TRANSITIVE PERMUTATION GROUPS OF DEGREE $p=2q+1$, p AND q BEING PRIME NUMBERS. II[1]

BY
NOBORU ITO

Introduction. Let p be a prime number such that $q = \frac{1}{2}(p-1)$ is also a prime number. Let Ω be the set of symbols $1,\cdots,p$, and $\mathfrak{G}$ be a nonsolvable transitive permutation group on Ω. In [10] and [11] the structure of such a permutation group $\mathfrak{G}$ has been studied, and, in particular, the following theorem [11, Theorem 1] has been proved: If $r = \frac{1}{4}(p-3)$ is also a prime number, then $\mathfrak{G}$ is triply transitive. The purpose of this work is to remove this additional assumption, namely, to prove the following theorem.

THEOREM. *If $\mathfrak{G}$ is not triply transitive, then $\mathfrak{G}$ is isomorphic to either $LF(2,7)$ with $p=7$ or $LF(2,11)$ with $p=11$.*

Hence, in particular, if $p>11$, then $\mathfrak{G}$ is triply transitive.

Now let $\mathfrak{N}$ be a minimal normal subgroup of $\mathfrak{G}$. Since $\mathfrak{G}$ is obviously primitive, $\mathfrak{N}$ is transitive on Ω. Let $\mathfrak{P}$ be a Sylow p-subgroup of $\mathfrak{G}$. Then $\mathfrak{P}$ is contained in $\mathfrak{N}$. As a minimal normal subgroup $\mathfrak{N}$ is a direct product of mutually isomorphic simple groups. Since the order of $\mathfrak{N}$ is divisible by p only to the first power, $\mathfrak{N}$ must be simple. On the other hand, by a theorem of Sylow, we have that $\mathfrak{G} = \mathfrak{N}Ns\mathfrak{P}$, where $Ns\mathfrak{P}$ denotes the normalizer of $\mathfrak{P}$ in $\mathfrak{G}$. Since $\mathfrak{P}$ obviously coincides with its own centralizer in $\mathfrak{G}$, $Ns\mathfrak{P}/\mathfrak{P}$ is a cyclic group of order dividing $p-1$. Since we have that $\mathfrak{G}/\mathfrak{N} \cong Ns\mathfrak{P}/Ns\mathfrak{P}\cap\mathfrak{N}$ and $Ns\mathfrak{P}\cap\mathfrak{N} \supseteq \mathfrak{P}$, $\mathfrak{G}/\mathfrak{N}$ is also a cyclic group of order dividing $p-1$. Since $\mathfrak{G}$ is nonsolvable, $\mathfrak{N}$ is nonsolvable, too. Therefore in order to prove the theorem we can assume the simplicity of $\mathfrak{G}$. So from now on let $\mathfrak{G}$ be simple.

If $Ns\mathfrak{P} = \mathfrak{P}$, then by a splitting theorem of Burnside $\mathfrak{G}$ contains a normal Sylow p-complement. Since $\mathfrak{G}$ is simple, this implies that $\mathfrak{G} = \mathfrak{P}$, contradicting the nonsolvability of $\mathfrak{G}$. If the order of $Ns\mathfrak{P}$ is even, let us consider an involution in $Ns\mathfrak{P}$. The cycle structure of this involution consists of q transpositions, and it is odd, contradicting the simplicity of $\mathfrak{G}$, because we can obviously assume the oddness of q. Hence the order of $Ns\mathfrak{P}$ must be equal to qp. Let $\mathfrak{Q}$ be a Sylow q-subgroup of $Ns\mathfrak{P}$ such that $\mathfrak{Q}$ fixes the symbol 1 of Ω. If $\mathfrak{Q}$ is not a Sylow q-subgroup of $\mathfrak{G}$, then $\mathfrak{G}$ contains a q-cycle. Hence by a theorem of Jordan [17] $\mathfrak{G}$ coincides with the alternating group $\mathfrak{A}$ on Ω. $\mathfrak{A}$ is triply transitive for $p \geqq 5$. Therefore in order to prove the theorem we can assume that $\mathfrak{Q}$ is

Received by the editors May 27, 1963.

[1] This paper is a continuation of [11] with the same title.

a Sylow q-subgroup of $\mathfrak{G}$. Let $Cs\mathfrak{Q}$ be the centralizer of $\mathfrak{Q}$ in $\mathfrak{G}$. If $Cs\mathfrak{Q}$ contains $\mathfrak{Q}$ properly, then $Cs\mathfrak{Q}$ contains a $2q$-cycle, which is odd, contradicting the simplicity of $\mathfrak{G}$. Therefore we have that $Cs\mathfrak{Q} = \mathfrak{Q}$. Let $Ns\mathfrak{Q}$ be the normalizer of $\mathfrak{Q}$ in $\mathfrak{G}$ and let $\mathfrak{R}$ be a Sylow q-complement of $Ns\mathfrak{Q}$: $Ns\mathfrak{Q} = \mathfrak{Q}\mathfrak{R}$ and $\mathfrak{Q} \cap \mathfrak{R} = 1$. Then $\mathfrak{R}$ is a cyclic group of order dividing $q-1$, say r, and $\mathfrak{R}$ fixes three orbits of $\mathfrak{Q}$ from Ω as a whole. Put $q-1 = rs$.

Now it is clear that the results of Brauer concerning the groups containing self-centralizing subgroups of prime orders, which will be mentioned just below, can be applied for G with two prime numbers p and q.

As in [11] our proofs mainly rely on the following results of Frobenius [8], [9], Brauer [4], Brauer and Tuan [3], [15], Wielandt [16], Manning [12] and Frame [7], which will be listed here for convenience.

Proposition A (Frobenius). *Let $\mathfrak{S}$ be the symmetric group on Ω. Let X_0, $X_{\substack{0\\0}}$ and X_{00} be irreducible characters of $\mathfrak{S}$ corresponding to Young diagrams*

$$\begin{array}{lll} 00\cdots0, & 00\cdots0 \text{ and } & 00\cdots0. \\ 0 & 0 & 00 \\ & 0 & \end{array}$$

Then $\mathfrak{G}$ is doubly transitive if and only if X_0 restricted on $\mathfrak{G}$ is irreducible; $\mathfrak{G}$ is triply transitive if and only if $\mathfrak{G}$ is doubly transitive and X_0 restricted on $\mathfrak{G}$ is orthogonal to both $X_{\substack{0\\0}}$ restricted on $\mathfrak{G}$ and X_{00} restricted on $\mathfrak{G}$.

We have that

$$X_0(S) = \alpha(S) - 1, \tag{1}$$

$$X_{\substack{0\\0}}(S) = \tfrac{1}{2}\{\alpha(S)-1\}\{\alpha(S)-2\} - \beta(S) \tag{2}$$

and

$$X_{00}(S) = \tfrac{1}{2}\alpha(S)\{\alpha(S)-3\} + \beta(S) \tag{3}$$

for every permutation S of $\mathfrak{S}$, where $\alpha(S)$ denotes the number of symbols of Ω fixed by S and $\beta(S)$ denotes the number of transpositions in the cycle structure of S. In particular, the degrees of X_0, $X_{\substack{0\\0}}$ and X_{00} are equal to $p-1$, $(q-1)p+1$ and $(q-1)p$, respectively.

Proposition B (Brauer). *The degree of an irreducible character X of $\mathfrak{G}$ is congruent to either 1 or 0 or -1 or $-\delta_p q$ modulo p and either 1 or 0 or -1 or $-\delta_q r$ modulo q, where δ_p and δ_q are equal to ± 1, respectively. Furthermore if $r = q-1$, then $-\delta_q r$ can be omitted from above. We say that X has p-type A or D or B or C, according as the degree of X is congruent to 1 or 0 or -1 or $-\delta_p q$ modulo p, respectively. Similarly we say that X has q-type A or D or B or C, according as the degree of X is congruent to 1 or 0 or -1 or $-\delta_q r$ with $r < q-1$ modulo q, respectively. The number of irreducible characters of $\mathfrak{G}$ of p-type A or B is equal to q and that of p-type C is equal to 2. If*

$r < q-1$, the number of irreducible characters of $\mathfrak{G}$ of q-type A or B is equal to r and that of q-type C is equal to s. If $r = q-1$, the number of irreducible characters of q-type A or B is equal to q. Let P be an element of order p of $\mathfrak{G}$. Then we have that $X(P) = 1$ or 0 or -1, according as X has p-type A or D or B. Let Q be an element of order q of $\mathfrak{G}$. Then we have that $X(Q) = 1$ or 0 or -1, according as X has q-type A or D or B. Two irreducible characters of p-type C take the same value at any p-regular element of $\mathfrak{G}$ and the sum of whose values at P equals δ_p. If $r < q-1$, then s irreducible characters of q-type C take the same value at any q-regular element of $\mathfrak{G}$ and the sum of whose values at Q equals δ_q.

PROPOSITION C (BRAUER AND TUAN). *If $\mathfrak{G}$ possesses a nonprincipal irreducible character of degree not greater than $\frac{1}{2}(p+1)$, then $\mathfrak{G}$ is isomorphic to $LF(2,p)$ or $p = 7$. Since $\mathfrak{G}$ contains a subgroup of index p in the present case, by a celebrated theorem of Galois* [6] *this implies that $p = 5$ or 7 or 11.*

PROPOSITION D (WIELANDT). *Let Λ be the set of symbols $1, \cdots, 2l$, where l is an odd prime number. Let $\mathfrak{X}$ be a uniprimitive, that is, primitive and not doubly transitive permutation group on Λ. Let $\mathfrak{Y}$ be the maximal subgroup of $\mathfrak{X}$ leaving the symbol 1 of Λ fixed. Then the following facts hold:* (a) *There exists a positive integer m such $2l = m^2+1$.* (b) *Λ is decomposed into three orbits of $\mathfrak{Y}$, $\{1\}$, $\mathfrak{M}_1$ and $\mathfrak{M}_2$, where the lengths of $\mathfrak{M}_1$ and $\mathfrak{M}_2$ are $\frac{1}{2}m(m+1)$ and $\frac{1}{2}m(m-1)$, respectively.* (c) *Let $1_{\mathfrak{Y}}$ be the principal character of $\mathfrak{Y}$ and $1_{\mathfrak{Y}}^0$ be the character of $\mathfrak{X}$ induced by $1_{\mathfrak{Y}}$. Then $1_{\mathfrak{Y}}^0$ is decomposed into three irreducible characters of $\mathfrak{X}$: $1_{\mathfrak{Y}}^0 = 1_{\mathfrak{X}} + \boldsymbol{l}_1 + \boldsymbol{l}_2$, where $1_{\mathfrak{X}}$ is the principal character of $\mathfrak{X}$ and $\boldsymbol{l}_1$ and $\boldsymbol{l}_2$ are rational characters whose degrees are $l-1$ and l, respectively. Let L be an element of $\mathfrak{X}$ of order l. Then we have that $\boldsymbol{l}_1(L) = -1$ and $\boldsymbol{l}_2(L) = 0$.*

PROPOSITION E (MANNING). *Let Λ be the set of symbols $1, \cdots, n$. Let $\mathfrak{X}$ be a uniprimitive permutation group on Λ. Let $\mathfrak{Y}$ be the subgroup of $\mathfrak{X}$ leaving the symbol 1 of Λ fixed. If there exists an orbit Λ_1 of $\mathfrak{Y}$ of length $l_1 > 2$, on which $\mathfrak{Y}$ is doubly transitive, then there exists an orbit Λ_2 of $\mathfrak{Y}$, whose length l_2 is greater than l_1 and divides $\frac{1}{2}l_1(l_1-1)$.*

PROPOSITION F (FRAME). *Let Λ be the set of symbols $1, \cdots, n$. Let $\mathfrak{X}$ be a transitive permutation group on Λ. Let $\mathfrak{Y}$ be the subgroup of X leaving the symbol 1 of Λ fixed. Let Λ_i be the orbits of $\mathfrak{Y}$ from Λ $(i = 1, \cdots, k)$. Let l_i denote the length of Λ_i $(i = 1, \cdots, k)$. Put $N = n^{k-2}l_1 \cdots l_k$. Let $1_{\mathfrak{Y}}$ be the principal character of $\mathfrak{Y}$ and $1_{\mathfrak{Y}}^0$ be the character of $\mathfrak{X}$ induced by $1_{\mathfrak{Y}}$. Let $1_{\mathfrak{Y}}^0 = \sum_{i=1}^{k'} e_i X_i$ be the decomposition of $1_{\mathfrak{Y}}^0$ into its irreducible parts $(e_i \geqq 1;\ i = 1, \cdots, k')$. Let x_i denote the degree of $\mathfrak{X}_i$ $(i = 1, \cdots, k')$. Put $D = x_1^{e_1{}^2} \cdots x_{k'}^{e_{k'}{}^2}$. Then the number N/D is an integer.*

The following facts are known [5, §270]. Let $\mathfrak{X}$ be a finite group of order x and X be an irreducible character of $\mathfrak{X}$. If X is not a real character, then we have that $\sum_{X \in \mathfrak{X}} X(X^2) = 0$. If X is a real character, then we have that $\sum_{X \in \mathfrak{X}} X(X^2) = x$ or $-x$. We say that X has the quadratic signature 1 or 0 or -1, according as $\sum_{X \in \mathfrak{X}} X(X^2) = x$ or 0 or $-x$.

Now let $\mathfrak{X}$ be a transitive permutation group on a set Λ. Let 1 be a symbol of Λ and let $\mathfrak{Y}$ be the subgroup of $\mathfrak{X}$ leaving 1 fixed. Let $\mathfrak{M}$ be an orbit of $\mathfrak{Y}$ from Λ and let i be a symbol of $\mathfrak{M}$. Let X be a permutation of $\mathfrak{X}$ which transfers 1 to i. Let the double coset $\mathfrak{Y}X\mathfrak{Y}$ of $\mathfrak{Y}$ with respect to $\mathfrak{X}$ correspond to $\mathfrak{M}$. This correspondence between the orbits of $\mathfrak{X}$ from Λ and the double cosets of $\mathfrak{Y}$ with respect to $\mathfrak{X}$ is one-to-one. If $\mathfrak{Y}X\mathfrak{Y} = \mathfrak{Y}X^{-1}\mathfrak{Y}$, we say that $\mathfrak{Y}X\mathfrak{Y}$ and the corresponding orbit are real.

PROPOSITION G (FRAME). *Let $\mathfrak{X}$ be a transitive permutation group on a set Λ. Let* 1 *be a symbol of Λ and $\mathfrak{Y}$ be the subgroup of $\mathfrak{X}$ leaving the symbol* 1 *fixed. Let π be the permutation character of $\mathfrak{X}$. Let c_i be the sum of multiplicities of irreducible components of π with the quadratic signature i $(i = 1, -1)$. Then the number of real double cosets (real orbits) of $\mathfrak{Y}$ is equal to* $\sum_{X \in \mathfrak{X}} \pi(X^2) = c_1 - c_{-1}$.

