, 2^m) \) can always be represented (uniquely) as an imprimitive permutation group of degree 3p.

References

[18] John Thompson wrote to the author that he does not intend to publish this "special" result, but he and Walter Feit are preparing to publish a proof of the full Burnside conjecture.

Department of Mathematics
Cornell University
Ithaca, New York, U.S.A.
and
Mathematical Institute
Nagoya University
Nagoya-Chikusa, Japan