Journal of Mathematics,
Osaka City University
Vol. 14, No. 1.

# ON TRANSITIVE GROUPS OF DEGREE 3P

Hirosi NAGAO

(Received April 17, 1963)

A group $\mathfrak{H}$ is called a *Burnside group* or *B-group* for short when every primitive permutation group which contains the regular representation of $\mathfrak{H}$ is doubly transitive. An example of such a group was first given by Burnside ([2], Chapter XVI, Theorem VIII). In fact, he proved that a cyclic group of prime power order $p^m$ $(m>1)$ is a B-group. Since then an abelian B-group has been studied by Kochendörffer [4], Manning [5] and Wielandt [7]. As for non-abelian B-group, Wielandt [8] showed that a dihedral group is a B-group and recently Nagai [6] has proved that a non-abelian group of order $3p$ is a B-group if $p$ is a prime number of the form $2\cdot 3^a+1$ $(a>2)$.

The purpose of this paper is to prove the following

THEOREM. *Let $p$ be a prime number of the form $6l+1$ with prime number $l>7$. A non-abelian group of order $3p$ is then a B-group.*

To prove the theorem, we make use of the method of Wielandt used in [10] and the results of Schur, Frame and Nagai.

## 1. Preliminary remarks.

We shall give here a summary of the results of Schur, Wielandt and Frame which will be needed afterwards. For the proofs we refer to Wielandt [9] and Frame [3].

The following convention and notation are appropriate: The words "representations" and "characters" always refer to the representations in the field of all complex numbers and their characters. The degree of a representation $\vartheta$ or a character $\chi$ will be denoted by $\mathrm{Dg}\,\vartheta$ or $\mathrm{Dg}\,\chi$.

Let $\mathfrak{G}$ be a transitive permutation group on $\Omega=\{1, 2, \cdots, n\}$ and $\mathfrak{G}^*$ the representation of $\mathfrak{G}$ by permutation matrices. The matrices which are commutative with every $G^*\in\mathfrak{G}^*$ give the *commutator ring* $\mathfrak{V}$ of $\mathfrak{G}^*$.

Let $\mathfrak{G}_1$ denote the subgroup of $\mathfrak{G}$ consisting of all permutations of $\mathfrak{G}$ each of which fixes the letter 1 and let

$$\Delta_0=\{1\},\ \Delta_1,\ \Delta_2,\ \cdots,\ \Delta_{k-1}$$

be the sets of transitivity of $\mathfrak{G}_1$. With each set of transitivity $\Delta$ of $\mathfrak{G}_1$ we associate a matrix $V(\Delta)=(v_{ij})_{i,j=1,\cdots,n}$ with elements

$$(1)\qquad v_{ij}=\begin{cases}1 & \text{when there are } G\in\mathfrak{G} \text{ and } d\in\Delta \text{ such that}\\ & 1^G=j \text{ and } d^G=i\,,\\ 0 & \text{otherwise.}\end{cases}$$

LEMMA 1 ([9], 28.4). *$\{V(\Delta_0), V(\Delta_1), \cdots, V(\Delta_{k-1})\}$ is a linear basis of the commutator ring $\mathfrak{B}$ of $\mathfrak{G}^*$.*

Let $\Delta$ be a given set of transitivity of $\mathfrak{G}_1$. We denote by $\Delta'$ the set of letters $\{1^{H^{-1}}|H\in\mathfrak{G},\ 1^H\in\Delta\}$. Then $\Delta'$ is also a set of transitivity of $\mathfrak{G}_1$ with the same length as $\Delta$ and $(\Delta')'=\Delta$. The matrix $V(\Delta')$ is the transposed matrix of $V(\Delta)$, i.e. $V(\Delta')=V(\Delta)'$.

LEMMA 2 ([9], 28.10). *For two given sets of transitivity $\Delta_i$, $\Delta_j$ of $\mathfrak{G}_1$*

$$(2)\qquad \operatorname{tr}\left(V(\Delta_i)'V(\Delta_j)\right)=\delta_{ij}n|\Delta_i|$$

*where $|\Delta_i|$ denotes the length of $\Delta_i$.*

Now let

$$(3)\qquad \mathfrak{G}^*=\sum_{i=0}^{r-1}e_i\vartheta_i$$

be the complete reduction of $\mathfrak{G}^*$ into irreducible representations. We assume that $\vartheta_0$ is the principal representation of $\mathfrak{G}$. Then $e_0$ is equal to 1.