The following notation will be used. $\mathfrak{H}$ is the maximal subgroup of $\mathfrak{G}$ leaving the symbol 1 of Ω fixed. $\mathfrak{K}$ is the maximal subgroup of $\mathfrak{G}$ leaving the symbols 1 and 2 of Ω individually fixed. Let $\mathfrak{X}$ be a subgroup of $\mathfrak{G}$. Then $1_{\mathfrak{X}}$ denotes the principal character of $\mathfrak{X}$ and $1^*_{\mathfrak{X}}$ is the character of $\mathfrak{G}$ induced by $1_{\mathfrak{X}}$. If $\mathfrak{X}$ is a subgroup of $\mathfrak{H}$, then $1^{\#}_{\mathfrak{X}}$ denotes the character of $\mathfrak{H}$ induced by $1_{\mathfrak{X}}$. Moreover $Ns\mathfrak{X}$ denotes the normalizer of $\mathfrak{X}$ in $\mathfrak{G}$. The orders of $\mathfrak{G}$ and $\mathfrak{H}$ will be denoted by g and h, respectively.

Now by a famous theorem of Burnside $\mathfrak{G}$ is doubly transitive. Therefore we have many equality relations between the reducible characters of $\mathfrak{G}$, which are mainly due to Frobenius [8], [9]:

$$\sum_{X \in \mathfrak{G}} \alpha(X) = g, \tag{4}$$

$$\sum_{X \in \mathfrak{G}} \{\alpha(X)\}^2 = 2g, \tag{5}$$

$$\sum_{X \in \mathfrak{G}} \beta(X) = \tfrac{1}{2}g, \tag{6}$$

$$1^*_{\mathfrak{H}}(X) = 1_{\mathfrak{G}}(X) + X_0(X) \tag{7}$$

for every permutation X of $\mathfrak{G}$,

$$1^*_{\mathfrak{K}}(X) = 1_{\mathfrak{K}}(X) + 2X_0(X) + X_{\substack{0\\0}}(X) + X_{00}(X) \tag{8}$$

for every permutation X of $\mathfrak{G}$, and

$$1^*_{Ns\mathfrak{K}}(X) = 1_{\mathfrak{G}}(X) + X_0(X) + X_{00}(X) \tag{9}$$

for every permutation X of $\mathfrak{G}$.

The main idea of the following proof is to use Proposition A. Namely the theorem will be assumed to be false. Then it will be shown that the decompositions of X_{0}^{0} restricted on $\mathfrak{G}$ and X_{00} restricted on $\mathfrak{G}$ into their irreducible components must have very peculiar forms, which are enough to get contradictions therefrom. Now one of the main roles of Proposition B is to exclude all but a few possibilities of the forms of the decompositions of X_{0}^{0} restricted on $\mathfrak{G}$ and X_{00} restricted on $\mathfrak{G}$ into their irreducible components. Since it can be certainly assumed that $p > 11$, Proposition C will be effectively used to exclude some of the remaining critical cases. Now as in [11] the following notation will be used. (X, Y) denotes a nonprincipal irreducible character of $\mathfrak{G}$, which has p-type X and q-type $Y (X,\ Y = A,\ B,\ C,\ D)$. Then Propositions B and C enable us to compute the least possible degree of (X, Y) as follows. In order to obtain the next least possible degree it is enough just to add pq to the corresponding least possible degree.

TYPE	LEAST POSSIBLE DEGREE	
(A,A)	$qp+1$	
(A,B)	$(q-2)p+1$	
(A,C)	$(q-r-1)p+1$ $(r-1)p+1$	$\delta_q = 1$ $\delta_q = -1$
(A,D)	$(q-1)p+1$	
(B,A)	$2p-1$	
(B,B)	$qp-1$	
(B,C)	$(q-r+1)p-1$ $(r+1)p-1$	$\delta_q = 1$ $\delta_q = -1$
(B,D)	$p-1$	
(C,A)	$\frac{1}{2}\{(2q+1)p+1\}$ $\frac{1}{2}(3p-1)$	$\delta_p = 1$ $\delta_p = -1$
(C,B)	$\frac{1}{2}\{(2q-3)p+1\}$ $\frac{1}{2}\{(2q-1)p-1\}$	$\delta_p = 1$ $\delta_p = -1$
(C,D)	$\frac{1}{2}\{(2q-1)p+1\}$ $\frac{1}{2}\{(2q+1)p-1\}$	$\delta_p = 1$ $\delta_p = -1$
(D,A)	p	
(D,B)	$(q-1)p$	
(D,C)	$(q-r)p$ rp	$\delta_q = 1$ $\delta_q = -1$
(D,D)	qp	

If $\mathfrak{H}$ is imprimitive on $\Omega - \{1\}$, then by a theorem of Wielandt (unpublished; for a proof see [10, Theorem 1]) $\mathfrak{G}$ is isomorphic to $LF(2,7)$ with $p = 7$. Hence the primitivity of $\mathfrak{H}$ will be assumed hereafter. Therefore $\mathfrak{H}$ is assumed to be uniprimitive on $\Omega - \{1\}$ and Proposition D is useful and necessary from the beginning. By Proposition D the following equality holds for every permutation X of $\mathfrak{H}$.

$$(10) \qquad 1_{\mathfrak{K}}^{*}(X) = 1_{\mathfrak{H}}(X) + \boldsymbol{b}(X) + \boldsymbol{d}(X),$$

where the degrees of $\boldsymbol{b}$ and $\boldsymbol{d}$ are equal to $q-1$ and q, respectively. Then the following equality follows from (7), (8), (10) and the transitivity of induced characters:

$$(11) \qquad \boldsymbol{b}^{*}(X) + \boldsymbol{d}^{*}(X) = X_0(X) + X_{\underset{0}{0}}(X) + X_{00}(X)$$

for every permutation X of $\mathfrak{G}$.

These equalities and Propositions E and F will be used to show that characters of q-type C exist and that they have p-type A, and that $\delta_q = -1$, namely the appearance of $(A,C)_i$ $(i = 1,\cdots,s)$ of degree $(r-1)p + 1$ in $\boldsymbol{b}^{*}, \boldsymbol{d}^{*}, X_{\underset{0}{0}}$ restricted on $\mathfrak{G}$ and X_{00} restricted on $\mathfrak{G}$. Then r will be shown to be odd and this implies that $(A,C)_i$ $(i = 1,\cdots,s)$ is not a real character. Now Proposition G will be used to show the existence of $(B,D)_0$ with degree $p-1$ such that $(B,D)_0$ restricted on $\mathfrak{H}$ equals $2\boldsymbol{d}$. At last the comparison of the decompositions of $(B,D)_0\overline{(B,D)}_0$ and $X_0\overline{(B,D)}_0$ into their irreducible components leads us to a required contradiction.

As an immediate consequence of the theorem, Theorem V in [11] can be improved as follows: Let p be a prime number > 23 satisfying the following conditions: (i) $\frac{1}{2}(p-1)$ and $\frac{1}{4}(p-3)$ are also prime numbers and (ii) $p-4$ is a prime number. Then every nonsolvable transitive permutation group of degree p contains the alternating group of the same degree.

1. **Triple transitivity (proof of theorem).** First of all, it is noted here that the simplicity of $\mathfrak{G}$, the uniprimitivity of $\mathfrak{H}$ on $\Omega - \{1\}$ and $p > 11$ have been assumed.

Since $1_{\mathfrak{K}}^{*}(X) = \alpha(X) - 1$ for every permutation X of $\mathfrak{H}$, using the orthogonality relations of the group characters we get the following equality from (10):

$$\sum_{X \in \mathfrak{H}} \{\alpha(X) - 1\}^2 = 3h.$$

Since the same equality holds for each of p conjugate subgroups of $\mathfrak{H}$ in $\mathfrak{G}$, this implies that

$$\sum_{X \in \mathfrak{G}} \alpha(X)\{\alpha(X) - 1\}^2 = 3g.$$

Then by (4) and (5) the following equality is obtained.

(12) $$\sum_{X\in\mathfrak{G}} \{\alpha(X)\}^3 = 6g.$$

By (1)–(5) this is transformed into

(13) $$\sum_{X\in\mathfrak{G}} \{X_{0_0}(X) + X_{00}(X)\} X_0(X) = g.$$

Now by (1), (3)–(5) we obtain that

(14) $$\sum_{X\in\mathfrak{G}} X_{00}(X)X_0(X) = \sum_{X\in\mathfrak{G}} \alpha(X)\beta(X).$$

The right-hand side of (14) is positive, because of the existence of an involution in $\mathfrak{H}$. Now by the orthogonality relations of the group characters two expressions

$$\sum_{X\in\mathfrak{G}} X_{0_0}(X)X_0(X) \quad \text{and} \quad \sum_{X\in\mathfrak{G}} X_{00}(X)X_0(X)$$

are positive integral multiples of g or zero. Hence the following equalities are obtained from (13) and (14):

(15) $$\sum_{X\in\mathfrak{G}} \alpha(X)\beta(X) = g,$$

(16) $$\sum_{X\in\mathfrak{G}} X_{0_0}(X)X_0(X) = 0$$

and

(17) $$\sum_{X\in\mathfrak{G}} X_{00}(X)X_0(X) = g.$$

Now the form of decompositions of $\boldsymbol{b}^*$ and $\boldsymbol{d}^*$ into their irreducible components will be determined to a certain extent. At first, by the reciprocity theorem of Frobenius and by (10) the decompositions of $\boldsymbol{b}^*$ and $\boldsymbol{d}^*$ into their irreducible components have the following forms:

(18) $$\boldsymbol{b}^*(X) = X_0(X) + \cdots$$

for every permutation X of $\mathfrak{G}$, and

(19) $$\boldsymbol{d}^*(X) = X_0(X) + \cdots$$

for every permutation X of $\mathfrak{G}$, where the parts $\cdots\cdots$ do not contain X_0 any more.

LEMMA 1. *There are only two possible cases of the decomposition of* $\boldsymbol{b}^*$ *into the irreducible characters of* $\mathfrak{G}$:

(i) $$\boldsymbol{b}^*(X) = X_0(X) + (A,B)(X)$$

for every permutation X *of* $\mathfrak{G}$, *where the degree of* (A,B) *is equal to* $(q-2)p+1$;

(ii) $$\boldsymbol{b}^*(X) = X_0(X) + \sum_{i=1}^{s} (A,C)_i(X) + \sum_{i=1}^{s-1} (B,D)_i(X)$$

for every permutation X of $\mathfrak{G}$, where the degrees of $(A,C)_i$ $(i = 1,\cdots,s)$ and $(B,D)_i$ $(i = 1,\cdots,s-1)$ are equal to $(r-1)p+1$ with $\delta_q = -1$ and $p-1$, respectively.

Proof. Let Q be an element of $\mathfrak{G}$ of order q. Then by (1) and Proposition D we have that $X_0(Q) = 0$ and $\boldsymbol{b}^*(Q) = -1$. Therefore an irreducible character of $\mathfrak{G}$ of q-type B or q-type C with $\delta_q = -1$ must appear in the part $\cdots$ of (18). If it is of q-type B, then inspecting the degree table we get (i). So let us assume that it is of q-type C with $\delta_q = -1$. Then since $\boldsymbol{b}^*$ is, by Proposition D, a rational character, the whole family of the characters of q-type C will appear in the part $\cdots$ of (18). Hence inspecting the degree table we see that they have type (A,C), degree $(r-1)p+1$ and multiplicity 1. Now it is obtained that

$$\boldsymbol{b}^*(X) = X_0(X) + \sum_{i=1}^{s} (A,C)_i(X) + \cdots \tag{20}$$

for every permutation X of $\mathfrak{G}$, where the part $\cdots$ does not contain X_0 and $(A,C)_i$ $(i = 1,\cdots,s)$ any more.

Let P be an element of $\mathfrak{G}$ of order p. Then by Proposition B we have that $X_0(P) = -1$ and $(A,C)_i(P) = 1$ $(i = 1,\cdots,s)$. Moreover since P is not contained in any of p conjugate subgroups of $\mathfrak{H}$ in $\mathfrak{G}$ we have that $\boldsymbol{b}^*(P) = 0$. Therefore irreducible characters of $\mathfrak{G}$ of p-type B or p-type C with $\delta_p = -1$ must appear in the part $\cdots$ of (20) with the sum of multiplicities at least $s-1$. But the sum of degrees of the part $\cdots$ in (20) equals $(s-1)(p-1)$. Therefore it is seen from the degree table that only the characters (B,D) of degree $p-1$ can appear. Assume that some (B,D) appears with multiplicity $v > 1$. Then by the reciprocity theorem of Frobenius we have that

$$(B,D)(X) = v\boldsymbol{b}(X) + \cdots \tag{21}$$

for every permutation X of $\mathfrak{H}$. For $X = 1$ this gives that $2q = v(q-1) + \cdots$. Therefore we have that $v = 2$ and that the sum of degrees of the part $\cdots$ in (21) equals 2. If it contains a linear character λ of $\mathfrak{H}$, then it is clear that $\lambda \neq 1_{\mathfrak{H}}$. Then by the reciprocity theorem of Frobenius λ^* is decomposed into the sum of (B,D) and a linear character of $\mathfrak{G}$, which is clearly different from $1_{\mathfrak{G}}$. This contradicts the simplicity of $\mathfrak{G}$. If it is an irreducible character τ of degree two, then by the reciprocity theorem of Frobenius we have that

$$\tau^*(X) = (B,D)(X) + \cdots \tag{22}$$

for every permutation X of $\mathfrak{G}$. Since the sum of degrees of the part $\cdots$ in (22) equals $p+1$, we see from the degree table that this part must be irreducible. But since $p+1 \equiv 2 \pmod{q}$, this character must have q-type C. Therefore the equality $(r-1)p+1 = p+1$ is obtained. Thus we have that $r = 2$. Then by a previous result [10, Theorem 2] $\mathfrak{G}$ is isomorphic to $LF(2,11)$ with $p = 11$, contradicting the assumption $p > 11$. Therefore all the (B,D)'s appear with multiplicity 1. Thus we get (ii).

LEMMA 2. *There are four possible cases of the decomposition of* $\boldsymbol{d}^*$ *into the irreducible characters of* $\mathfrak{G}$:

$$\text{(i)} \qquad \boldsymbol{d}^*(X) = X_0(X) + (A,D)(X)$$

for every permutation X *of* $\mathfrak{G}$, *where the degree of* (A,D) *is equal to* $(q-1)p+1$;

$$\text{(ii)} \qquad \boldsymbol{d}^*(X) = X_0(X) + (A,B)(X) + (D,A)(X)$$

for every permutation X *of* $\mathfrak{G}$, *where the degrees of* (A,B) *and* (D,A) *are equal to* $(q-2)p+1$ *and* p, *respectively*;

$$\text{(iii)} \qquad \boldsymbol{d}^*(X) = X_0(X) + \sum_{i=1}^{s} (A,C)_i(X) + (B,A)(X) + \sum v_j(B,D)_j(X)$$

for every permutation X *of* $\mathfrak{G}$, *where the degrees of* $(A,C)_i$ $(i = 1,\cdots,s)$, (B,A) *and* $(B,D)_j$*'s are equal to* $(r-1)p+1$, $2p-1$ *and* $p-1$, *respectively. Furthermore* v_j*'s are positive integers not greater than two, whose sum is equal to* $s-2$;

$$\text{(iv)} \qquad \boldsymbol{d}^*(X) = X_0(X) + \sum_{i=1}^{s} (A,C)_i(X) + (D,A)(X) + \sum v_j(B,D)_j(X)$$

for every permutation X *of* $\mathfrak{G}$, *where the degrees of* $(A,C)_i$ $(i = 1,\cdots,s)$, (D,A) *and* $(B,D)_j$*'s are equal to* $(r-1)p+1$, p *and* $p-1$, *respectively. Furthermore* v_j*'s are positive integers not greater than two, whose sum is equal to* $s-1$.

