Bannai, E.
Osaka J. Math.
13 (1976), 123–129

ON MULTIPLY TRANSITIVE PERMUTATION GROUPS IV

EIICHI BANNAI*)

(Received February 12, 1975)

Introduction

By combining the results of Miyamoto [5] and Bannai [1, 2], we have obtained the following theorem ([2, Main Theorem]) which is an odd prime version of a theorem of M. Hall [3].

Theorem. Let p be an odd prime. Let G be a $2p$-ply transitive permutation group such that $G_{1,2,\cdots,2p}$ (=the pointwise stabilizer of $2p$ points) is of order prime to p. Then G is one of $S_n(2p\leq n\leq 3p-1)$ and $A_n(2p+2\leq n\leq 3p-1)$, where S_n and A_n denote the symmetric and alternating groups of degree n.

The purpose of this paper is to generalize the above theorem. Namely, we will prove the following theorem.

Theorem 1. *Let p be an odd prime. Let G be a $2p$-ply transitive permutation group such that either*
(i) *each element in G of order p fixes at most $2p+(p-1)$ points, or*
(ii) *a Sylow p subgroup of $G_{1,2,\cdots,2p}$ is cyclic.*
Then G is one of $S_n(2p\leq n\leq 4p-1)$ and $A_n(2p+2\leqq n\leq 4p-1)$.

Note that Theorem 1 (i) and Theorem 1 (ii) are some odd prime versions of a theorem of Nagao [6] and a theorem of Noda and Oyama [7] respectively.

The essential part of the proof of Theorem 1 (i) is picked up as follows:

Theorem A. *Let p be an odd prime. Then there exists no $(p+3)$-ply transitive permutation group G on a set $\Omega=\{1,2,\cdots,n\}$ which satisfies the following two conditions:*
(1) *a Sylow p subgroup $P(\neq 1)$ of $G_{1,2,\cdots,p+3}$ fixes at most $p-1$ points in $\Omega-\{1,2,\cdots,p+3\}$, and P is semiregular on $\Omega-I(P)$, where $I(P)$ denotes the set of the points which are fixed by any element of P.*
(2) $|\Omega-I(P)|\not\equiv p \pmod{p^2}$.

Note that Theorem A generalizes Lemma 1.5 in Miyamoto [5] to some

*) Supported in part by the Sakkokai Foundation.

extent. We remark that in our proof of Theorem A the idea of Miyamoto and Nagao ingeniously using the formula of Frobenius (cf. [5, Lemma 1.1]) is essential.

1. Proof of Theorem A

Let G and P be as in the assumption of Theorem A. Then, we will derive a contradiction.

By the assumptions, and by using Theorem 1[1)] in [1] (if $|\Omega-I(P)|\equiv 0 \pmod{p^2}$) we may assume that P is of order p and is generated by the element

$$a=(1)\cdots(p+3)\cdots(p+3+r)(p+4+r,\ \cdots,\ 2p+3+r)\cdots,$$

where $I(P)=I(a)=\{1, 2, \cdots, p+3+r\}$ and $0\leq r\leq p-1$.

By the lemma of Jordan-Witt, we get $N_G(P)^{I(P)}\geq A^{I(P)}$. Therefore, $C_G(P)^{I(P)}\geq A^{I(P)}$, because of $|P|=p$.

First, from (1.1) to (1.4), we only treat the case $|\Omega-I(P)|\not\equiv 0 \pmod{p^2}$. Similar results will be proved later as (1.1′) to (1.4′) for the case $|\Omega-I(P)|\equiv 0 \pmod{p^2}$.

(1.1) $C_G(a)$ is transitive on $\Omega-I(P)$.

By the remark following Lemma 1.1 in [5], we get the following formula for any *p-ply* transitive permutation groups X on a set Ω:

$$\frac{|X|}{p}=\sum_{x\in X}\alpha_p(x)\geq\sum_i\frac{|X|}{|C_X(u_i)|}\cdot\frac{1}{p}\cdot\sum_y{}'\alpha^*(y),$$

where $\alpha_p(x)$ denotes the number of p cycles in the cylce structure of x, u_i ranges all representatives of conjugacy classes (in X) of elements of order p, y ranges all p'-elements in $C_X(u_i)$ and $\alpha^*(y)$ denotes the number of the fixed points of y (acting) on $\Omega-I(u_i)$.