LEMMA 3 ([9], 29.2). *Let $k$ be the number of the sets of transitivity of $\mathfrak{G}_1$. Then*

$$k=\sum_{i=0}^{r-1}e_i^2\,.$$

From this lemma we have immediately

LEMMA 4. *$\mathfrak{G}$ is doubly transitive if and only if $r=2$ and $e_0=e_1=1$.*

Corresponding to the reduction (3) of $\mathfrak{G}^*$ we have the complete reduction of $\mathfrak{B}$:

$$(4)\qquad \mathfrak{B}=\sum_{\mu=0}^{r-1}z_\mu\mathfrak{B}_\mu$$

where $z_\mu=\operatorname{Dg}\vartheta_\mu$ and $\operatorname{Dg}\mathfrak{B}_\mu=e_\mu$. In fact there is a unitary matrix $U$ such that

$$(5)\qquad U^{-1}V(\Delta_i)U=\begin{pmatrix}\ddots & & 0\\ & V_\mu(\Delta_i)\times E_{z_\mu} & \\ 0 & & \ddots\end{pmatrix}$$

where $E_{z_\mu}$ is the unit matrix of degree $z_\mu$ and $V(\Delta_i)\to V_\mu(\Delta_i)$ gives an irreducible representation $\mathfrak{V}_\mu$ of $\mathfrak{V}$. From (4) we have

LEMMA 5 ([9], 29.3, 29.5). *$\mathfrak{V}$ is commutative if and only if $e_0=e_1=\cdots=e_{r-1}=1$. Especially if $k\leq 4$ then $\mathfrak{V}$ is commutative.*

Let $\mathfrak{C}_j$ be a class of conjugate elements of $\mathfrak{G}$ and let $C_j=\sum_{G\in\mathfrak{C}_j} G^*$. If $\mathfrak{V}$ is commutative then each $V(\Delta_i)$ is a linear combination of $C_j$ with rational coefficients: $V(\Delta_i)=\sum_j x_j C_j$. The matrices of $\mathfrak{V}$ are transformed by a unitary matrix into diagonal form. If

$$U^{-1}V(\Delta_i)U=\begin{pmatrix}\ddots & & & 0 \\ & \ddots & & \\ & & a_\mu E_{z_\mu} & \\ & & & \ddots \\ 0 & & & & \ddots\end{pmatrix} \tag{6}$$

then

$$a_\mu=\sum_j x_j\frac{|\mathfrak{C}_j|\chi_\mu(G_j)}{z_\mu}\qquad (x_j\text{: rational numbers}) \tag{7}$$

where $|\mathfrak{C}_j|$ denotes the number of elements of $\mathfrak{C}_j$, $G_j\in\mathfrak{C}_j$ and $\chi_\mu$ denotes the character of $\vartheta_\mu$.

Frame [3] gave a number theoretical relationship between $n=|\Omega|$, $n_i=|\Delta_i|$ and $z_i=\mathrm{Dg}\,\vartheta_i$.

LEMMA 6 ([3]). *The number*

$$n^{k-1}\prod_{i=1}^{k-1}n_i\Big/\prod_{i=1}^{r-1}z_i^{e_i^2}$$

*is a rational integer.*

We now conclude this section with some more remarks.

REMARK 1. The characteristic roots of $V(\Delta_i)$, $V(\Delta_i)'V(\Delta_j)$ are algebraic integers.

REMARK 2. If $z_i=\mathrm{Dg}\,\vartheta_i$ is different from all other $z_j=\mathrm{Dg}\,\vartheta_j$ in (3), then $\mathrm{tr}\,V_\mu(\Delta_i)$ in (5) is a rational integer.

REMARK 3 ([9], 8.6). If $\mathfrak{G}$ is primitive and not a regular group of prime degree then $n_i=|\Delta_i|>1$ for $i\neq 0$.