Proof. Let P be an element of $\mathfrak{G}$ of order p. Then by (1) we have that $X_0(P) = -1$. Since P is not contained in any of p conjugate subgroups of $\mathfrak{H}$ in $\mathfrak{G}$, we have that $\boldsymbol{d}^*(P) = 0$. Hence an irreducible character of $\mathfrak{G}$ of p-type A or p-type C with $\delta_p = 1$ must appear in the part $\cdots$ of (19). Then inspecting the degree table we see that no irreducible character of p-type C with $\delta_p = 1$ can appear. Now if it is (A,D), then we get (i). If it is (A,B), then it is easy to see that we get (ii). Hence let us assume that it has type (A,C). Since by Proposition D, $\boldsymbol{d}^*$ is a rational character, the whole family of the characters of q-type C will appear in the part $\cdots$ of (19). Now inspecting the degree table we see that $\delta_q = -1$ and that they have degree $(r-1)p+1$ and multiplicity 1. Thus we have that

$$(23) \qquad \boldsymbol{d}^*(X) = X_0(X) + \sum_{i=1}^{s} (A,C)_i(X) + \cdots$$

for every permutation X of $\mathfrak{G}$, where the part $\cdots$ does not contain X_0 and $(A,C)_i$ $(i = 1,\cdots,s)$ any more. By Proposition B we have that $\sum_{i=1}^{s}(A,C)_i(P) = s$. Therefore irreducible characters of $\mathfrak{G}$ of p-type B or p-type C with $\delta_p = -1$ must appear in the part $\cdots$ of (23) with the sum of multiplicities at least $s-1$. But the sum of degrees ofthe part $\cdots$ of (23) equals $(s-1)(p-1)+p$. Hence checking up the degree table we see that no character of p-type C with $\delta_p = -1$ can appear, and that at most one character (B,A) with degree $2p-1$ can appear. If it actually appears, we get (iii). Otherwise only characters of type (B,D), whose degrees are $p-1$, appear with the sum of multiplicities $s-1$. Hence we obtain that

$$\mathbf{d}^*(X) = X_0(X) + \sum_{i=1}^{s}(A,C)_i(X) + \sum v_j(B,D)_j(X) + \cdots \tag{24}$$

for every permutation X of $\mathfrak{G}$, where $\sum v_j = s-1$.

Let Q be an element of $\mathfrak{G}$ of order q. Then by (1) and Propositions B and D we have that $\mathbf{d}^*(Q) = 0$, $X_0(Q) = 0$, $\sum_{i=1}^{s}(A,C)_i(Q) = -1$ and $(B,D)_j(Q) = 0$ for every j. Therefore an irreducible character of $\mathfrak{G}$ of q-type A must appear in the part $\cdots$ of (24). But since the sum of degrees of the part $\cdots$ of (24) equals p, it must be (D,A) with degree p. Thus we get (iv).

The fact that v_j's are not greater than two is obvious by the reciprocity theorem of Frobenius.

Lemma 3. *Case* (i) *in Lemma* 2 *cannot occur.*

Proof. Let us assume that case (i) in Lemma 2 occurs. Then from (11) we have that $X_{0_0} = (A,D)$. Thus

$$X_{0_0} \text{ restricted on } \mathfrak{G}$$

is irreducible. By a theorem of Tsuzuku [14] this implies the triple transitivity of $\mathfrak{G}$, contradicting the assumption.

Before proceeding the same way further, let us consider two kinds of new permutation representations of $\mathfrak{G}$. The first of them is as follows. Let $\{\Omega\}_2$ be the family of all the subsets of Ω each of which consists of two (different) symbols of Ω. Then since $\mathfrak{G}$ is a permutation group on Ω, we can consider $\mathfrak{G}$ as a permutation group $\pi\{\mathfrak{G}\}$ on $\{\Omega\}_2$. Since $\mathfrak{G}$ is doubly transitive on Ω, $\pi\{\mathfrak{G}\}$ is transitive on $\{\Omega\}_2$. Furthermore since $\mathfrak{G}$ is simple, $\pi\{\mathfrak{G}\}$ is faithful. It is easy to see that the maximal subgroup of $\pi\{\mathfrak{G}\}$ leaving the symbol $\{1, 2\}$ of $\{\Omega\}_2$ fixed coincides with $Ns\mathfrak{K}$. The second of them is as follows. Let $(\Omega)_2$ be the set of all the ordered pairs (x,y) such that x and y are different symbols of Ω. Then we can consider $\mathfrak{G}$ as a permutation group $\pi(\mathfrak{G})$ on $(\Omega)_2$. Since $\mathfrak{G}$ is doubly transitive, $\pi(\mathfrak{G})$ is transitive on $(\Omega)_2$. Furthermore since $\mathfrak{G}$ is simple, $\pi(\mathfrak{G})$ is faithful. It is easy to see that the maximal subgroup of $\pi(\mathfrak{G})$ leaving the symbol $(1, 2)$ of $(\Omega)_2$ fixed coincides with $\mathfrak{K}$. Now a symbol $\{x,y\}$ of $\{\Omega\}_2$ can be considered as the set of two symbols (x,y) and (y,x) of $(\Omega)_2$. In this sense we can prove the following lemma.

Lemma 4. *An orbit of $Ns\mathfrak{K}$ as a subgroup of $\pi\{\mathfrak{G}\}$ is decomposed into at most four orbits of $\mathfrak{K}$ as a subgroup of $\pi(\mathfrak{G})$.*

Proof. Since by assumption $\mathfrak{H}$ is primitive on $\Omega - \{1\}$, using a theorem of Witt [17] we see that $\mathfrak{K}$ fixes just two symbols 1 and 2 of Ω. Thus the index of $\mathfrak{K}$ in $Ns\mathfrak{K}$ equals two. Now let S be an orbit of $Ns\mathfrak{K}$ as a subgroup of $\pi\{\mathfrak{G}\}$. Then it is clear that S is decomposed into at most two orbits of $\mathfrak{K}$ as a subgroup of $\pi\{\mathfrak{G}\}$. Now let T be an orbit of $\mathfrak{K}$ as a subgroup of $\pi\{\mathfrak{G}\}$. Then in the sense stated above T is a set of orbits of $\mathfrak{K}$ as a subgroup of $\pi(\mathfrak{G})$. Let U be an orbit of $\mathfrak{K}$ as a subgroup of $\pi(\mathfrak{G})$, which is contained in T, and U^S be the symmetrization of U, namely the set of all the ordered pairs (x,y) of $(\Omega)_2$ such that (y,x) belongs to U. Then U^S is also an orbit of $\mathfrak{K}$ as a subgroup of $\pi(\mathfrak{G})$. Now we want to show that T equals the set of U and U^S. Let us suppose that there exists an ordered pair (x,y) from T, which is not contained in U. Let (a,b) be an ordered pair of U. Then there exists a permutation K of $\mathfrak{K}$ which transfers $\{x,y\}$ into $\{a,b\}$. Then we see that K transfers (y,x) into (a,b). Hence (y,x) belongs to U and, therefore, (x,y) belongs to U^S as required.

Now it is known [5, §207] that the number of orbits of $\mathfrak{K}$ as a subgroup of $\pi(\mathfrak{G})$ equals the norm of $1^*_{\mathfrak{K}}$, and by (8) it equals the norm of $1_{\mathfrak{G}} + 2X_0 + X^0_0 + X_{00}$ restricted on $\mathfrak{G}$. Similarly the number of orbits of $Ns\mathfrak{K}$ as a subgroup of $\pi\{\mathfrak{G}\}$ equals the norm of $1^*_{Ns\mathfrak{K}}$, and by (9) it equals the norm of $1_{\mathfrak{G}} + X_0 + X_{00}$ restricted on $\mathfrak{G}$.

The following lemma can be implied from Proposition D.

Lemma 5. $2r - 2 \leqq s$.

Proof. By Proposition D there exists a positive integer m such that $2q = m^2 + 1$. Furthermore by Proposition D, $\Omega - \{1\}$ is decomposed into three orbits of $\mathfrak{K}$, $\{2\}$ and, say, Γ_1 and Γ_2, where the lengths of Γ_1 and Γ_2 are equal to $\frac{1}{2}m(m+1)$ and $\frac{1}{2}m(m-1)$, respectively. Now let us consider $Ns\mathfrak{Q} = \mathfrak{Q}\mathfrak{N}$. Since $\mathfrak{G}$ is doubly transitive, we can choose $\mathfrak{N}$ to fix the symbols 1 and 2 of Ω individually. Then $\mathfrak{N}$ also fixes Γ_1 and Γ_2 as a whole. On the other hand, $\mathfrak{N}$ fixes just one more symbol, say 3, of Ω. If 3 belongs to Γ_2, then any element $(\neq 1)$ of $\mathfrak{N}$ does not leave any symbol of Γ_1 fixed. Hence we have that $\frac{1}{2}m(m+1) \equiv 0 \pmod{r}$. On the other hand, since $Cs\mathfrak{Q} = \mathfrak{Q}$, we have, by a theorem of Sylow, that $q \equiv 1 \pmod{r}$, namely $\frac{1}{2}(m^2+1) \equiv 1 \pmod{r}$. Therefore we obtain that $\frac{1}{2}(m+1) \equiv 0 \pmod{r}$. But since

$$s = (q-1)/r = (m-1)\{(m+1)/2r\},$$

we have that $s \geqq m - 1 \geqq 2r - 2$. Similarly if 3 belongs to Γ_1, then we have that $\frac{1}{2}(m-1) \equiv 0 \pmod{r}$ and that $s = (q-1)/r = (m+1)\{(m-1)/2r\}$. Thus we have that $s \geqq m + 1 \geqq 2r + 2$.

Lemma 6. *X_{00} restricted on $\mathfrak{G}$ does not contain an irreducible character of type (A,B) of degree $(q-2)p+1$ as its irreducible component.*

Proof. Assume that Lemma 6 is false. Then we have that

$$X_{00}(X) = X_0(X) + (A,B)(X) \tag{25}$$

for every permutation X of $\mathfrak{G}$. Hence the number of orbits of $Ns\mathfrak{K}$ as a subgroup of $\pi\{\mathfrak{G}\}$ equals six. Therefore by Lemma 4 the number of orbits of $\mathfrak{K}$ as a subgroup of $\pi(\mathfrak{G})$ is at most twenty-four. Now let us assume that either case (ii) of Lemma 1 or case (iii) of Lemma 2 or case (iv) of Lemma 2 occurs. Then by [11] we see that

$$\underset{0}{X_0} \text{ restricted on } \mathfrak{G}$$

contains all the $(A,C)_i$ $(i = 1,\cdots,s)$ and all the $(B,D)_j$'s as its irreducible components. Then using [11] we see that the norm of $1^*_{\mathfrak{K}}$ is at least $2s + 9$. Therefore we obtain that $s \leqq 7$. Now by Lemma 5 we have that $r \leqq 4$. Together with $2q = m^2 + 1$ these facts imply that $q = 5$ and $p = 11$, contradicting the assumption. Therefore under (25) case (i) of Lemma 1 and case (ii) of Lemma 2 must occur. Therefore by [11] we have that

$$\underset{0}{X_0}(X) = (A,B)_1(X) + (D,A)(X) \tag{26}$$

for every permutation X of $\mathfrak{G}$, where the degrees of $(A,B)_1$ and (D,A) are equal to $(q-2)p+1$ and p, respectively.

Now $\mathfrak{K}$ as a subgroup of $\pi(\mathfrak{G})$ possesses at least fourteen orbits, namely $(1,2)$, $(2,1)$, $(1,\Gamma_1)$, $(\Gamma_1,1)$, $(2,\Gamma_1)$, $(\Gamma_1,2)$, $(1,\Gamma_2)$, $(\Gamma_2,1)$, $(2,\Gamma_2)$, $(\Gamma_2,2)$ and at least four orbits from (Γ_1,Γ_2), (Γ_2,Γ_1), $(\Gamma_1)_2$ and $(\Gamma_2)_2$. If $(A,B) \neq (A,B)_1$, then the norm of $1^*_{\mathfrak{K}}$ equals only thirteen. This is a contradiction. Therefore it must be $(A,B) = (A,B)_1$. Then the norm of $1^*_{\mathfrak{K}}$ equals fifteen. Hence only one of (Γ_1,Γ_2), (Γ_2,Γ_1), $(\Gamma_1)_2$ and $(\Gamma_2)_2$ is decomposed into two orbits of $\mathfrak{K}$ as a subgroup of $\pi(\mathfrak{G})$. If $\mathfrak{K}$ as a subgroup of $\pi(\mathfrak{G})$ is intransitive on (Γ_1,Γ_2) or on (Γ_2,Γ_1), then it is also intransitive on (Γ_2,Γ_1) or on (Γ_1,Γ_2), respectively. Hence it is transitive both on (Γ_1,Γ_2) and on (Γ_2,Γ_1). If $\mathfrak{K}$ as a subgroup of $\pi(\mathfrak{G})$ is transitive on $(\Gamma_1)_2$, $\mathfrak{K}$ is doubly transitive on Γ_1. Since by assumption $\mathfrak{H}$ is uniprimitive on $\Omega - \{1\}$, by Proposition E there must exist an orbit of $\mathfrak{K}$, whose length is greater than $\frac{1}{2}m(m+1)$. It is absurd. Hence $\mathfrak{K}$ as a subgroup of $\pi(\mathfrak{G})$ is intransitive on $(\Gamma_1)_2$, and, therefore, it is transitive on $(\Gamma_2)_2$. Let us assume that $(\Gamma_1)_2$ is decomposed into two orbits W_1 and W_2 of $\mathfrak{K}$ as a subgroup of $\pi(\mathfrak{G})$. Since $\mathfrak{K}$ is transitive on Γ_1, the lengths of W_1 and W_2 are multiples of $\frac{1}{2}m(m+1)$. Let these lengths be $\frac{1}{2}m(m+1)w_1$ and $\frac{1}{2}m(m+1)w_2$, respectively. Then we have that