In our situation, let us take $X=G$. Since we are assuming that $|\Omega-I(P)|\not\equiv 0 \pmod{p^2}$, G contains an element of order p which fixes less than $|I(a)|$ points. Hence,

$$\frac{|G|}{p}=\sum_{x\in G}\alpha_p(x)\gneqq\frac{|G|}{|C_G(a)|}\cdot\frac{1}{p}\cdot\sum_y{}'\alpha^*(y).$$

Now, $\sum_y{}'\alpha^*(y)\geq\sum_{y\in C_G(a)}\alpha^*(y)-p\cdot\sum_{y\in C_G(a)}$(the number of p cycles in $y^{I(a)}$). Since $C_G(a)^{I(a)}\geq A^{I(a)}$ and $A^{I(a)}$ is *p-ply* transitive (on $I(a)$), we get $p\cdot\sum_{y\in C_G(a)}$(the number of p cycles in $y^{I(a)}$)$=|C_G(a)|$ by the formula of Frobenius. On the other hand,

1) Theorem 1 in [1] is stated only for the case $r=0$. But it is evident that the assertion is also true for $1\leq r\leq p-1$.

$$\sum_{y \in C_G(a)} \alpha^*(y) = t_a |C_G(a)| ,$$

where t_a is the number of orbits of $C_G(a)$ on $\Omega - I(a)$. Hence, we get

$$\frac{|G|}{p} \gneqq \frac{1}{p}(t_a - 1)|G| .$$

Therefore, $t_a=1$, and so $C_G(a)$ is transitive on $\Omega - I(a)$.

(1.2) $C_{G_1}(a)$ is transitive on $\Omega - I(a)$. Moreover, if j is one of 0, 1, 2 and 3 and if $p+3+r-j \geq p+2$, then $C_{G_{1,2,\dots,j}}(a)$ is transitive on $\Omega - I(a)$.

Proof is quite similar as in (1.1). Here we have only to notice that $C_{G_{1,2,\dots,j}}(a)^{I(a)-\{1,2,\dots,j\}} \geq A^{I(a)-\{1,2,\dots,j\}}$ and so is p-*ply* transitive.

Since $C_G(a)$ is transitive on $\Omega - I(a)$, a normal subgroup $C_{G_{1,2,\dots,p+3+r}}(a)$ is half transitive on $\Omega - I(a)$. Let $\Delta_1, \Delta_2, \cdots, \Delta_k$ be the orbits of $C_{G_{1,2,\dots,p+3+r}}(a)$ on $\Omega - I(a)$.

(1.3) $k \leq 2$.

Since $C_{G_{1,2,\dots,p+3+r}}(a)$ acts trivially on the set $\{\Delta_1, \Delta_2, \cdots, \Delta_k\}$, $C_G(a)^{I(a)}$ acts on the set $\{\Delta_1, \Delta_2, \cdots, \Delta_k\}$ transitively. Let Y be the subgroup of $C_G(a)$ which fixes Δ_1. Then, $|C_G(a)^{I(a)}: Y^{I(a)}| = k$. Since $C_{G_1}(a)$ is also transitive on $\Omega - I(a)$, $|C_{G_1}(a)^{I(a)}: Y_1^{I(a)}|$ is $\geq k$. But, in order that this holds, Y must be transitive on $I(a)$. Similarly, if $r \geq 1$, then $|C_{G_{1,2}}(a)^{I(a)}: Y_{1,2}{}^{I(a)}| \geq k$ by (1.2), and so, Y must be doubly transitive on $I(a)$. On the other hand, we may assume without loss of generality that $Y^{I(a)}$ contains an element of just a p cycle. If $r \geq 1$, then since there exists no nontrivial doubly transitive permutation group of degree $p+3+r$ containing an element of a p cycle we get $Y^{I(a)} \geq A^{I(a)}$ (cf. [8, Theorem 13.9]). On the other hand, if $r=0$, then $Y^{I(a)}$ becomes triply transitive by a lemma of Livingstone and Wagner [4, Lemma 6]. So, in any way, we get $Y^{I(a)} \geq A^{I(a)}$. Hence $k \leq 2$.