REMARK 4 ([9], 18.7). If $n_i=|\Delta_i|=2$ for some $i$ then $\mathfrak{G}$ contains a regular normal subgroup of index 2.

## 2. Former results of Nagai.

Let $\mathfrak{H}$ be a non-abelian group of order $3p$ where $p$ is a prime number greater than 3: $\mathfrak{H}=\{A, B\}$, $A^p=B^3=1$, $B^{-1}AB=A^j$ ($j^3\equiv 1$, $j\not\equiv 1 \pmod p$)). In what is to follow we shall consider a permutation group $\mathfrak{G}$ as follows:

($*$) *The group $\mathfrak{G}$ is a primitive permutation group of degree $3p$ which contains $\mathfrak{H}$ as its regular subgroup and is not doubly transitive.*

We now give a summary of the former results of Nagai concerning the groups as above, which will be needed afterwards.

LEMMA 7 ([6], (a), (b)). *Under the assumption ($*$) the order of $\mathfrak{G}$ contains the prime $p$ to the first power and the centralizer of a Sylow $p$-subgroup $\mathfrak{P}$ of $\mathfrak{G}$ coinsides with $\mathfrak{P}$.*

By this lemma we can apply the results of Brauer [1] to our case. Without loss of generality we may assume that $\mathfrak{G}$ contains $P=(1, \cdots, p)$ $(p+1, \cdots, 2p)$ $(2p+1, \cdots, 3p)$. Let $\mathfrak{N}=\mathfrak{N}(\mathfrak{P})$ be the normalizer of $\mathfrak{P}=\{P\}$, and let $q=|\mathfrak{N}:\mathfrak{P}|$. Then $\mathfrak{N}$ is generated by $P$ and an element $Q$ of order $q$ and they satisfy

$$Q^{-1}PQ = P^{\gamma^t} \tag{8}$$

where $\gamma$ is a primitive root (mod $p$) and $t$ is a positive integer such that

$$tq = p-1\,. \tag{9}$$

The irreducible characters of $\mathfrak{G}$ are of four different types:

I. Character $A_\rho$ of degree $a_\rho=u_\rho p+1$.
II. Character $B_\sigma$ of degree $b_\sigma=v_\sigma p-1$.
III. Character $C^{(\nu)}$ of degree $(wp+\delta)/t$ $(\delta=\pm 1)$.
IV. Character $D_\tau$ of degree $d_\tau=x_\tau p$.

The characters of type III are called *exceptional characters.*

The characters of $\mathfrak{N}$ are easily determined. Let $\omega$ be a primitive $q$th root of unity. There are $q$ linear characters $\omega_\mu$ $(\mu=0, 1, 2, \cdots, q-1)$ of $\mathfrak{N}$ which are defined by

$$\omega_\mu(Q^j) = \omega^{\mu j}\,, \qquad \omega_\mu(P^i) = 1$$

and the other irreducible characters are $t$ algebraically conjugate characters $Y^{(\nu)}$ of degree $q$.

LEMMA 8 ([1], Lemma 3). *The restriction $A_\rho|\mathfrak{N}$ of $A_\rho$ to $\mathfrak{N}$ contains $u_\rho+1$ of the $\omega_\mu$, $B_\sigma|\mathfrak{N}$ contains $v_\sigma-1$ of the $\omega_\mu$, $C^{(\nu)}|\mathfrak{N}$ contains $(w+\delta)/t$ of the $\omega_\mu$ and $D_\tau|\mathfrak{N}$ contains $x_\tau$ of the $\omega_\mu$.*

Now let $\Pi$ be the character of the permutation representation $\mathfrak{G}^*$ of $\mathfrak{G}$ and let

$$\Pi = X_0+\sum_{i=1}^{k-1} e_i X_i \tag{10}$$

be the complete reduction of $\Pi$ where $\chi_0$ is the principal character of $\mathfrak{G}$. Since $\mathfrak{G}$ is not doubly transitive $k \geq 3$.

LEMMA 9 ([6], (c), (d)). *In* (10), *every constituent* $\chi_i$ *is not exceptional and* $Dg\,\chi_i > 1$ *for* $i \neq 0$.