$$w_1 + w_2 = \tfrac{1}{2}m(m+1) - 1 = \tfrac{1}{2}(m+2)(m-1). \tag{27}$$

Now by Proposition F we have that

$$N = \{p(p-1)\}^{13}\{\tfrac{1}{2}m(m+1)\}^4\{\tfrac{1}{2}m(m-1)\}^4\,\tfrac{1}{2}m(m-1)\{\tfrac{1}{2}m(m-1)-1\}$$
$$\cdot\ \{\tfrac{1}{2}m(m-1)\}^2\{\tfrac{1}{2}m(m+1)\}^2 w_1w_2\{\tfrac{1}{2}m(m+1)\}^2$$

is divisible by

$$D = (p-1)^9\{(q-2)p+1\}^4 p.$$

Put $F = N/D$. Dividing F by q^4p^{12} we have that

$$\begin{aligned} F_1 &= 2^4\{\tfrac{1}{2}m(m+1)\}^8\{\tfrac{1}{2}m(m-1)\}^7\{\tfrac{1}{2}m(m-1)-1\}w_1w_2/\{(q-2)p+1\}^4 \\ &= m^{15}(m+1)^9(m-1)^7(m-2)w_1w_2/2^8(m^4-m^2-4)^4 \end{aligned}$$

is an integer. Since m is odd, dividing F_1 by m^{15} we have that

$$F_2 = (m+1)^9(m-1)^7(m-2)w_1w_2/2^8(m^4-m^2-4)^4$$

is an integer. Let l be an odd prime divisor of m^2-1. Then $m^4-m^2-4 \equiv -4 \pmod{l}$. Hence l is relatively prime to m^4-m^2-4. Put $m-1 = 2^AB$ and $m+1 = 2^CD$, where B and D are odd. Let l_1 be any prime divisor of $m-2$. Then $m^4-m^2-4 \equiv 8 \pmod{l_1}$. Since l_1 is odd, this shows that l_1 is relatively prime to m^4-m^2-4. Hence dividing F_2 by $B^9D^7(m-2)$ we have that

$$F_3 = 2^{9C+7A-8}w_1w_2/(m^4-m^2-4)^4$$

is an integer. Since $m^4-m^2-4 = m^2(m+1)(m-1)-4$, m^4-m^2-4 is divisible by 4 and not by 8. Hence dividing F_3 by $2^{9C+7A-16}$ we have that

$$F_4 = w_1w_2/\{\tfrac{1}{4}(m^4-m^2-4)\}^4$$

is an integer. By (27) this implies, in particular, that

$$\tfrac{1}{4}(m+2)^2(m-1)^2 > \{\tfrac{1}{4}(m^4-m^2-4)\}^4.$$

Now the following series of implications can be easily seen:

$$\begin{aligned} 4^3(m+2)^2(m-1)^2 &> (m^4-m^2-4)^4 > (m^4-m^2-6)^4 \\ &= (m^2-3)^4(m^2+2)^4, \\ 4^2(m+2)(m-1) &> (m^2-3)^2(m^2+2)^2, \\ 4(m+2) &> (m^2-3)(m^2+2), \\ 4 &> m^2-3. \end{aligned}$$

Hence we obtain that $m < 3$ and $p < 11$, contradicting the assumption.

Lemma 7. *Case* (i) *of Lemma* 1 *and case* (ii) *of Lemma* 2 *cannot occur.*

Proof. If either of these cases occurs, then by (11) X_0 restricted on $\mathfrak{G}$ or

0

X_{00} restricted on $\mathfrak{G}$ must contain an irreducible character of type (A,B) of degree $(q-2)p+1$ as an irreducible component. By Lemma 6 X_{00} restricted on $\mathfrak{G}$ cannot contain such an irreducible character as an irreducible component. Therefore $\underset{0}{X_0}$ restricted on $\mathfrak{G}$ must contain (A,B) of degree $(q-2)p+1$. Hence we have that

$$\underset{0}{X_0}(X) = (A,B)(X) + (D,A)(X) \tag{28}$$

for every permutation X of $\mathfrak{G}$, where the degree of (D,A) is p, and

$$X_{00}(X) = X_0(X) + \sum_{i=1}^{s} (A,C)_i(X) + \cdots \tag{29}$$

for every permutation X of $\mathfrak{G}$, where the part $\cdots$ in (29) does not contain X_0 and $(A,C)_i$ $(i=1,\cdots,s)$ any more.

Let P be an element of $\mathfrak{G}$ of order p. Then by (1), (3) and Proposition B we have that $X_{00}(P)=0$, $X_0(P)=-1$ and $\sum_{i=1}^{s}(A,C)_i(P)=s$. Therefore irreducible characters of $\mathfrak{G}$ of p-type B or p-type C with $\delta_p=-1$ must appear in the part $\cdots$ of (29) with the sum of multiplicities at least $s-1$. But the sum of degrees of the part $\cdots$ of (29) is $(s-1)(p-1)$. Hence only the characters of type (B,D) with degree $p-1$ can appear in the part $\cdots$ of (29). Thus (D,A) does not appear in (29). Then the difference of the norms of $1^*_{\mathfrak{K}}$ and $1^*_{Ns\mathfrak{K}}$ is just seven. On the other hand, this difference is equal to the difference of the number of orbits of $\mathfrak{K}$ as a subgroup of $\pi(\mathfrak{G})$ and the number of orbits of $Ns\mathfrak{K}$ as a subgroup of $\pi\{\mathfrak{G}\}$. Now the orbit $\{1,2\}$ of $Ns\mathfrak{K}$ as a subgroup of $\pi\{\mathfrak{G}\}$ contains two orbits $(1,2)$ and $(2,1)$ of $\mathfrak{K}$ as a subgroup of $\pi(\mathfrak{G})$. The same things hold between four orbits $(1,\Gamma_1)$, $(\Gamma_1,1)$, $(2,\Gamma_1)$, $(\Gamma_1,2)$ and for another four orbits $(1,\Gamma_2)$, $(\Gamma_2,1)$, $(2,\Gamma_2)$, $(\Gamma_2,2)$ of $\mathfrak{K}$ as a subgroup of $\pi(\mathfrak{G})$. Thus we have already seven differences. But any orbit of $Ns\mathfrak{K}$ as a subgroup of $\pi\{\mathfrak{G}\}$ from $\{\Gamma_1,\Gamma_2\}$ contains at least two orbits of $\mathfrak{K}$ as a subgroup of $\pi(\mathfrak{G})$, namely, one, which is contained in (Γ_1,Γ_2) and the other, which is contained in (Γ_2,Γ_1). This is a contradiction.

Now by Lemmas 1 and 2 we obtain that

$$\boldsymbol{b}^*(X) = X_0(X) + \sum_{i=1}^{s} (A,C)_i(X) + \sum_{i=1}^{s-1} (B,D)_i(X) \tag{30}$$

for every permutation X of $\mathfrak{G}$, and

$$\begin{aligned} \boldsymbol{d}^*(X) &= X_0(X) + \sum_{i=1}^{s} (A,C)_i(X) + (D,A)(X) \\ &\quad + 2\sum^{t} (B,D)_j(X) + \sum^{u} (B,D)_k(X) \end{aligned} \tag{31.1}$$

for every permutation X of $\mathfrak{G}$, or

$$(31.2)\qquad \begin{aligned} \boldsymbol{d}^*(X) = X_0(X) + \sum_{i=1}^{s}(A,C)_i(X) + (B,A)(X) \\ + \; 2\sum^{t}(B,D)_j(X) + \sum^{u}(B,D)_k(X) \end{aligned}$$

for every permutation X of $\mathfrak{G}$, where $2t+u=s-1$ in (31.1) and $2t+u=s-2$ in (31.2).

We say that (B,D) in $2\sum^t(B,D)_j$ has type $2\boldsymbol{d}$, and that (B,D) in $\sum^u(B,D)_k$ has type $\boldsymbol{d}$. They are different, because by the reciprocity theorem of Frobenius (B,D) restricted on $\mathfrak{H}$ equals $2\boldsymbol{d}$, if it has type $2\boldsymbol{d}$, and conversely. Furthermore we say that (B,D) in (30) has type $\boldsymbol{b}$.

Lemma 8. *(B,D) of type $\boldsymbol{b}$ cannot be of type $\boldsymbol{d}$ nor of type $2\boldsymbol{d}$.*

Proof. If (B,D) has type $\boldsymbol{b}$, then by the reciprocity theorem of Frobenius (B,D) restricted on $\mathfrak{H}$ contains $\boldsymbol{b}$ as its irreducible component. Hence it cannot be of type $2\boldsymbol{d}$. If it has type $\boldsymbol{d}$, then $\boldsymbol{d}$ also appears as an irreducible component of (B,D) restricted on $\mathfrak{H}$. Therefore (B,D) restricted on $\mathfrak{H}$ contains a linear character λ, which is clearly different from $1_{\mathfrak{H}}$. By the reciprocity theorem of Frobenius λ^* contains (B,D) as its irreducible component. Hence λ^* contains a linear character of $\mathfrak{G}$, which is clearly different from $1_{\mathfrak{G}}$, contradicting the simplicity of $\mathfrak{G}$.

From the proof of Lemma 7 we obtain that

$$(32)\qquad \begin{aligned} X_{00}(X) = X_0(X) + \sum_{i=1}^{s}(A,C)_i(X) + \sum^{s(1)}(B,D)_i(X) \\ + \; 2\sum^{t(1)}(B,D)_j(X) + \sum^{t(3)}(B,D)_k(X) + \sum^{u(1)}(B,D)_l(X) \end{aligned}$$

for every permutation X of $\mathfrak{G}$, where (B,D) in $\sum^{s(1)}(B,D)_i$ has type $\boldsymbol{b}$, (B,D) in $2\sum^{t(1)}(B,D)_j$ has type $2\boldsymbol{d}$ and does not appear in $\underset{0}{X_0}$ restricted on $\mathfrak{G}$, (B,D) in $\sum^{t(3)}(B,D)_k$ has type $2\boldsymbol{d}$ and appears also in $\underset{0}{X_0}$ restricted on $\mathfrak{G}$ and (B,D) in $\sum^{u(1)}(B,D)_l$ has type $\boldsymbol{d}$.

Furthermore we have that

$$(33)\qquad s(1)+2t(1)+t(3)+u(1) = s-1\,.$$

On the other hand, by (11) we obtain that

$$(34.1)\qquad \begin{aligned} \underset{0}{X_0}(X) = \sum_{i=1}^{s}(A,C)_i(X) + (D,A)(X) + \sum^{s(2)}(B,D)_i(X) \\ + \; 2\sum^{t(2)}(B,D)_j(X) + \sum^{t(3)}(B,D)_k(X) + \sum^{u(2)}(B,D)_l(X) \end{aligned}$$

for every permutation X of $\mathfrak{G}$, or

$$\underset{0}{X_0}(X) = \sum_{i=1}^{s}(A,C)_i(X) + (B,A)(X) + \sum^{s(2)}(B,D)_i(X) \tag{34.2}$$
$$+ 2\sum^{t(2)}(B,D)_j(X) + \sum^{t(3)}(B,D)_k(X) + \sum^{u(2)}(B,D)_l(X)$$

for every permutation X of $\mathfrak{G}$, where (B,D) in $\sum^{s(2)}(B,D)_i$ has type $\boldsymbol{b}$, (B,D) in $2\sum^{t(2)}(B,D)_j$ has type $2\boldsymbol{d}$ and does not appear in X_{00} restricted on $\mathfrak{G}$, (B,D)'s in $\sum^{t(3)}(B,D)_k$ are the same as those in (32) and (B,D) in $\sum^{u(2)}(B,D)_l$ has type $\boldsymbol{d}$.

Furthermore we have that

$$s(2) + 2t(2) + t(3) + u(2) = s - 1 \tag{35.1}$$

or

$$s(2) + 2t(2) + t(3) + u(2) = s - 2. \tag{35.2}$$

(31.1), (34.1) and (35.1) correspond with each other. On the other hand, (31.2), (34.2) and (35.2) correspond with each other. Moreover we have that

$$s(1) + s(2) = s - 1, \tag{36}$$

$$t(1) + t(2) + t(3) = t \tag{37}$$

and

$$u(1) + u(2) = u. \tag{38}$$

LEMMA 9. *r must be odd.*

Proof. Let us assume that r is even. Take an involution I in $\mathfrak{N}$. Then we have that $\alpha(I) = 3$ and $\beta(I) = q - 1$. Now since (B,D) has degree $2q$, by a theorem of Brauer [2] it contains two linear characters on $Ns\mathfrak{Q}$. Therefore we have that

$$-2 \leqq (B,D)(I) \leqq 2. \tag{39}$$

Similarly we obtain that

$$-3 \leqq (D,A)(I) \leqq 3 \tag{40.1}$$

and

$$-5 \leqq (B,A)(I) \leqq 5. \tag{40.2}$$

By Proposition B we can put $(A,C)_i(I) = x$ for $i = 1,\cdots,s$. Then from (32), (1), (3), (33) and (39) we obtain that

$$q - 1 \leqq 2 + sx + 2(s-1),$$

which implies that

$$r - 2 \leqq x. \tag{41}$$

On the other hand, from (34.1), (2), (40.1), (35.1) and (39) or from (34.2), (2), (40.2), (35.2) and (39) we obtain that

$$2 - q \leqq sx - 3 - 2(s-1),$$

which implies that

$$(3-q)/s + 2 \geqq x. \tag{42}$$

From (41) and (42) we obtain that

$$(3-q)/s + 2 \geqq r - 2,$$

which implies that

$$(1/s) + 2 \geqq r.$$

Thus we obtain that $2 \geqq r$ and hence $r = 2$. Then by a previous result [11, Theorem 2] this implies that $p \leqq 11$, contradicting the assumption.

Lemma 9 has two important consequences, which are the following lemmas.

Lemma 10. $s \equiv 0 \pmod 4$.

Proof. Since $q - 1 = rs$, by Lemma 9 we have only to show that $q \equiv 1 \pmod 4$. By Proposition D there exists an odd integer $2m_1 + 1$ such that $2q = (2m_1 + 1)^2 + 1$. This implies that $q - 1 = 2m_1(m_1 + 1)$.

Lemma 11. *$(A,C)_i$ is not a real character. Hence the quadratic signature of $(A,C)_i$ is zero $(i = 1,\cdots,s)$.*

Proof. $\mathfrak{Q}\mathfrak{R}$ possesses s irreducible characters $c_1,\cdots,c_s$ of degree r. Now it is well known that the number of real irreducible characters is equal to the number of classes of conjugate real elements. By Lemma 9 the order of $\mathfrak{Q}\mathfrak{R}$ is odd. Therefore the identity is the only real element in $\mathfrak{Q}\mathfrak{R}$. Obviously $1^{\mathfrak{Q}\mathfrak{R}}$ is a real character. Hence c_i is not a real character. By a theorem of Brauer-Nesbitt [1] c_i vanishes at every element $(\neq 1)$ of order dividing r $(i = 1,\cdots,s)$. Hence $c_i(Q_i)$ must be not real for some element Q_i $(\neq 1)$ of $\mathfrak{Q}$. On the other hand, from the property of exceptional characters (13) we can assume that $(A,C)_i + c_i$ or $(A,C)_i - c_i$ takes a rational value at every element of $\mathfrak{Q}\mathfrak{R}$. Therefore $(A,C)_i$ is not a real character $(i = 1,\cdots,s)$.