(1.4) $C_{G_{1,2,\dots,p,\{p+1,p+2\},p+3,\dots,p+3+r}}(a)$ is transitive on $\Omega - I(a)$.

If $C_G(a)^{I(a)} = A^{I(a)}$, then $k=1$ and $C_{G_{1,2,\dots,p+3+r}}(a)$ is transitive on $\Omega - I(a)$, so we have the assertion. If $C_G(a)^{I(a)} = S^{I(a)}$, then $k=1$ or 2. In any way, $C_{G_{1,2,\dots,p,\{p+1,p+2\},p+3,\dots,p+3+r}}(a)$ is transitive on $\Omega - I(a)$.

Next, let us assume that $|\Omega - I(P)| \equiv 0 \pmod{p^2}$. Then the order of a Sylow p subgroup of $G_{1,2,3}$ is p^2 by the assumption and Theorem 1 in [1].

(1.1′) If $p+3+r \geq 2p$, then $C_G(a)$ is either transitive or has two orbits on $\Omega - I(a)$. If $(p+2 \leq) p+3+r \leq 2p-1$, then $C_G(a)$ has two orbits on $\Omega - I(a)$.

If $p+3+r \geq 2p$, and if G contains an element of order p which fixes less than $|I(a)|$ points, then the same argument as in (1.1) proves the assertion. If $p+3+r \leq 2p-1$, then every element in G of order p fixes $|I(a)|$ points because of $|\Omega - I(p)| \equiv 0 \pmod{p^2}$. Therefore,

$$\frac{|G|}{p} = \sum_{x \in G} \alpha_p(x) \geq \frac{|G|}{|C_G(a)|} \cdot \frac{1}{p} \cdot \sum_y{}' \alpha^*(y), \text{ and}$$

$$\sum_y{}'\alpha^*(y) = (t_a-1)\cdot|C_G(a)|\,,$$

where t_a denotes the number of orbits of $C_G(a)$ on $\Omega-I(a)$. Hence, $t_a=2$ (and all elements of order p in G are conjugate).

(1.2′) Let j be one of 0, 1, 2 and 3. If $p+3+r-j\geq 2p$, then $C_{G_{1,2,\cdots,j}}(a)$ is either transitive or has two orbits on $\Omega-I(a)$. If $2p-1\geq p+3+r-j\geq p+2$, then $C_{G_{1,2,\cdots,j}}(a)$ has two orbits on $\Omega-I(a)$.

Proof is similar as in (1.1′) (i.e., as in (1.1)).

(1.3′) Let $\Delta_1, \Delta_2, \cdots, \Delta_{k_1}$ and $\Gamma_1, \Gamma_2, \cdots, \Gamma_{k_2}$ be the partition of Ω into the orbits of $C_{G_{1,2,\cdots,p+3+r}}(a)$ on $\Omega-I(a)$, such that $\{\Delta_1, \Delta_2, \cdots, \Delta_{k_1}\}$ and $\{\Gamma_1, \Gamma_2, \cdots, \Gamma_{k_2}\}$ are fixes by $C_{G_{1,2,\cdots,j}}(a)$ with $p+3+r-j$ being the greatest integer not exceeding $2p-1$. Then $k_1\leq 2$ and $k_2\leq 2$.