From this lemma we have easily the following possibilities of the complete reduction of $\Pi$ ([6], (g), (h)):

Case I: $\Pi = \chi_0 + \chi_1 + 2\chi_2$, $Dg\,\chi_1 = p+1$, $Dg\,\chi_2 = p-1$.
Case II: $\Pi = \chi_0 + \chi_1 + \chi_2 + \chi_3$, $Dg\,\chi_1 = p+1$, $Dg\,\chi_2 = Dg\chi_3 = p-1$.
Case III: $\Pi = \chi_0 + \chi_1 + \chi_2$, $Dg\,\chi_1 = 2p-1$, $Dg\,\chi_2 = p$.
Case IV: $\Pi = \chi_0 + \chi_1 + \chi_2$, $Dg\,\chi_1 = p-1$, $Dg\,\chi_2 = 2p$.
Case V: $\Pi = \chi_0 + \chi_1 + 2\chi_2$, $Dg\,\chi_1 = p-1$, $Dg\,\chi_2 = p$.
Case VI: $\Pi = \chi_0 + \chi_1 + \chi_2 + \chi_3$, $Dg\,\chi_1 = p-1$, $Dg\,\chi_2 = Dg\chi_3 = p$.

Under some condition the possility of Case IV can be excluded.

PROPOSITION 1 ([6], (j)). *Let* $\mathfrak{G}$ *be a group which satisfies the condition* (*). *If* $p > 7$ *and* $4p$ *is not of the form* $3c^2+1$ *then Case IV does not occur.*

The possibility of Case V will be easily excluded from the following lemma.

LEMMA 10 ([6], (e)). $\Pi$ *restricted to* $\mathfrak{N}$ *contains just three different linear characters* $\omega_\mu$, *one of which is the principal character* $\omega_0$.

If $\Pi$ decomposes as in Case V, then from Lemma 8 $\Pi$ contains some $\omega_\mu$ with multiplicity 2. This contradicts Lemma 10. Thus we have

PROPOSITION 2. *Let* $\mathfrak{G}$ *be a group which satisfies the condition* (*). *Then Case V does not occur.*

### 3. Remaining cases.

Under the condition (*) we shall now consider the cases except Case IV and V separately.

*Case VI*: Suppose $\Pi$ decomposes as in Case VI. Since $\Pi$ is a rational character and $\chi_1$ is its only constituent of degree $p-1$, $\chi_1$ is also a rational character and $\chi_2$ and $\chi_3$ are both rational or algebraically conjugate.

Now, from Lemma 8, $\chi_i$ $(i=2, 3)$ restricted to $\mathfrak{N}$ contains one linear character $\omega_i$ $(i=2, 3)$ of $\mathfrak{N}$ and for an element $B$ of order 3 in $\mathfrak{H}$

$$0 = \Pi(B) = 1 + \omega_2(B) + \omega_3(B)\,.$$

Therefore $\chi_i(B) = \omega_i(B)$ $(i=2, 3)$ is a primitive third root of unity. Thus

$\chi_i$ $(i=2, 3)$ is not rational and the field $\mathrm{P}(\chi_i(G))$ which is obtained by adjoining $\{\chi_i(G) \mid G \in \mathfrak{G}\}$ to the field P of rational numbers is of rank 2 over P and not real since it contains a primitive third root of unity $\chi_i(B)$. In this way we can see that

$$\chi_3(G) = \overline{\chi_2(G)} \tag{11}$$

for all $G \in \mathfrak{G}$.

From Lemma 3, the number of the sets of transitivity of $\mathfrak{G}_1$ is now 4, therefore, from Lemma 5, the commutator ring $\mathfrak{V}$ of $\mathfrak{G}^*$ is commutative. Further there is a set of transitivity $\Delta(\neq \Delta_0)$ such that $\Delta' = \Delta$. Then $V(\Delta) = V(\Delta)'$ and the characteristic roots of $V(\Delta)$ are all real. Let $U$ be a unitary matrix which transforms $V(\Delta)$ in diagonal form:

$$U^{-1}V(\Delta)U = \begin{pmatrix} v & & & 0 \\ & aE_{p-1} & & \\ & & bE_p & \\ 0 & & & cE_p \end{pmatrix}$$

where $v = |\Delta|$. From Remark 1 and 2, $a$ is a rational integer and from (7) and (11) $c = \bar{b}$. On the other hand, $b$ is real therefore $b = c$.