Now from (32), (33), (34.1), (34.2), (35.1) and (35.2) we obtain that

$$(*.1)\qquad \begin{aligned} (1/g) \sum_{X \in \mathfrak{G}} [\tfrac{1}{2}\alpha(X)\{\alpha(X) - 3\} + \beta(X)]^2 &= 2s + 2t(1), \\ (1/g) \sum_{X \in \mathfrak{G}} [\tfrac{1}{2}\{\alpha(X) - 1\}\{\alpha(X) - 2\} - \beta(X)]^2 &= 2s + 2t(2), \end{aligned}$$

or

$$(*.2)\qquad (1/g) \sum_{X \in \mathfrak{G}} [\tfrac{1}{2}\{\alpha(X) - 1\}\{\alpha(X) - 2\} - \beta(X)]^2 = 2s + 2t(2) - 1,$$

where (*,1) and (*.2) correspond to (34.1), (35.1) and (34.2), (35.2), respectively, and

$$(1/g)\sum_{X\in\mathfrak{G}}\,[\tfrac{1}{2}\alpha(X)\{\alpha(X)-3\}+\beta(X)][\tfrac{1}{2}\{\alpha(X)-1\}\{\alpha(X)-2\}-\beta(X)]=s+t(3).$$

By (4), (5), (6), (12) and (15) these equalities are transformed into the following forms:

$$(43)\qquad (1/g)\sum_{X\in\mathfrak{G}}\{\alpha(X)\}^4+(4/g)\sum_{X\in\mathfrak{G}}\{\alpha(X)\}^2\beta(X)+(4/g)\sum_{X\in\mathfrak{G}}\{(\beta X)\}^2$$
$$=8s+8t(1)+30,$$

$$(44.1)\qquad (1/g)\sum_{X\in\mathfrak{G}}\{\alpha(X)\}^4-(4/g)\sum_{X\in\mathfrak{G}}\{\alpha(X)\}^2\beta(X)+(4/g)\sum_{X\in\mathfrak{G}}\{\beta(X)\}^2$$
$$=8s+8t(2)+10,$$

or

$$(44.2)\qquad (1/g)\sum_{X\in\mathfrak{G}}\{\alpha(X)\}^4-(4/g)\sum_{X\in\mathfrak{G}}\{\alpha(X)\}^2\beta(X)+(4/g)\sum_{X\in\mathfrak{G}}\{\beta(X)\}^2$$
$$=8s+8t(2)+6,$$

where (44.1) and (44.2) correspond to (*.1) and (*.2), respectively, and

$$(45)\qquad (1/g)\sum_{X\in\mathfrak{G}}\{\alpha(X)\}^4-(4/g)\sum_{X\in\mathfrak{G}}\{\beta(X)\}^2=4s+4t(3)+18.$$

From (43), (44.1) and (45) we obtain that

$$(46.1)\qquad (4/g)\sum_{X\in\mathfrak{G}}\{\beta(X)\}^2=2s+2t(1)+t(2)-t(3)+1.$$

Similarly from (43), (44.2) and (45) we obtain that

$$(46.2)\qquad (2/g)\sum_{X\in\mathfrak{G}}\{\beta(X)\}^2=s+t(1)+t(2)-t(3).$$

Now we can prove the following lemma, which is implied from Proposition G.

Lemma 12. *There exists a* (B,D) *of type* $2d$.

Proof. Let X be a generalized character of a finite group $\mathfrak{X}$. We define the trace of X as the (algebraic) sum of the multiplicities of irreducible components of X. Then by (8), (31)–(38) the trace of $1_{\mathfrak{R}}^*$ equals $4s+3$ (case of (31.1)–(46.1)) or $4s+2$ (case of (31.2)–(46.2)). Let m_i be the sum of multiplicities of irreducible components in $1_{\mathfrak{R}}^*$ with the quadratic signature i $(i=1,0,-1)$. Then we have that

$$(47.1)\qquad m_1+m_0+m_{-1}=4s+3$$

or

$$(47.2) \qquad m_1 + m_0 + m_{-1} = 4s + 2.$$

Now by Proposition G the number R of real orbits of $\mathfrak{K}$ as a subgroup of $\pi(\mathfrak{G})$ can be calculated as follows:

$$\begin{aligned} R &= (1/g) \sum_{X \in \mathfrak{G}} 1^*_{\mathfrak{K}}(X^2) = (1/g) \sum_{X \in \mathfrak{G}} \alpha(X^2)\{\alpha(X^2) - 1\} \\ &= (1/g) \sum_{X \in \mathfrak{G}} \{\alpha(X) + 2\beta(X)\}\{\alpha(X) + 2\beta(X) - 1\} \\ &= (4/g) \sum_{X \in \mathfrak{G}} \{\beta(X)\}^2 + 4 \end{aligned}$$

by (4), (5), (6) and (15)

$$= m_1 - m_{-1}.$$

Using (46.1) or (46.2) we obtain that

$$(48.1) \qquad m_1 - m_{-1} = 2s + 2t(1) + t(2) - t(3) + 5$$

or

$$(48.2) \qquad m_1 - m_{-1} = 2s + 2t(1) + t(2) - t(3) + 4.$$

Now by Lemma 11 we have that $m_0 \geqq 2s$. Therefore we obtain that

$$(49.1) \qquad m_1 + m_{-1} \leqq 2s + 3$$

or

$$(49.2) \qquad m_1 + m_{-1} \leqq 2s + 2.$$

Now let us assume that Lemma 12 is false. Then the number t in (31.1) or (31.2) is zero and, therefore, $t(1)$, $t(2)$ and $t(3)$ are all zero. But then from (48.1), (49.1) or (48.2), (49.2) we get a contradiction.

So let $(B,D)_0$ be an irreducible character of $\mathfrak{G}$ of type $2\boldsymbol{d}$.

Let $\mathfrak{M}$ be a minimal normal subgroup of $\mathfrak{H}$. Since $\mathfrak{H}$ is primitive on $\Omega - \{1\}$, $\mathfrak{M}$ is transitive on $\Omega - \{1\}$ and the index of $\mathfrak{K} \cap \mathfrak{M}$ in $\mathfrak{M}$ equals $2q$. In particular, $\mathfrak{M}$ contains $\mathfrak{Q}$. As a minimal normal subgroup $\mathfrak{M}$ is a direct product of mutually isomorphic simple groups. Since the order of $\mathfrak{Q}$ is equal to q, $\mathfrak{M}$ itself must be simple. Using a theorem of Sylow we have that $\mathfrak{H} = (Ns\mathfrak{Q} \cap \mathfrak{H})\mathfrak{M}$, which implies that $\mathfrak{H}/\mathfrak{M} \cong \mathfrak{Q}\mathfrak{N}/\mathfrak{Q}(\mathfrak{N} \cap \mathfrak{M}) \cong \mathfrak{N}/\mathfrak{N} \cap \mathfrak{M}$. Since $\mathfrak{H}$ is a primitive group of degree $2q$, $\mathfrak{H}$ is nonsolvable. Therefore $\mathfrak{M}$ is nonsolvable, too. If $\mathfrak{M}$ is imprimitive on $\Omega - \{1\}$, then let $\mathfrak{L}$ be a proper subgroup of $\mathfrak{M}$ containing $\mathfrak{K} \cap \mathfrak{M}$ properly. If the index of $\mathfrak{L}$ in $\mathfrak{M}$ equals two, the commutator subgroup of $\mathfrak{M}$ must be different from $\mathfrak{M}$ contradicting the simplicity of $\mathfrak{M}$. If the index of $\mathfrak{K} \cap \mathfrak{M}$ in $\mathfrak{L}$ equals two, $Ns(\mathfrak{K} \cap \mathfrak{M}) \cap \mathfrak{H}$ contains $\mathfrak{K}$ and $\mathfrak{L}$. Since $\mathfrak{K}$ is a maximal subgroup of $\mathfrak{H}$, we obtain that $Ns(\mathfrak{K} \cap \mathfrak{M}) \cap \mathfrak{H} = \mathfrak{H}$ and that $\mathfrak{K} \cap \mathfrak{M}$ is normal in $\mathfrak{M}$. Since $\mathfrak{M}$ is transitive on $\Omega - \{1\}$, this implies that $\mathfrak{K} \cap \mathfrak{M} = 1$ contradicting the nonsolvability of $\mathfrak{M}$. Hence $\mathfrak{M}$ is uniprimitive on $\Omega - \{1\}$.

Lemma 13. *$\mathfrak{M}$ does not possess an irreducible character ($\neq 1_{\mathfrak{M}}$) whose degree is not greater than $\frac{1}{2}(q+1)$. Hence the degree of nonlinear irreducible character of $\mathfrak{H}$ is greater than $\frac{1}{2}(q+1)$.*

Proof. Otherwise by Proposition C applied with q instead of p $\mathfrak{M}$ is isomorphic to $LF(2,q)$. Then $\mathfrak{N} \cap \mathfrak{M}$ has order $\frac{1}{2}(q-1)$. By Lemma 5 this implies that $s=2$, $r=2$, $q=5$ and $p=11$, contradicting the assumption.

Lemma 14. *Let $(B, D)_i$ be an irreducible character of $\mathfrak{G}$ of type $\boldsymbol{b}$. Then $(B,D)_i$ restricted on $\mathfrak{H}$ is decomposed into the sum of $\boldsymbol{b}$ and an irreducible character $\boldsymbol{a}_i$* of *$\mathfrak{H}$ of degree $q+1$.*

Proof. By the reciprocity theorem of Frobenius $\boldsymbol{b}$ appears as an irreducible component of $(B,D)_i$ restricted on $\mathfrak{H}$ with multiplicity 1. Therefore we have that

$$(B,D)_i(X) = \boldsymbol{b}(X) + \cdots$$

for every permutation X of $\mathfrak{H}$, where the part $\cdots$ does not contain $\boldsymbol{b}$ any more. If a linear character λ of $\mathfrak{H}$ appears in the part $\cdots$, then we clearly have that $\lambda \neq 1_{\mathfrak{H}}$ and that λ^* is the sum of $(B,D)_i$ and a linear character of $\mathfrak{G}$, which is different from $1_{\mathfrak{G}}$. This contradicts the simplicity of $\mathfrak{G}$. Now if the part $\cdots$ is reducible, then the degree of at least one component is greater than one and is not greater than $\frac{1}{2}(q+1)$. This contradicts Lemma 13.

Lemma 15. *There exists at least three different $(B,D)_i$ of type $\boldsymbol{b}$, say $(B,D)_1$, $(B,D)_2$ and $(B,D)_3$ such that $\boldsymbol{a}_1 = \boldsymbol{a}_2 = \boldsymbol{a}_3$.*

Proof. There exist $s-1$ different $(B,D)_i$'s of type $\boldsymbol{b}$. Now let us assume that Lemma 15 is false. Then since by Lemma 9 r is odd, s is even and we have at least $\frac{1}{2}(s-2)+1$ different $\boldsymbol{a}_i$'s. Since by Lemma 5 $s \geqq 2r-2$, we obtain that $\frac{1}{2}(s-2)+1 \geqq r-1$. Thus the first q-block of irreducible characters of $\mathfrak{H}$ contains at least $r+1$ characters of q-type A and B, because it contains $1_{\mathfrak{H}}$ and $\boldsymbol{b}$, too. By a theorem of Brauer [2, Theorem 2] this is a contradiction.

Lemma 16. *The decomposition of $\boldsymbol{a}_1^*$ into its irreducible components has the following form*:

$$\boldsymbol{a}_1^*(X) = (B,D)_1(X) + (B,D)_2(X) + (B,D)_3(X) + \sum_{i=1}^{s} (A,C)_i(X) + \cdots \tag{50}$$

for every permutation X of G, where the part $\cdots$ in (50) *does not contain $(B,D)_1$, $(B,D)_2$, $(B,D)_3$ and $(A,C)_i$ $(i=1,\cdots,s)$ any more.*

Proof. It is enough to prove that all the $(A,C)_i$ $(i=1,\cdots,s)$ appear in $\boldsymbol{a}_1^*$ with multiplicity 1. Then it is enough to show the appearance of some $(A,C)_i$ with multiplicity 1, because of the property of exceptional characters [13]. Let P be an element of $\mathfrak{G}$ of order p. Then by Proposition B we have that

$(B,D)_1(P) = (B,D)_2(P) = (B,D)_3(P) = -1$. Since P is not contained in any of p conjugate subgroups of $\mathfrak{H}$ in $\mathfrak{G}$ we have that $\boldsymbol{a}_1^*(P) = 0$. Therefore irreducible characters of $\mathfrak{G}$ of p-type A or p-type C with $\delta_p = 1$ must appear in the part $\cdots$ of (50) with the sum of multiplicities at least three. Then since the sum of degrees of the part $\cdots$ of (50) is equal to $(q-2)p+3$, inspecting the degree table we see the appearance of some $(A,C)_i$ with multiplicity 1.

Let X be a generalized character of $\mathfrak{H}$. We denote by $x_A(X)$, $x_B(X)$ and $x_D(X)$ the sum of multiplicities of irreducible components of X of q-type A, B and D, respectively.

Let $\boldsymbol{c}_i$ be the irreducicble characters of $\mathfrak{H}$ of q-type C $(i = 1,\cdots,s)$. Then by a theorem of exceptional characters [13] we can assume that

$$(51) \qquad (A,C)_j(X) = \varepsilon \boldsymbol{c}_j(X) + a \sum_{i=1}^{s} \boldsymbol{c}_i(X) + \cdots$$

for every permutation X of $\mathfrak{H}$ $(j = 1,\cdots,s)$, where $\varepsilon = \pm 1$, a and $a+\varepsilon$ are non-negative integers, and the part $\cdots$ in (51) does not contain $\boldsymbol{c}_i$ any more $(i = 1,\cdots,s)$. By a theorem of Brauer [2, Theorem 10] the degree of $\boldsymbol{c}_i$ is congruent to $-\delta_q(\mathfrak{H})r$ modulo q. Now we can prove the following lemma.

Lemma 17. *$\varepsilon = 1$, $a = 0$ and $\delta_q(\mathfrak{H}) = -1$.*

Proof. By the reciprocity theorem of Frobenius and by (30), (31) and (50) the part $\cdots$ in (51) contains $\boldsymbol{b}$, $\boldsymbol{d}$ and $\boldsymbol{a}_1$ as irreducible components with multiplicity 1. Hence we have that

$$(52) \qquad (A,C)_j(X) = \boldsymbol{c}_j(X) + a \sum_{i=1}^{s} \boldsymbol{c}_i(X) + \boldsymbol{b}(X) + \boldsymbol{d}(X) + \boldsymbol{a}_1(X) + \cdots$$

for every permutation X of $\mathfrak{H}$ $(j = 1,\cdots,s)$, where the part $\cdots$ of (52) does not contain $\boldsymbol{c}_i$ $(i = 1,\cdots,s)$, $\boldsymbol{b}$, $\boldsymbol{d}$ and $\boldsymbol{a}_1$ any more.