Proof of (1.3′). Let $\Delta_1, \cdots, \Delta_k$ be the ste of orbits of $C_{G_{1,2,\cdots,p+3+r}}(a)$ on $\Omega-I(a)$. Then $C_{G_{1,\cdots,j}}(a)^{I(a)}$ $(j=0, 1, \cdots, p+3+r)$ acts on the set $\{\Delta_1, \cdots, \Delta_k\}$. First assume that $C_G(a)^{I(a)}$ and $C_{G_1}(a)^{I(a)}$ are both transitive on $\{\Delta_1, \cdots, \Delta_k\}$. Let Y be the stabilizer of Δ_1 in $C_G(a)$. Then $Y^{I(a)}$ is transitive. Moreover, Y satisfies the following condition: for any three points i_1, i_2, i_3 in $I(a)$, a Sylow p subgroup of $C_{G_{i_1,i_2,i_3}}{}^{I(a)}$ fixes just r points on $I(a)-\{i_1, i_2, i_3\}$ and semiregular on the remaining points. Using this fact, we get $Y^{I(a)}$ primitive. Because if $r=p-1$, then for $j=2$, $p+3+r-j\geq 2p$ and so $C_{G_{1,2}}(a)^{I(a)-\{1,2\}}$ is transitive on $\{\Delta_1, \cdots, \Delta_k\}$, hence $Y^{I(a)}$ is doubly transitive. If $r<p-1$, we easily get $Y^{I(a)}$ primitive, by noticing that the number of blocks is at most 2. Hence $Y^{I(a)}\geq A^{I(a)}$. Hence $k=2$. But this is a contradiction, because $|\Delta_1|$ is dividsible by p^2 as $|\Omega-I(P)|\equiv 0 \pmod{p^2}$ but $C_{G_{1,\cdots,p+3+r}}(a)$ is not divisible by p^2. Next assume that both $C_G{}^{I(a)}$ and $C_{G_1}(a)^{I(a)}$ have two orbits on $\{\Delta_1, \cdots, \Delta_k\}$ (say, $\{\Delta_1, \cdots, \Delta_{k_1}\}$ and $\{\Gamma_1, \cdots, \Gamma_{k_2}\}$, $k_1+k_2=k$). Let $Y(\Delta)$ be the stabilizer of Δ_1 in $C_G(a)$ and let $Y(\Gamma)$ be the stabilizer of Γ_1 in $C_G(a)$. Then the same argument as above shows that $Y(\Delta)^{I(a)}\geq A^{I(a)}$, and $Y(\Gamma)^{I(a)}\geq A^{I(a)}$. So, $k_1\leq 2$ and $k_2\leq 2$. Finally, if $C_G(a)^{I(a)}$ is transitive and $C_{G_1}(a)^{I(a)}$ has two orbits on $\{\Delta_1, \cdots, \Delta_k\}$ (say, $\{\Delta_1, \cdots, \Delta_{k_1}\}$ and $\{\Gamma_1, \cdots, \Gamma_{k_2}\}$), then $C_{G_{1,2}}(a)^{I(a)}$ has the same two orbits on $\{\Delta_1, \cdots, \Delta_k\}$. (Because this is true if $r\geq 1$, and if $r=0$ we get $Y^{I(a)}$ 3-transitive on $I(a)$ and $Y^{I(a)}\geq A^{I(a)}$ and we get a contradiction.) Now the same argument as before shows that $Y(\Delta)_1{}^{I(a)-\{1\}}\geq A^{I(a)-\{1\}}$ and $Y(\Gamma)_1{}^{I(a)-\{1\}}\geq A^{I(a)-\{1\}}$. So, we completed the proof of (1.3′).

(1.4′) $C_{G_{1,2,\cdots,p,\{p+1,p+2\},p+3,\cdots,p+3+r}}(a)$ has two orbits on $\Omega-I(a)$.

Proof is similar as in (1.4).

(1.5) Completion of the proof of Theorem A.

The method in this step is owing to Miyamoto [5, Lemma 1.5]. Let b be an element of order p in $C_G(a)$ such that

$$b = (1, 2, \cdots, p)(p+1)\cdots(p+3+r)(p+4+r)\cdots(2p+3+r)\cdots$$

and ab fixes the points $2p+4+r, \cdots, 3p+3+r$ (this is possible because of the assumption (2)). Now, let us set

$$K = G_{1,2,\cdots,p,\{p+1,p+2\},p+3,\cdots,p+3+4}, \quad \text{and}$$
$$L = \langle b\rangle\cdot K.$$