Now applying (2) to $\mathrm{tr}\,(V(\Delta_0)'V(\Delta)) = \mathrm{tr}\,(V(\Delta))$ and $\mathrm{tr}\,(V(\Delta)'V(\Delta))$ we have

$$\text{(i)} \qquad 0 = v + (p-1)a + 2pb\,,$$

$$\text{(ii)} \qquad 3pv = v^2 + (p-1)a^2 + 2pb^2\,.$$

From (i), $b$ is a rational integer and $v \equiv a \pmod p$.
From (ii)

$$a^2 < 3pv/(p-1) < 9p^2/(p-1) \leq p^2 \qquad \text{if} \quad p > 7$$

and hence $|a| < p$ if $p > 7$. In the following we assume $p > 7$. Then combining $v \equiv a \pmod p$ and $|a| < p$ we have

$$a = v - \alpha p \qquad (\alpha = 0, 1, 2 \text{ or } 3)\,. \tag{12}$$

Substituting $v = a + \alpha p$ in (i) we have $b = -(a+\alpha)/2$. Substitute these in (ii). Then we have

$$p(6\alpha - 2\alpha^2) = 3a^2 + 6(\alpha-1)a + \alpha^2\,. \tag{13}$$

If $\alpha = 0$, then $a = 0$ or 2 by (13) and hence $v = 0$ or 2 by (12). Since $v = |\Delta| > 0$, $v = 2$. Then from Remark 4 $\mathfrak{G}$ can not be primitive. If $\alpha = 1$ or 2, then we have $4p = 3a^2 + 1$ or $3(a+1)^2 + 1$ by (13). If $\alpha = 3$, then $a = -3$ or $-1$ by (13) and $v = 3p - 3$ or $3p - 1$ by (12). Since the lengths of the other three sets of transitivity are not all 1 (Remark 3), this is impossible. Thus we have

PROPOSITION 3. *Let $\mathfrak{G}$ be a permutation group which satisfies the condition* (*). *If $p>7$ and $4p$ is not of the form $3c^2+1$ then Case VI does not occur.*

*Case III*: Suppose $\Pi$ decomposes as in Case III. The number of the sets of transitivity of $\mathfrak{G}$ is now 3. Therefore there is a set of transitivity $\Delta\ (\neq\Delta_0)$ with length $v\leq(3p-1)/2$. Let $U$ be a unitary matrix which transforms $V(\Delta_i)$ in diagonal form:

$$U^{-1}V(\Delta)U=\begin{pmatrix} v & & 0 \\ & aE_{2p-1} & \\ 0 & & bE_p \end{pmatrix}$$

From Remark 1 and 2, $a$ and $b$ are rational integers and from (2) we have

$$\text{(i)} \qquad 0=v+(2p-1)a+pb\,,$$

$$\text{(ii)} \qquad 3pv=v^2+(2p-1)a^2+pb^2\,.$$

From (i), we have $v\equiv a \pmod p$. From (ii), we have

$$a^2<3pv/(2p-1)<9p^2/(2p-1)\leq p^2 \qquad \text{if} \quad p\geq 5$$

and hence $|a|<p$. Now assume $p\geq5$. Since $v\leq(3p-1)/2<2p$, combining $v\equiv a \pmod p$ and $|a|<p$ we have

$$a=v-\alpha p \qquad (\alpha=0,\ 1 \text{ or } 2)\,. \tag{14}$$

Substituting $v=a+\alpha p$ in (i) we have $b=-(\alpha+2a)$. Substitute these in (ii). Then we have

$$p(3\alpha-\alpha^2)=6a^2+3(2\alpha-1)a+\alpha^2\,. \tag{15}$$

If $\alpha=0$, then $a=v=0$ by (15) and (14). This is impossible. If $\alpha=1$ or 2, we have $-p\alpha^2\equiv\alpha^2 \pmod 3$ by (15). Since $p\equiv1 \pmod 3$, $2\alpha^2\equiv0 \pmod 3$. This is a contradiction. Thus we have