By Lemma 13 the degree of $\boldsymbol{c}_i$ is not smaller than $q - r$ $(i = 1,\cdots,s)$. Now let us assume that $a = 1$. Then from (52) we obtain that

$$(r-1)p + 1 \geqq (s-1)(q-r) + 3q,$$

which implies that

$$0 \geqq (s - 2r + 3)q + 1.$$

By Lemma 5 this is a contradiction. Thus we obtain that $a = 0$ and $\varepsilon = 1$. Put $x_A = x_A\{(A,C)_j\}$, $x_B = x_B\{(A,C)_j\}$ and $x_D = x_D\{(A,C)_j\}$. Then the sum of degrees of irreducible components of $(A,C)_j$ restricted on $\mathfrak{H}$ has the form $y_Aq + x_A, y_Bq - x_B$ and y_Dq, respectively, where y_A, y_B and y_D are non-negative integers. Since $(r-1)p + 1 > p$, by the reciprocity theorem of Frobenius no linear character of $\mathfrak{H}$ can appear in (52). Hence we have that

$$y_A \geqq x_A \text{ and } y_B \geqq x_B. \tag{53}$$

Now let us assume that $\delta_q(\mathfrak{H}) = 1$ and that the degree of $\boldsymbol{c}_i$ is equal to $xq - r$. Then we have the following equality:

$$(r-1)p + 1 = xq - r + y_A q + x_A + y_B q - x_B + y_D q, \tag{54}$$

which implies the congruence

$$x_B + 2r \equiv x_A \pmod{q}. \tag{55}$$

Now if $x_B + 2r \geqq q$, then $x_B \geqq q - 2r$ and by (53) $y_B \geqq q - 2r$. Hence from (54) we obtain that

$$(r-1)p + 1 \geqq y_B(q-1) \geqq (q-2r)(q-1),$$

which implies that $4r \geqq q + 1$. By Lemma 5 this implies that $r = 2$. Then by a previous result [10, Theorem 2] $\mathfrak{G}$ is isomorphic to $LF(2, 11)$ with $p = 11$, contradicting the assumption $p > 11$. Hence we obtain that $x_B + 2r < q$. Therefore from (55) we have that $x_A \geqq 2r$ and by (53) that $y_A \geqq 2r$. Hence from (54) we obtain that

$$(r-1)p + 1 \geqq y_A q \geqq 2rq,$$

which implies the contradiction that $r \geqq 2q$.

Now by Lemmas 13 and 17 the degree of $\boldsymbol{c}_i$ is not smaller than $q + r(i = 1, \cdots, s)$.

Lemma 18. *No irreducible character of $\mathfrak{G}$ whose degree is not greater than $8q$ can contain any $\boldsymbol{c}_i$ as its irreducible component, when it is restricted on $\mathfrak{H}$.*

Proof. Let $\boldsymbol{X}$ be an irreducible character of $\mathfrak{G}$ such that $\boldsymbol{X}$ restricted on $\mathfrak{H}$ contains some $\boldsymbol{c}_i$ as its irreducible component. If $\boldsymbol{X} = (A, C)_j$, then the degree of $\boldsymbol{X}$ is equal to $(r-1)p + 1 = (2r-2)q + r$. If $r = 3$, then $q \equiv 1 \pmod{3}$ and $p = 2q + 1 \equiv 0 \pmod{3}$, which is absurd. Therefore by Lemma 9 we have that $r \geqq 5$. Hence the degree of $\boldsymbol{X}$ is greater than $8q$. If $\boldsymbol{X} \neq (A, C)_j$ $(j = 1, \cdots, s)$, then from the property of exceptional characters $\boldsymbol{X}$ restricted on $\mathfrak{H}$ contains all the $\boldsymbol{c}_i$'s as its irreducible components. Hence the degree of $\boldsymbol{X}$ is not smaller than $s(q + r)$. By Lemma 5 we have that $s \geqq 2r - 2 \geqq 8$. Thus the degree of $\boldsymbol{X}$ is greater than $8q$.

Now let us consider two reducible characters $\boldsymbol{X}_0(B,D)_0$ and $\overline{(B,D)}_0(B,D)_0$ of $\mathfrak{G}$. Then the decomposition of $\boldsymbol{X}_0(B,D)_0$ into its irreducible parts can be easily obtained as follows. Let $\boldsymbol{X}$ be an irreducible character of $\mathfrak{G}$ and let $\boldsymbol{X}$ restricted on $\mathfrak{H}$ contain $\boldsymbol{d}$ as its irreducible component of multiplicity x. Then $\bar{\boldsymbol{X}}$ restricted on $\mathfrak{H}$ contains $\boldsymbol{d}$ as its irreducible component of multiplicity x, too, because $\boldsymbol{d}$ is rational by Proposition D. Now by the orthogonality relations of group characters we have that

$$\sum_{X \in \mathfrak{H}} \bar{\boldsymbol{X}}(X)(B,D)_0(X) = 2xh.$$

Since the same equality holds for each of p conjugate subgroups of $\mathfrak{H}$ in $\mathfrak{G}$, this implies that

$$\sum_{X\in\mathfrak{G}} \alpha(X)\bar{X}(X)(B,D)_0(X) = 2xg$$
$$= \sum_{X\in\mathfrak{G}} \bar{X}(X)(B,D)_0(X) + \sum_{X\in\mathfrak{G}} X_0(X)\bar{X}(X)(B,D)_0(X).$$

If $X \neq (B,D)_0$, then $\sum_{X\in\mathfrak{G}} \bar{X}(X)(B,D)_0(X) = 0$. Hence by the orthogonality relations of group characters we see that X appears in $X_0(B,D)_0$ as an irreducible component of multiplicity $2x$. Similarly if $X = (B,D)_0$, then X appears in $X_0(B,D)_0$ as an irreducible component of multiplicity 3. Thus the following two equalities can be easily obtained from (31. 1) and (31. 2):

$$\begin{aligned} X_0(X)(B,D)_0(X) &= 3(B,D)_0(X) + 2X_0(X) \\ &\quad + 2\sum_{i=1}^{s}(A,C)_i(X) + 2(D,A)(X) + 4\sum_{(j\neq 0)}^{t-1}(B,D)_j(X) \\ &\quad + 2\sum^{u}(B,D)_k(X) \end{aligned} \tag{56.1}$$

for every permutation X of $\mathfrak{G}$, or

$$\begin{aligned} X_0(X)(B,D)_0(X) &= 3(B,D)_0(X) + 2X_0(X) \\ &\quad + 2\sum_{i=1}^{s}(A,C)_i(X) + 2(B,A)(X) + 4\sum_{(j\neq 0)}^{t-1}(B,D)_j(X) \\ &\quad + 2\sum^{u}(B,D)_k(X) \end{aligned} \tag{56.2}$$

for every permutation X of $\mathfrak{G}$.

The following lemma can be proved in the same way as Lemma 14.

LEMMA 19. *Let $(B,D)_i$ be an irreducible character of $\mathfrak{G}$ of type $\boldsymbol{d}$. Then $(B,D)_i$ restricted on $\mathfrak{H}$ is decomposed into the sum of $\boldsymbol{d}$ and an irreducible character $\boldsymbol{d}_i$ of $\mathfrak{H}$ of degree q.*

Some $\boldsymbol{d}_i$'s are possibly coincident for different i's.

Now let us consider (56.1) and (56.2) only for elements of $\mathfrak{H}$. Then by (10) and Lemma 19, (56.1) and (56.2) will be transformed into the following forms:

$$\begin{aligned} \{1_{\mathfrak{H}}(X) + \boldsymbol{b}(X) + \boldsymbol{d}(X)\}2\boldsymbol{d}(X) &= 6\boldsymbol{d}(X) + 2\{1_{\mathfrak{H}}(X) + \boldsymbol{b}(X) + \boldsymbol{d}(X)\} \\ &\quad + 2\sum_{i=1}^{s}(A,C)_i(X) + 2(D,A)(X) \\ &\quad + 8(t-1)\boldsymbol{d}(X) + 2u\boldsymbol{d}(X) + 2\sum^{u}\boldsymbol{d}_i(X) \end{aligned} \tag{\#.1}$$

for every permutation X of $\mathfrak{H}$, or

$$\begin{aligned}\{1_{\mathfrak{H}}(X)+\boldsymbol{b}(X)+\boldsymbol{d}(X)\}2\boldsymbol{d}(X)=6\boldsymbol{d}(X)&+2\{1_{\mathfrak{H}}(X)+\boldsymbol{b}(X)+\boldsymbol{d}(X)\}\\ &+2\sum_{i=1}^{s}(A,C)_i(X)+2(B,A)(X)\\ &+8(t-1)\boldsymbol{d}(X)+2u\boldsymbol{d}(X)+2\sum^{u}\boldsymbol{d}_i(X)\end{aligned}\tag{\#.2}$$

for every permutation X of $\mathfrak{H}$.

Now the following two equalities can be easily obtained from (#.1) and (#.2).

$$\begin{aligned}\boldsymbol{b}(X)\boldsymbol{d}(X)+\{\boldsymbol{d}(X)\}^2=1_{\mathfrak{H}}(X)&+\boldsymbol{b}(X)+(4t+u-1)\boldsymbol{d}(X)\\ &+\sum^{u}\boldsymbol{d}_i(X)+\sum_{i=1}^{s}(A,C)_i(X)+(D,A)(X)\end{aligned}\tag{57.1}$$

for every permutation X of $\mathfrak{H}$, or

$$\begin{aligned}\boldsymbol{b}(X)\boldsymbol{d}(X)+\{\boldsymbol{d}(X)\}^2=1_{\mathfrak{H}}(X)&+\boldsymbol{b}(X)+(4t+u-1)\boldsymbol{d}(X)\\ &+\sum^{u}\boldsymbol{d}_i(X)+\sum_{i=1}^{s}(A,C)_i(X)+(B,A)(X)\end{aligned}\tag{57.2}$$

for every permutation X of $\mathfrak{H}$.

By Lemmas 17 and 18 we see that $\boldsymbol{c}_i$ appears in (57.1) and (57.2) as an irreducible component with multiplicity 1 $(i=1,\cdots,s)$.

Now let us consider $\overline{(B,D)_0}(B,D)_0$. We have already that

$$\overline{(B,D)_0}(B,D)_0(X)=1_{\mathfrak{G}}(X)+3X_0(X)+\cdots\tag{58}$$

for every permutation X of $\mathfrak{G}$, where the part $\cdots$ in (58) does not contain $1_{\mathfrak{G}}$ and X_0 any more.

Lemma 20. *$\overline{(B,D)_0}(B,D)_0$ contains $(A,C)_i$ $(i=1,\cdots,s)$ as an irreducible component with multiplicity* 1.

Proof. Let P be an element of $\mathfrak{G}$ of order p. Then by Proposition B we have that $\overline{(B,D)_0}(P)=(B,D)_0(P)=-1$, $1_{\mathfrak{G}}(P)=1$ and $X_0(P)=-1$. Therefore the part $\cdots$ of (58) contains irreducible characters of $\mathfrak{G}$ of p-type A or p-type C with $\delta_p=1$ with the sum of multiplicities at least three. Now the sum of degrees of irreducible characters of the part $\cdots$ of (58) equals $(2q-4)p+3$. By a property of exceptional characters [13] all the $(A,C)_i$'s appear in (58) with the same multiplicity. Therefore inspecting the degree table, it is easily seen that $(A,C)_i$ $(i=1,\cdots,s)$ appears in the part $\cdots$ of (58) with multiplicity $x\geqq 1$:

$$\overline{(B,D)_0}(X)(B,D)_0(X)=1_{\mathfrak{G}}(X)+3X_0(X)+x\sum_{i=1}^{s}(A,C)_i(X)+\cdots\tag{59}$$

for every permutation X of $\mathfrak{G}$, where the part $\cdots$ of (59) does not contain $1_{\mathfrak{G}}$, X_0 and $(A,C)_i$ $(i=1,\cdots,s)$ any more.

If $x \geqq 3$, then the sum of degrees of irreducible components in the part $\cdots$ of (59) is not greater than $(3s-q-1)p+3-3s$. But since we already know that $q=rs+1 \geqq 5s+1$, this shows a contradiction. If $x=2$, then we have that

$$(60)\qquad \overline{(B,D)}_0(X)(B,D)_0(X)=1_{\mathfrak{G}}(X)+3X_0(X)\ +\ 2\sum_{i=1}^{s}(A,C)_i(X)+\cdots$$

for every permutation X of $\mathfrak{G}$. Since by Proposition B we have that

$$2\sum_{i=1}^{s}(A,C)_i(P)=2s,$$

irreducible characters of $\mathfrak{G}$ of p-type B or p-type C with $\delta_p=-1$ must appear in the part $\cdots$ of (60) with the sum of multiplicities at least $2s-3$. But the sum of degrees of irreducible components of the part $\cdots$ of (60) is equal to $(2s-2)p-(2s-3)$. Then it is easy to see that the decomposition of $\overline{(B,D)_0}(B,D)_0$ into its irreducible components has one of the following two forms:

$$(60.\mathrm{i})\qquad \begin{aligned}\overline{(B,D)}_0(X)(B,D)_0(X)&=1_{\mathfrak{G}}(X)+3X_0(X)\\ &\quad+2\sum_{i=1}^{s}(A,C)_i(X)+(D,A)(X)+\sum^{2s-3}(B,D)_j(X)\end{aligned}$$

for every permutation X of $\mathfrak{G}$, where the degrees of (D,A) and $(B,D)_j$'s are equal to p and $p-1$, respectively, and

$$(60.\mathrm{ii})\qquad \begin{aligned}\overline{(B,D)}_0(X)(B,D)_0(X)&=1_{\mathfrak{G}}(X)+3X_0(X)\\ &\quad+2\sum_{i=1}^{s}(A,C)_i(X)+(B,A)(X)+\sum^{2s-4}(B,D)_j(X)\end{aligned}$$

for every permutation X of $\mathfrak{G}$, where the degrees of (B,A) and $(B,D)_j$'s are equal to $2p-1$ and $p-1$, respectively.

Let us consider (60.i) and (60.ii) only for permutations of $\mathfrak{H}$. Then by Lemmas 17 and 18 we obtain that

$$4\{d(X)\}^2=2\sum_{i=1}^{s}c_i(X)+\cdots$$

for every permutation X of $\mathfrak{H}$, where the part $\cdots$ does not contain c_i $(i=1,\cdots,s)$ any more. This shows clearly a contradiction. This proves Lemma 20.

Thus we obtain that

$$(61)\qquad \overline{(B,D)}_0(X)(B,D)_0(X)=1_{\mathfrak{G}}(X)+3X_0(X)\ +\sum_{i=1}^{s}(A,C)_i(X)+\cdots$$

for every permutation X of $\mathfrak{G}$, where the part $\cdots$ of (61) does not contain $1_{\mathfrak{G}}$, X_0 and $(A,C)_i$ $(i=1,\cdots,s)$ any more and the sum of degrees of irreducible components in the part $\cdots$ of (61) is equal to $(q+s-3)p-(s-3)$.