Then, $|C_L(a): C_K(a)|=p$, and since $C_L(a)$ and $C_K(a)$ has m orbits on $\Omega-I(a)$, where $m=1$ or 2 according as $|\Omega-I(P)|\not\equiv 0 \pmod{p^2}$ and $|\Omega-I(P)|\equiv 0 \pmod{p^2}$, we have $m\cdot\frac{p-1}{p}|C_L(a)|=\sum_{y\in C_L(a)-C_K(a)}\alpha^*(y)$. Let s be the number of orbits of length p of $\langle a, b\rangle$ on $\Omega-I(P)$. Then in our case, $s\geq 2$. The $s(p-1)$ elements a^ib^j (i are s of $0, 1, \cdots, p-1$ (which depend on j) such that $|I(a^ib^j)|=|I(a)|$ and $j=1, 2, \cdots, p-1$) are not conjugate to each other. Clearly, a^ib^j and $a^{i'}b^{j'}$ are not conjugate if $j\neq j'$. a^ib^j and $a^{i'}b^j$ are not conjugate if $i\neq i'$, because otherwise there exists an element of order p in $C_L(a)\cap N_L(\langle a, b\rangle)$ which does not centralize $\langle a, b\rangle$, and this contradicts the fact (assumption) that $\langle a, b\rangle$ is a Sylow p subgroup of $G_{1,2,3}$. Thus we have $s(p-1)$ conjugacy classes in $C_L(a)-C_K(a)$ represented by the elements a^ib^j (i are s of $0, 1, \cdots, p-1$ (which depend on j) such that $|I(a^ib^j)|=|I(a)|$ and $j=1, 2, \cdots, p-1$), and any of which has p fixed points on $\Omega-I(a)$. Since the restriction on any orbit of $\langle a, b\rangle$ of length p is self-centralizing, we have

$$\begin{aligned}\sum_{y\in C_L(a)-C_k(a)}\alpha^*(y) &\geq s(p-1)\cdot p\cdot |C_L(a): C_L(\langle a, b\rangle)|\cdot|\{y\in C_L(\langle a, b\rangle) \mid p\nmid o(y)\}| \\ &= s(p-1)\cdot p\cdot|C_L(a): C_L(\langle a, b\rangle)|\cdot|C_L(\langle a, b\rangle): \langle a, b\rangle| \\ &= \frac{s(p-1)}{p}\cdot|C_L(a)|.\end{aligned}$$

Therefore, $\frac{m\cdot(p-1)}{p}\cdot|C_L(a)|\geq\frac{s(p-1)}{p}\cdot|C_L(a)|$. But this is a contradiction, because $m=1$ and $s\geq 2$ if $|r-I(p)|\not\equiv 0 \pmod{p^2}$ and $m=2$ and $s=p\geq 3$ if $|r-I(p)|\equiv 0 \pmod{p^2}$.

Thus we have completed the proof of Theorem A.

2. Proof of Theorem 1 (i)

Let p be an odd prime, and let G be a $2p$-*ply* transitive permutation group which satisfies the assumptions of Theorem 1 (i). Let P be a Sylow p subgroup of $G_{1,2,\cdots,2p}$. If $P=1$, then we have already shown that G is one of $S_n(2p\leq n\leq 3p-1)$ and $A_n(2p+2\leq n\leq 3p-1)$. Suppose that $P\neq 1$ in the following. Then $|I(P)|=2p+r$ with $0\leq r\leqq p-1$.

We divide our proof into the following two cases:

Case 1 $|\Omega-I(P)|\equiv p \pmod{p^2}$

Case 2 $|\Omega-I(P)|\not\equiv p \pmod{p^2}$

First let us assume that Case 1 holds. Assume that $|\Omega|\geq 4p$. Then there exist two elements a and b of order p which commute to each other such that

$$a=(1)\cdots(2p)(2p+1)\cdots(2p+r)(2p+1+r,\ \cdots,\ 3p+r)(3p+r+1,\ \cdots,\ 4p+r)\cdots$$
$$b=(1\cdots p)(p+1,\ \cdots,\ 2p)(2p+1)\cdots(2p+r)(2p+1+r)\cdots(3p+r)\cdots(4p+r)\cdots .$$

Then $\langle a, b\rangle$ has $p+3$ orbits of length p because of the assumption that $|\Omega-I(P)|\equiv p \pmod{p^2}$. Since $\langle a, b\rangle$ fixes the set $\{p+1, \cdots, 2p, 2p+1+r, \cdots, 3p+r\}$ of $2p$ points as a whole, there exists an elemten c of order p such that $c\in C_G(\langle a, b\rangle)$ and c fixes the $2p$ points $p, p+1, \cdots, 2p-1, 2p+r+1, \cdots, 3p+r$ pointwisely. Since c must have a p cycle on the set $\{1, 2, \cdots, 2p+r\}$ of $2p+r$ points, and since $|\Omega-I(P)|\equiv p \pmod{p^2}$, the group $\langle a, c\rangle$ has at least $p+2$ orbits of length p. But this clearly contradicts the assumption of Theorem 1 (i). Thus $|\Omega|\leq 4p-1$, and G is one of S_n and A_n, with $n\leq 4p-1$.