PROPOSITION 4. *Let $\mathfrak{G}$ be a permutation group which satisfies the condition* (*). *If $p\geq5$ then Case III does not occur.*

*Case I*: Let $\Pi$ decompose as in Case I. We now assume that $p$ is a prime number of the form $6l+1$ with prime number $l\neq2$. In the following we shall show that $l\leq7$ follows from our assumption.

The index $q=|\mathfrak{N}:\mathfrak{P}|$ is a divisor of $p-1$ and a multiple of 3 since $\mathfrak{N}\geq\mathfrak{H}$. Therefore $q=3$, 6, $3l$ or $6l$. When $q=3$ or 6 Case I does not occur by [6], (i). Suppose now that $q=3l$ or $6l$. Let $L$ be an element of order $l$ in $\mathfrak{N}$. The lengths of the sets of transitivity of $\{L\}$ are all $l$ but three sets of transitivity of length 1. Without loss of generality we may assume that $L\in\mathfrak{G}_1$. Then every set of transitivity of $\mathfrak{G}_1$ is a union of some sets of transitivity of $\{L\}$. The number of the sets of transitivity of $\mathfrak{G}_1$ is now 6 and the lengths of the sets of transitivity of $\mathfrak{G}_1$ are

(A) $n_0=1,\ n_1=m_1l+1,\ n_2=m_2l+1,\ n_3=m_3l,\ n_4=m_4l,\ n_5=m_5l$,

or (B) $n_0=1,\ n_1=m_1l+2,\ n_2=m_2l,\ n_3=m_3l,\ n_4=m_4l,\ n_5=m_5l$.

By Remark 3 and 4, each $m_i$ here is not 0, and from $\sum_{i=0}^{5} n_i=3p$ it follows that $\sum_{i=0}^{5} m_i=18$. Therefore in either case (A) or (B) there is at least one $m_i$ $(3\leq i\leq 5)$ such that $m_i\leq 5$. Let $\Delta$ be a set of transitivity of $\mathfrak{G}_1$ with length $ml\leq 5l$, and let $U$ be a unitary matrix which transforms $V(\Delta)$ in the following form:

$$U^{-1}V(\Delta)U=\begin{pmatrix} ml & & 0 \\ & aE_{p+1} & \\ 0 & & \begin{pmatrix} b & e \\ d & c\end{pmatrix}\times E_{p-1}\end{pmatrix}.$$

Then from (2) we have

$$\text{(i)}\qquad 0=ml+(p+1)a+(p-1)(b+c),$$

$$\text{(ii)}\qquad 3pml=m^2l^2+(p+1)a^2+(p-1)(|b|^2+|c|^2+|d|^2+|e|^2).$$

By Remark 2, $a$ is a rational integer and, by (i), (ii) above and Remark 1, $b+c$ and $|b|^2+|c|^2+|d|^2+|e|^2$ are also rational integers. From (i) we have $a\equiv 0 \pmod{l}$. Let $a=ul$. If $u=0$, then, by (i), $0=m+6(b+c)$. But this is impossible since $m\leq 5$. Thus we have $u\neq 0$. From (ii) we have now

$$((18-m)l+3)m\geq 2(3l+1)l.$$

The left hand side considered as a function in $m\leq 5$ takes the maximum $65l+15$ at $m=5$. Thus we have

$$65l+15\geq 2(3l+1)l$$

and hence $10\geq l$. In this way, we have

PROPOSITION 5. *Let $\mathfrak{G}$ be a permutation group which satisfies the condition* (*). *If $p$ is of the form $6l+1$ where $l$ is a prime number greater than 7, then Case I does not occur.*

*Case II*: Let $\Pi$ decompose as in Case II. We assume that $p$ is a prime number of the form $6l+1$ with prime number $l\neq 2$, and we shall show that $l\leq 7$.