Now by Lemmas 17, 18, 20, (57) and (61) we obtain the following important lemma.

Lemma 21. *$\overline{(B\ D)_0}(B\ D)_0$ contains an irreducible component such that it is different from $(A,C)_i$ $(i = 1,\cdots,s)$ and it contains c_i $(i = 1,\cdots,s)$ as its irreducible components with multiplicity three when it is restricted on $\mathfrak{H}$.*

Proof. Let X be an irreducible character of $\mathfrak{G}$ such that X is different from $(A,C)_i\,(i = 1,\cdots,s)$ and X restricted on $\mathfrak{H}$ contains c_i $(i = 1,\cdots,s)$ as its irreducible components. Then it is enough to show that X is the only character with this property. In fact, the left-hand side of (61), when it is restricted on $\mathfrak{H}$ equals $4d^2$, and by (57) and Lemmas 17 and 20 c_i $(i = 1,\cdots,s)$ appears in $4d^2$ as an irreducible component with multiplicity four. Now by Lemma 18 and by inspecting the degree table we see that the degree of X cannot be smaller than $(q-2)p+1$. By (61) this proves Lemma 21.

Now checking up the degree table again, we see that X has only the following nine candidates, each of which will be eliminated case after case. (I) (A,A) of degree $qp+1$, (II) (A,B) of degree $(q-2)p+1$, (III) (A,D) of degree $(q-1)p+1$, (IV) (B,A) of degree $(q+2)p-1$, (V) (B,B) of degree $qp-1$, (VI) (B,D) of degree $(q+1)p-1$, (VIII) (D,A) of degree $(q+1)p$, (VIII) (D,B) of degree $(q-1)p$ and (IX) (D,D) of degree qp.

Lemma 22. *Cases* (I), (IV) *and* (VII) *cannot occur.*

Proof. Let us assume that case (I) occurs. Then we have that

$$\overline{(B,D)}_0(X)(B,D)_0(X) = 1_{\mathfrak{G}}(X) + 3X_0(X) + \sum_{i=1}^{s} (A,C)_i(X) + (A,A)(X) + \cdots$$

for every permutation X of $\mathfrak{G}$, where the sum of degrees of irreducible components in the part $\cdots$ equals $(s-3)p-(s-2)$.

Let P be an element of $\mathfrak{G}$ of order p. Then by Proposition B we have that $\overline{(B,D)}_0(P)(B,D)_0(P) = 1$, $1_{\mathfrak{G}}(P) = 1$, $X_0(P) = -1$, $\sum_{i=1}^{s}(A,C)_i(P) = s$ and $(A,A)(P) = 1$. Therefore irreducible characters of p-type B or p-type C with $\delta_p = -1$ must appear in the part $\cdots$ with the sum of multiplicities at least $s-2$. Since $(s-2)(p-1) > (s-3)p-(s-2)$, this is a contradiction. Cases (IV) and (VII) can be similarly eliminated.

In the remaining cases the q-type of X is not A. This fact is important for the following proofs.

Lemma 23. *Cases* (III), (VI) *and* (IX) *cannot occur.*

Proof. Let us assume that case (III) occurs. Then we have that

$$\overline{(B,D)}_0(X)(B,D)_0(X) = 1_{\mathfrak{G}}(X) + 3X_0(X) + \sum_{i=1}^{s} (A,C)_i(X) + (A,D)(X) + \cdots \tag{62}$$

for every permutation X of $\mathfrak{G}$, where the sum of degrees of irreducible components in the part $\cdots$ of (62) equals $(s-2)(p-1)$.

Let P be an element of $\mathfrak{G}$ of order p. Then by Proposition B we have that $\overline{(B,D)}_0(P)\ (B,D)_0(P) = 1$, $1_{\mathfrak{G}}(P) = 1$, $3X_0(P) = -3$, $\sum_{i=1}^{s} (A,\ C)_i(P) = s$ and $(A,D)(P) = 1$. Therefore irreducible characters of $\mathfrak{G}$ of p-type B or p-type C with $\delta_p = -1$ must appear in the part $\cdots$ of (62) with the sum of multiplicities at least $s-2$. Hence we have that

$$\overline{(B,D)}_0(X)(B,D)_0(X) = 1_{\mathfrak{G}}(X) + 3X_0(X) + \sum_{i=1}^{s} (A,C)_i(X) + (A,D)(X) + \sum^{s-2} (B,D)_i(X) \tag{63}$$

for every permutation X of $\mathfrak{G}$, where the degrees of $(B,D)_i$'s are equal to $p-1$. Now let us put

$$\sum^{s-2} (B,D)_i = \sum_{\text{type b}} (B,D)_j + \sum_{\text{type 2d}} (B,D)_k + \sum_{\text{type d}} (B,D)_l + \sum_{\text{others}} (B,D)_m.$$

Let us consider (B,D) in $\sum_{\text{others}}(B,D)_m$. If (B,D) restricted on $\mathfrak{H}$ contains an irreducible character of $\mathfrak{H}$ of q-type B as an irreducible component, then the component has degree $q-1$. In fact, otherwise, (B,D) restricted on $\mathfrak{H}$ contains a linear character λ $(\neq 1_{\mathfrak{H}})$ of $\mathfrak{H}$ as an irreducible component. Then by the Frobenius reciprocity theorem λ^* contains (B,D) and hence a linear character $(\neq 1_{\mathfrak{G}})$ of $\mathfrak{G}$ as its irreducible components, contradicting the simplicity of $\mathfrak{G}$. Similarly if (B,D) restricted on $\mathfrak{H}$ contains an irreducible character of $\mathfrak{H}$ of q-type A as an irredicible component, then the component has degree $q+1$.

Now let us consider (63) only for permutations of $\mathfrak{H}$. Then we have that

$$4\{\boldsymbol{d}(X)\}^2 = 4\,1_{\mathfrak{H}}(X) + 3\boldsymbol{b}(X) + 3\boldsymbol{d}(X) + \sum_{i=1}^{s} (A,C)_i(X) + (A,D)(X) + \sum^{s-2} (B,D)_i(X) \tag{64}$$

for every permutation of $\mathfrak{H}$.

Let $\boldsymbol{y}$ be an irreducible character of $\mathfrak{H}$ which is different from $\boldsymbol{c}_i$ $(i = 1,\cdots,s)$. Then by a property of exceptional characters the multiplicity of $\boldsymbol{y}$ in $\sum_{i=1}^{s}(A,C)_i$ restricted on $\mathfrak{H}$ is a multiple of s and therefore, by Lemma 10, a multiple of 4.

Now let us consider (A,D) restricted on $\mathfrak{H}$. By Lemma 21 we have that

$$(A,D)(X) = 3\sum_{i=1}^{s} \boldsymbol{c}_i(X) + \cdots \tag{65}$$

for every permutation X of $\mathfrak{H}$, where the part $\cdots$ does not contain $\boldsymbol{c}_i$ $(i = 1,\cdots,s)$ any more. We put $x_A = x_A\{(A,D)\}$ and $x_B = x_B\{(A,D)\}$. Let Q be an element of $\mathfrak{H}$ of order q. Let us observe (65) at Q. Then by Proposition B and Lemma 17 we obtain that

$$0 = -3 + x_A - x_B.$$

If x_B is odd, then at least one irreducible component $\boldsymbol{b}_0$ of q-type B of (A,D) restricted on $\mathfrak{H}$ must appear in $\sum^{s-2}(B,D)_i$ of (64), because of (30), (31.1) and (31.2) and since the multiplicity of $\boldsymbol{b}_0$ in $\sum_{i=1}^{s}(A,C)_i$ is, as we have noticed above a multiple of four. Therefore by Lemmas 14 and 19 and the remark above, the degree of $\boldsymbol{b}_0$ is equal to $q-1$. This gives us a contradiction, because then by the reciprocity theorem of Frobenius (A,D) must appear in $\boldsymbol{b}_0^*$ and must have degree not greater than $(q-1)p$. Hence x_B is even and x_A must be odd. Therefore at least one irreducible component $\boldsymbol{a}_0$ of q-type A of (A,D) restricted on $\mathfrak{H}$ must appear in $\sum^{s-2}(B,D)_i$ of (64), because the same argument made for $\boldsymbol{b}_0$ holds for $\boldsymbol{a}_0$, too. Then again by Lemmas 14 and 19 and the remark above the degree of $\boldsymbol{a}_0$ is equal to $q+1$. Then using the reciprocity theorem of Frobenius we see that the multiplicity of $\boldsymbol{a}_0$ in (A,D) restricted on $\mathfrak{H}$ must be one. Therefore from (64) we see that $\boldsymbol{a}_0$ must appear in $\sum^{s-2}(B,D)_i$ of (64) with the sum of multiplicity at least three. Using again the reciprocity theorem of Frobenius we obtain that

$$(q+1)p \geqq (q-1)p + 1 + 3(p-1),$$

which is clearly a contradiction. Cases (VI) and (IX) can be similarly eliminated.

Now let us consider case (II). Then we have that

$$\begin{aligned}\overline{(B,D)}_0(X)(B,D)_0(X) &= 1_{\mathfrak{G}}(X) + 3X_0(X)\\ &\quad + \sum_{i=1}^{s}(A,C)_i(X) + (A,B)(X) + \cdots\end{aligned} \tag{66}$$

for every permutation X of $\mathfrak{G}$, where the sum of degrees of irreducible components in the part $\cdots$ of (66) is equal to $(s-1)p-(s-2)$.

Let P be an element of $\mathfrak{G}$ of order p. Then by Proposition B (66) at P shows that

$$1 = 1 - 3 + s + 1 + \cdots.$$

Therefore irreducible characters of $\mathfrak{G}$ of p-type B or p-type C with $\delta_p = -1$ must appear in the part $\cdots$ of (65) with the sum of multiplicities at least $s-2$. Hence it is easy to see that we have only the following subcases for the decompositions of $\overline{(B,D)}_0(B,D)_0$.

$$\begin{aligned}\overline{(B,D)}_0(X)(B,D)_0(X) = 1_{\mathfrak{G}}(X) &+ 3X_0(X) \\ &+ \sum_{i=1}^{s} (A,C)_i(X) + (A,B)(X) + (D,A)(X) \\ &+ \sum^{s-2} (B,D)_i(X)\end{aligned} \tag{II.a}$$

for every permutation X of $\mathfrak{G}$, where the degrees of (D,A) and $(B,D)_i$'s are equal to p and $p-1$, respectively.

$$\begin{aligned}\overline{(B,D)}_0(X)(B,D)_0(X) = 1_{\mathfrak{G}}(X) &+ 3X_0(X) \\ &+ \sum_{i=1}^{s} (A,C)_i(X) + (A,B)(X) + (B,A)(X) \\ &+ \sum^{s-3} (B,D)_i(X)\end{aligned} \tag{II.b}$$

for every permutation X of $\mathfrak{G}$, where the degrees of (B,A) and $(B,D)_i$'s are equal to $2p-1$ and $p-1$, respectively.

The same things hold for cases (V) and (VIII), too. Therefore we obtain that

$$\begin{aligned}\overline{(B,D)}_0(X)(B,D)_0(X) = 1_{\mathfrak{G}}(X) &+ 3X_0(X) \\ &+ \sum_{i=1}^{s} (A,C)_i(X) + (B,B)(X) + (D,A)(X) \\ &+ \sum^{s-4} (B,D)_i(X)\end{aligned} \tag{V.a}$$

for every permutation X of $\mathfrak{G}$, where the degrees of (D,A) and $(B,D)_i$'s are equal to p and $p-1$, respectively.

$$\begin{aligned}\overline{(B,D)}_0(X)(B,D)_0(X) = 1_{\mathfrak{G}}(X) &+ 3X_0(X) \\ &+ \sum_{i=1}^{s} (A,C)_i(X) + (B,B)(X) + (B,A)(X) \\ &+ \sum^{s-5} (B,D)_i(X)\end{aligned} \tag{V.b}$$

or every permutation X of $\mathfrak{G}$, where the degrees of (B,A) and $(B,D)_i$'s are equal to $2p-1$ and $p-1$, respectively.

$$\begin{aligned}\overline{(B,D)}_0(X)(B,D)_0(X) = 1_{\mathfrak{G}}(X) &+ 3X_0(X) \\ &+ \sum_{i=1}^{s} (A,C)_i(X) + (D,B)(X) + (D,A)(X) \\ &+ \sum^{s-3} (B,D)_i(X)\end{aligned} \tag{VIII.a}$$

for every permutation X of $\mathfrak{G}$, where the degrees of (D,A) and $(B,D)_i$'s are equal to p and $p-1$, respectively.

$$\begin{aligned}\overline{(B,D)}_0(X)(B,D)_0(X) = 1_{\mathfrak{G}}(X) &+ 3X_0(X)\\ &+ \sum_{i=1}^{s}(A,C)_i(X) + (D,B)(X) + (B,A)(X)\\ &+ \sum^{s-4}(B,D)_i(X)\end{aligned} \tag{VIII.b}$$

for every permutation X of $\mathfrak{G}$, where the degrees of (B,A) and $(B,D)_i$'s are equal to $2p-1$ and $p-1$, respectively.

Lemma 24. *(D,A) in* (31.1) (*and in* (57.1)) *contains no linear component, when it is restricted on $\mathfrak{H}$.*

Proof. By (31.1) and Proposition D we see that (D,A) is a rational character. Moreover by (31.1) and the reciprocity theorem of Frobenius (D,A) restricted on $\mathfrak{H}$ contains $\boldsymbol{d}$ as its irreducible component with multiplicity 1. Now put $x_A = x_A\{(D,A)\}$ and $x_B = x_B\{(D,A)\}$. Let Q be an element of $\mathfrak{H}$ of order q. Then using Proposition B and Lemma 18 we have that

$$(D,A)(Q) = 1 = x_A - x_B.$$

Since the degree of irreducible characters of $\mathfrak{H}$ of q-type B is at least $q-1$, we have that $x_B \leqq 1$. If $x_B = 1$, then $x_A = 2$ and (D,A) restricted on $\mathfrak{H}$ contains two linear characters. By (7) these two linear characters are different from $1_{\mathfrak{H}}$. Since (D,A) is rational, these two linear characters are algebraically conjugate with each other. Hence their field is the field of either the cubic roots of unity or the quartic roots of unity. Now we already know that $\mathfrak{H}/\mathfrak{M} \cong \mathfrak{N}/\mathfrak{N}\cap\mathfrak{M}$ and $\mathfrak{M}$ is simple. Therefore r must be divisible by three or four. But since r is odd by Lemma 9, r is divisible by three. This implies the absurdity $q \equiv 1 \pmod 3$ and $p \equiv 0 \pmod 3$. Hence $x_B = 0$ and $x_A = 1$. Therefore the component of q-type A of (D,A) restricted on $\mathfrak{H}$ is rational and hence by (7) cannot be linear.