Secondly, let us assume that Case 2 holds. Then the permutation group $G_{1,2,\cdots,p-3}$ on $\Omega-\{1, 2, \cdots, p-3\}$ satisfies the assumptions of Theorem A, and so we get a contradiction. Thus, the proof of Theorem 1 (i) is completed.

3. Proof of Theorem 1 (ii)

Let G satisfy the assumption of Theorem 1 (ii), and let P be a Sylow p subgroup of $G_{1,2\cdots,2p}$ which is cyclic. If $P=1$, then we have already shown that G is one of $S_n(2p\leq n\leq 3p-1)$ and $A_n(2p+2\leq n\leq 3p-1)$. Suppose that $P\neq 1$. Then $|I(P)|=2p+r$ with $0\leq r\leq p-1$, because $N_G(P)^{I(P)}$ is a $2p$-*ply* transitive group whose stabilizer of $2p$ points is of order prime to p. If P is semiregular on $\Omega-I(P)$, then G is one of S_n and A_n, with $3p\leq n\leqq 4p-1$. Henceforth, we assume that P is not semiregular on $\Omega-I(P)$, and we will derive a contradiction. We assume moreover that G is of the least possible degree among them. Clearly, $|P|\geq p^2$. Let a be an element of order p in P. Since P is cyclic and is not semiregular on $\Omega-I(P)$, $N_G(\langle a\rangle)^{I(a)}$ is $2p$-*ply* transitive group such that $N_G(\langle a\rangle)^{I(a)}_{1,2,\cdots,2p}$ has a cyclic Sylow p subgroup which is nontrivial. Therefore, $N_G(\langle a\rangle)^{I(a)}$ is one of S_n and A_n with $3p\leq n\leq 4p-1$ by the minimal nature of G. Thus, we may assume that P is generated by the element b of the form

$$b=(1)\cdots(2p+r)(2p+1+r,\ \cdots,\ 3p+r)(3p+1+r,\ \cdots,\ 4p+r,\ \cdots)\cdots .$$

Clearly $C_G(P)^{I(P)}\geq A^{I(P)}$ and each element of order p in $N_{G_{I(P)}}(P)$ centralizes P. Therefore, let c be an element of order p such that

$$c=(1, 2, \cdots, p)(p+1)\cdots(2p+r)\cdots$$

and that $|I(c)|=3p+r$. Then we may assume (by rechoosing P) without loss of generality that c normalizes P and therefore centralizes P. Since c fixes p or $2p$ points on $\Omega-\{1,2,\cdots,3p+r\}$ and since P is semiregular on the set of fixed points of c in $\Omega-\{1,2,\cdots,3p+r\}$, we have $|P|=p$. But this is a contradiction, and so the proof of Theorem 1 (ii) is completed.

THE OHIO STATE UNIVERSITY AND THE UNIVERSITY OF TOKYO

References

[1] E. Bannai: *On multiply transitive permutation groups* I, Osaka J. Math. **11** (1974), 401–411.

[2] E. Bannai: *On multiply transitive permutation groups* II, Osaka J. Math. **11** (1974), 413–416.

[3] M. Hall, Jr.: *On a theorem of Jordan*, Pacific. J. Math. **4** (1954), 219–226.

[4] D. Livingston and Wagner: *Transitivity of finite permutation groups on unordered set*, Math. Z. **90** (1965), 393–403.

[5] I. Miyamoto: *Multiply transitive permutation groups and odd primes*, Osaka J. Math. **11** (1974), 9–13.

[6] H. Nagao: *On multiply transitive groups* V, J. Algebra **9** (1968), 240–248.

[7] R. Noda and T. Oyama: *On multiply transitive groups* VI, J. Algebra **11** (1969), 145–154.

[8] H. Wielandt: Finite Permutation Groups, Academic Press, New York and London, 1964.