The number of the sets of transitivity of $\mathfrak{G}_1$ is now 4. In the same way as in Case I, we can see that the lengths of the sets of transitivity of $\mathfrak{G}_1$ are as follows:

(A) $n_0=1,\ n_1=m_1l+1,\ n_2=m_2l+1,\ n_3=m_3l,$

or (B) $n_0=1,\ n_1=m_1l+2,\ n_2=m_2l,\ n_3=m_3l\ .$

*Case A*: From Lemma 6, it follows that $(m_1l+1)(m_2l+1)m_3/2^3(3l+1)l$ is an integer. Therefore $m_3\equiv 0 \pmod{l}$ and we have $l\leq m_3\leq 16$. If $l=13$ or 11, we have $m_3=l$ since $m_3$ is a multiple of $l$ and less than 17. Then $(m_1l+1)(m_2l+1)/2^3(3l+1)$ is an integer. On the other hand, for $m_3=l=13$ or 11, $m_1+m_2=5$ or 7. By a direct calculation we can see that $(m_1l+1)(m_2l+1)/2^3(3l+1)$ is not an integer for any such $m_1$, $m_2$. This is a cotradiction and we have $l\leq 7$.

*Case B*: Let $\Delta$ be a set of trasitivity of $\mathfrak{G}_1$ with length $n_2$ or $n_3$, and let $U$ be a unitary matrix which transforms the matrices of $\mathfrak{V}$ in diagonal form:

$$U^{-1}V(\Delta)U=\begin{pmatrix} m & & & 0 \\ & aE_{p+1} & & \\ & & bE_{p-1} & \\ 0 & & & cE_{p-1}\end{pmatrix}. \tag{15}$$

We have then

$$\text{(i)}\qquad 0=ml+(p+1)a+(p-1)(b+c)\,,$$

$$\text{(ii)}\qquad 3pml=m^2l^2+(p+1)a^2+(p-1)(|b|^2+|c|^2)\,.$$

Here $a$, $b+c$ and $|b|^2+|c|^2$ are rational integers. By (i), $a\equiv 0 \pmod{l}$. Let $a=ul$.

We first consider the case $u\neq 0$ for $\Delta=\Delta_2$ or $\Delta_3$. From (ii), we have

$$((18-m)l+3)m\geq 2(3l+1)u^2l\geq 2(3l+1)l\,. \tag{16}$$

The left hand side here considered as a function in integral variable $m$ takes the maximum $81l+27$ at $m=9$. Thus we have

$$81l+27\geq 2(3l+1)l$$

and hence $l<14$. The cases $l=13$ and $l=11$ will be discussed later.

We next consider the case $u=0$ for $\Delta=\Delta_2$ and $\Delta_3$. From (i), we now have $0=m+6(b+c)$. Therefore $m\equiv 0 \pmod{6}$. But, since $m\leq 16$, $m=6$ or 12. If $m=12$, for instance $m_2=12$, then it must hold that $m_3=6$,

$m_1=0$. This is a contradiction. Thus $m_2=m_3=6$. If $m=6$, then $ml=6l=p-1$. By (i), $b+c=-1$ and, by (ii), $|b|^2+|c|^2=2p+1$. If $b$ is imaginary then we have $c=\bar{b}$ from (7). Therefore $|b|^2+|c|^2=2|b|^2=2p+1$. This is a contradiction since $b$ is an algebraic integer. Thus $b$ must be real. Then $2p+1=b^2+c^2=b^2+(b+1)^2=2b(b+1)+1$ and hence $p=b(b+1)=-bc$. In this way, we see that $b$ and $c$ are the roots of the quadratic equation

$$x^2+x-p = 0\,. \tag{17}$$

Now we proved that if

$$U^{-1}V(\Delta_i)U = \begin{pmatrix} p-1 & & & 0 \\ & 0E_{p+1} & & \\ & & b_iE_{p-1} & \\ 0 & & & c_iE_{p-1} \end{pmatrix} \qquad (i = 2, 3)$$