Lemma 25. *(D,A) in subcases* a *is decomposed into the sum of two irreducible components with degrees q and $q+1$, respectively, when it is restricted on $\mathfrak{H}$.*

Proof. (D,A) restricted on $\mathfrak{H}$ cannot be irreducible on $\mathfrak{H}$, because p does not divide h. By Lemma 18 $\boldsymbol{c}_i$ $(i = 1,\cdots,s)$ cannot be an irreducible component of (D,A) restricted on $\mathfrak{H}$. Let Q be an element of $\mathfrak{H}$ of order q. By Proposition B we have that $(D,A)(Q)=1$. Therefore (D,A) restricted on $\mathfrak{H}$ contains an irreducible component of q-type A. Let one component be linear. Then by (7) it is different from $1_{\mathfrak{H}}$ and it must appear in (57.1) or in (57.2). Then the only possible source for it is (D,A) in (57.1). But this contradicts Lemma 24. The rest is obvious.

Lemma 26. *Subcases* (II.a), (V.a) *and* (VIII.a) *cannot occur.*

Proof. Let us assume that subcase (II.a) occurs. Let us consider (A,B) restricted on $\mathfrak{H}$. By assumption we have that

$$(A,B)(X) = 3\sum_{i=1}^{s} \boldsymbol{c}_i(X) + \cdots \tag{67}$$

for every permutation X of $\mathfrak{H}$, where the part $\cdots$ does not contain $\boldsymbol{c}_i$ $(i = 1,\cdots,s)$ any more. Put $x_A = x_A\{(A,B)\}$ and $x_B = x_B\{(A,B)\}$. Let Q be an element of $\mathfrak{H}$ of order q. Consider (67) at Q. Then by Proposition B and Lemma 17 we have that

$$-1 = -3 + x_A - x_B.$$

If x_B is not a multiple of 4, then by Lemma 25 at least one irreducible component $\boldsymbol{b}_0$ of q-type B of (A,B) restricted on $\mathfrak{H}$ must appear in $\sum^{s-2}(B,D)_i$ of (II.a), since the multiplicity of $\boldsymbol{b}_0$ in $\sum_{i=1}^{s}(A,C)_i$ is, as we have noticed in the proof of Lemma 23, a multiple of 4. Then by Lemmas 14 and 19 and the remark made in the beginning of the proof of Lemma 23 the degree of $\boldsymbol{b}_0$ is equal to $q-1$. Then the multiplicity of $\boldsymbol{b}_0$ in (A,B) is one. Therefore as in the proof of Lemma 23 we see that the multiplicity of $\boldsymbol{b}_0$ in $\sum^{s-2}(B,D)_i$ is at least three. Then using the reciprocity theorem of Frobenius we obtain that

$$(q-1)p \geqq (q-2)p + 1 + 3p - 1).$$

This is clearly a contradiction. Hence x_B must be a multiple of 4 and hence x_A cannot be a multiple of 4. Therefore at least one irreducible component $\boldsymbol{a}_0$ of q-type A of (A,B) restricted on $\mathfrak{H}$ must appear in $(D,A) + \sum^{s-2}(B,D)_i$ of (II.a), since the multiplicity of $\boldsymbol{a}_0$ in $\sum_{i=1}^{s}(A,C)_i$ is, as above, a multiple of 4. Using Lemmas 14, 19 and 25 we see that the degree of $\boldsymbol{a}_0$ is equal to $q+1$. Therefore the multiplicity of $\boldsymbol{a}_0$ in (A,B) is one, and hence as in the proof of Lemma 23 the multiplicity of $\boldsymbol{a}_0$ in $(D,A) + \sum^{s-2}(B,D)_i$ of (II.a) is at least three. Let us consider $\boldsymbol{a}_0^*$. Then we have that

$$\boldsymbol{a}_0^*(X) = (A,B)(X) + \cdots$$

for every permutation X of $\mathfrak{G}$, where the sum of degrees of the part $\cdots$ equals $3p-1$. Therefore we see that

$$\boldsymbol{a}_0^*(X) = (A,B)(X) + 2(D,A)(X) + (B,D)_1(X),$$

where X runs over all the permutations of $\mathfrak{G}$ and (D,A) and $(B,D)_1$ come from (II.a). Then by the reciprocity theorem of Frobenius we have that

$$(D,A)(X) = 2\boldsymbol{a}_0(X) + \cdots$$

for every permutation X of $\mathfrak{H}$ and the part $\cdots$ does not contain $\boldsymbol{a}_0$ any more. For $X = 1$ this gives us an absurdity $p = 2q + 1 = 2(q+1)$. Subcases (V.a) and (VIII.a) can be similarly eliminated.

Lemma 27. *If* (B,A) *in* (31.2) (*and in* (57.2)) *restricted on* $\mathfrak{H}$ *contains an irreducible component* $\boldsymbol{b}_0$ *of* q*-type* B, *then the degree of* $\boldsymbol{b}_0$ *is equal to* $q-1$.

Proof. By the reciprocity theorem of Frobenius $\boldsymbol{d}$ appears in (B,A) in (31.2) restricted on $\mathfrak{H}$ as an irreducible component of multiplicity 1. Put $x_A = x_A\{(B,A)\}$ and $x_B = x_B\{(B,A)\}$. Let Q be an element of $\mathfrak{H}$ of order q. Then using Proposition B as the value of (B,A) at Q we obtain $1 = x_A - x_B$. In particular, we have that $x_A \geqq 2$. Since obviously (B,A) restricted on $\mathfrak{H}$ does not contain a linear component, this gives us a contradiction $q + 2(q+1) + 2q - 1 > 2p - 1$, if the degree of $\boldsymbol{b}_0$ is bigger than $q-1$.

Lemma 28. *If* (B,A) *in subcases* b *restricted on* $\mathfrak{H}$ *contains an irreducible component* $\boldsymbol{b}_1$ *of* q*-type* B, *then the degree of* $\boldsymbol{b}_1$ *is equal to* $q-1$. *If it contains* (*at least*) *two irreducible components of* q*-type* A, *then their degrees are equal to* $q+1$.

Proof. Put $x_A = x_A\{(B,A)\}$ and $x_B = x_B\{(B,A)\}$. Then as in the proof of Lemma 27 we obtain that $x_A = x_B + 1$. Hence if $\boldsymbol{b}_1$ appears, then we have that $x_A \geqq 2$. Now it is easy to see that the degree of $\boldsymbol{b}_1$ is equal to either $q-1$ or $2q-1$. Let us assume that it is equal to $2q-1$. Then the multiplicity of $\boldsymbol{b}_1$ in (B,A) restricted on $\mathfrak{H}$ is one. Therefore as in the proof of Lemma 23 we see that the multiplicity of $\boldsymbol{b}_1$ in (A,B) (case (II.b)) or in (B,B) (case (V.b)) or in (D,B) (case (VIII.b)) must be at least three. Using the reciprocity theorem of Frobenius we obtain that

$$(2q-1)p \geqq 3\{(q-2)p+1\},$$

which implies that $p \leqq 7$, contradicting the assumption.

If $x_A \geqq 2$, then $x_B \geqq 1$. Therefore it is easy to see that the degrees of irreducible components of q-type A are equal to either $q+1$ or $2q+1$. But since $2q+1\,(=p)$ is not a divisor of h, the latter cannot occur.

Lemma 29. *Subcases* (II.b), (V.b) *and* (VIII.b) *cannot occur.*

Proof. Let us assume that subcase (II.b) occurs. Let us consider (A,B) restricted on $\mathfrak{H}$. Then by Lemma 21 we have that

$$(A,B)(X) = 3\sum_{i=1}^{s} \boldsymbol{c}_i(X) + \cdots \tag{68}$$

for every permutation X of $\mathfrak{H}$, where the part $\cdots$ does not contain $\boldsymbol{c}_i$ $(i = 1,\cdots,s)$ any more. Put $x_A = x_A\{(A,B)\}$ and $x_B = x_B\{(A,B)\}$. Let Q be an element of $\mathfrak{H}$ of order q. Consider (68) at Q. Then using Proposition B and Lemma 17 we have that

$$-1 = -3 + x_A - x_B.$$

If x_B is not a multiple of 4, then at least one irreducible component $\boldsymbol{b}_0$ of q-type B of (A,B) restricted on $\mathfrak{H}$ must appear in $(B,A) + \sum^{s-3}(B,D)_i$ of (II.b), since the multiplicity of $\boldsymbol{b}_0$ in $\sum_{i=1}^{s}(A,C)_i$ is, as we have noticed in the proof of Lemma 23, a multiple of 4. Then by Lemmas 14, 19 and 28 the degree of $\boldsymbol{b}_0$ is equal to $q-1$. Using the reciprocity theorem of Frobenius we see that the multiplicity of $\boldsymbol{b}_0$ in (A,B) is one. Therefore as in the proof of Lemma 23 we see that the multiplicity of $\boldsymbol{b}_0$ in $(B,A) + \sum^{s-3}(B,D)_i$ of (II.b) is at least three. Then using again the reciprocity theorem of Frobenius we obtain that

$$(q-1)p \geqq (q-2)p + 1 + 3(p-1).$$

This is a contradiction. Hence x_B must be a multiple of 4 and hence x_A cannot be a multiple of 4. Therefore at least one irreducible component $\boldsymbol{a}_0$ of q-type A of (A,B) restricted on $\mathfrak{H}$ must appear in $(B,A) + \sum^{s-3}(B,D)_i$ of (II.b), since the multiplicity of $\boldsymbol{a}_0$ in $\sum_{i=1}^{s}(A,C)_i$ is, as above, a multiple of 4. Assume that the degree of $\boldsymbol{a}_0$ is equal to $q+1$. Using the reciprocity theorem of Frobenius we see that the multiplicity of $\boldsymbol{a}_0$ in $(B,A) + \sum^{s-3}(B,D)_i$ of (II.b) is, as in the proof of Lemma 23, at least three. Let us consider $\boldsymbol{a}_0^*$. Then we have that

$$\boldsymbol{a}_0^*(X) = (A,B)(X) + \cdots$$

for every permutation X of $\mathfrak{G}$, where the sum of degrees of the part $\cdots$ equals $3p-1$. Now it is obviously impossible to find three characters of $(B,A) + \sum^{s-3}(B,D)_i$ of (II.b) to fit in this part $\cdots$. Hence we can assume that all the irreducible components of q-type A of (A,B) restricted on $\mathfrak{H}$, each of which appears in $(B,A) + \sum^{s-3}(B,D)_i$ of (II.b), have degree greater than $q+1$. Let $\boldsymbol{a}_1$ be one of such components. Then $\boldsymbol{a}_1$ must appear in (B,A) restricted on $\mathfrak{H}$ and the multiplicity of $\boldsymbol{a}_1$ in it must be one. Therefore as in the proof of Lemma 23 we see that the multiplicity of $\boldsymbol{a}_1$ in (A,B) is at least three. Using the reciprocity theorem of Frobenius we can easily see that it is at most four. An yway since $x_A = x_B + 2 \equiv 2 \pmod 4$, $x_A - 4 \equiv 2 \pmod 4$ and $x_A - 3 \equiv 3 \pmod 4$, (A,B) restricted on $\mathfrak{H}$ must possess another irreducible component, say $\boldsymbol{a}_2$, of q type A, which must appear in $(B,A) + \sum^{s-3}(B,D)_i$ of (II.b). Then $\boldsymbol{a}_2$ must appear in (B,A) restricted on $\mathfrak{H}$. Then by Lemma 28 the degrees of $\boldsymbol{a}_1$ and $\boldsymbol{a}_2$ are equal to $q+1$. This is a contradiction. Subcases (V.b) and (VIII.b) can be similarly eliminated.

2. **Remarks and consequences to** [11].

(1) Up to the present time only two permutation groups satisfying the conditions of Proposition D are known and they have degree $2l = 10$. Thus if there is no other permutation group satisfying the conditions of Proposition D, then the theorem is a trivial corollary of this fact. Anyway the theorem also can be formulated as follows: Let a permutation group $\mathfrak{X}$ of degree $2l$ satisfy the conditions of Proposition D. Let $2l+1$ be a prime number. If $\mathfrak{X}$ has a transitive extension, then $l = 5$.

(2) By the theorem the permutation group $\mathfrak{A}$ of degree q of Lemma 13 in [11] is always triply transitive. Hence the permutation group $\mathfrak{G}$ of Theorem IV in [11] is always quintuply transitive. In particular, we obtain the following improvement of Theorem V in [11]: Let p be a prime number > 23 satisfiying the following conditions: (i) $\frac{1}{2}(p-1)$ and $\frac{1}{4}(p-3)$ are also prime numbers and (ii) $p-4$ is a prime number. Then every nonsolvable transitive permutation group of degree p contains the alternating group of the same degree.

References

1. R. Brauer and C. Nesbitt, *On the modular characters of groups*, Ann. of Math. (2) **42** (1941), 556–590.

2. R. Brauer, *On groups whose order contains a prime number to the first power.* I, Amer. J. Math. **64** (1942), 401–420.

3. ———, *On groups order whose contains a prime number to the first power.* II, Amer. J. Math. **64** (1942), 421–440.

4. ———, *On permutation groups of prime degree and related classes of groups*, Ann. of Math. (2) **44** (1943), 57–79.

5. W. Burnside, *Theory of groups of finite order*, Cambridge Univ. Press, Cambridge, 1911.

6. L. E. Dickson, *Linear groups with an exposition of the Galois field theory*, Teubner, Leipzig, 1901.

7. J. S. Frame, *The double cosets of a finite group*, Bull. Amer. Math. Soc. **47** (1941), 458–467·

8. G. Frobenius, *Über die Charaktere der symmetrischen Gruppe*, S.-B. Preuss. Akad. Wiss. Berlin (1900), 516–534.

9. ———, *Über die Charaktere der mehrfach transitiven Gruppen*, S.-B. Preuss. Akad. Wiss. Berlin (1904), 528–571.

10. N. Ito, *A note on transitive groups of degree p*, Osaka Math. J. **14** (1962), 213–218.

11. ———, *Transitive permutation groups of degree $p = 2q + 1$, p and q being prime numbers*, Bull. Amer. Math. Soc. **69** (1963), 165–192.

12. W. A. Manning, *A theorem concerning simply transitive primitive groups*, Bull. Amer. Math. Soc. **35** (1929), 330–332.

13. M. Suzuki, *On finite groups with cyclic Sylow subgroups for all odd primes*, Amer. J. Math. **77** (1955), 657–691.

14. T. Tsuzuku, *On multiple transitivity of permutation groups*, Nagoya Math. J. **18** (1961), 93–109.

15. H. F. Tuan, *On groups whose orders contain a prime number to the first power*, Ann. of Math. (2) **45** (1944), 110–140.

16. H. Wielandt, *Primitive Permutationsgruppen vom Grad 2p*, Math. Z. **63** (1956), 478–485.

17. ———, *Permutationsgruppen*, Vorlesungsausarbeitungen von J. Andrė, Tübingen, 1955.

Nagoya University,
Nagoya, Japan