then $b_i$ and $c_i$ are the roots of (17). If $b_2=b_3$ and $c_2=c_3$ then $V(\Delta_2)=V(\Delta_3)$ which contradicts the linear independence of $V(\Delta_i)$. Thus we have $b_2=c_3$ and $c_2=b_3$. Since the characteristic roots of $V(\Delta_2)$ are all real, $V(\Delta_2)'=V(\Delta_2)$. Therefore by (2)

$$\begin{aligned} 0 &= \operatorname{tr}(V(\Delta_2)'V(\Delta_3)) = \operatorname{tr}(V(\Delta_2)V(\Delta_3)) \\ &= (p-1)^2+2(p-1)b_2c_2 = (p-1)^2-2(p-1)p\,. \end{aligned}$$

This is a contradiction. Thus we have proved that for $\Delta=\Delta_2$ or $\Delta_3$ $u\neq 0$ and then we may assume that $l=13$ or 11.

Now when $m_2$ or $m_3$ is less than 6, let $\Delta$ in (15) be a set of transitivity $\Delta_i$ ($i=2$ or 3) such that $m_i=m<6$. The left hand side in (16) then takes the maximum $65l+15$ at $m=5$ under the condition $m\leq 5$. Thus we have $l<11$, i.e. $l\leq 7$.

Now assume that $m_2$ and $m_3\geq 6$, then $m_1\leq 6$. From (16) we have $13\geq u^2l$. Since $l=13$ or 11, $u=\pm 1$ and hence $a=\pm l$. From (i), we then have

$$0 = m\pm(p+1)+6(b+c)\,.$$

Combining this and $p+1\equiv 2 \pmod 6$, we have $m\equiv \pm 2 \pmod 6$. In this way, we see that $m_i\equiv\pm 2 \pmod 6$ for $i=2, 3$. Hence $m_i=8$, 10 or 14 ($i=2, 3$), but $m_i=14$ is impossible. If $m_2=10$, then $m_3=8$ and $m_1=0$. This is impossible. In the same way, we have $m_3\neq 10$. Thus we have $m_1=2$, $m_2=m_3=8$. Then, for $l=11$, 13, $(m_1l+2)m_2m_3/2^3(3l+1)$ is not an integer. This is a contradiction. Thus we have

PROPOSITION 6. *Let $\mathfrak{G}$ be a permutation group which satisfies the* *condition* (*). *If* $p$ *is of the form* $6l+1$ *where* $l$ *is a prime number greater than* 7, *then Case II does not occur.*

*Proof of Theorem.* In order to prove Theorem, by Propition 1~6, it is sufficient to show that if $p=6l+1$ is a prime number as in Theorem then $4p$ is not of the form $3c^2+1$. If $4p=3c^2+1$ with positive integer $c$, then $24l+4=3c^2+1$. Thus we have $8l=(c-1)(c+1)$. Therefore $c\equiv\pm1$ (mod $l$). Let $c=xl\pm1$. Then $8=x(xl\pm2)$ and hence

$$l-2\leq xl\pm2\leq 8, \qquad l\leq 10.$$

Thus we have $l\leq 7$ and this is a contradiction.

## References


1. R. Brauer, *On permutation groups of prime degree and related classes of groups*, Ann. of Math. **44** (1943), 57–79.
2. W. Burnside, Theory of groups of finite order, Cambridge Univ. Press (1911).
3. J. S. Frame, *The double cosets of a finite group*, Bull. Amer. Soc. **47** (1941), 458–467.
4. R. Kochendörffer, *Untersuchungen über eine Vermutung von W. Burnside*, Schriften Math. Sem. Inst. Angew. Math. Univ. Berlin **3** (1937), 155–180.
5. D. Manning, *On simply transitive groups with trasitive abelian subgroups of the same degree*, Trans. Amer. Math. Soc. **40** (1936), 324–342.
6. O. Nagai, *On transitive groups that contain non-abelian regular subgroups*, Osaka Math. J. **13** (1961), 199–207.
7. H. Wielandt, *Zur Theorie der einfach transitiven Permutationsgruppen*, Math. Z. **40** (1935), 582–587.
8. ——————, *Zur Theorie der einfach transitiven Permutationsgruppen, II*, Math. Z. **52** (1950), 384–393.