

Title	A note on transitive permutation groups of degree p
Author(s)	Ito, Noboru
Citation	Osaka Mathematical Journal. 14(2) P.213-P.218
Issue Date	1962
Text Version	publisher
URL	https://doi.org/10.18910/8403
DOI	10.18910/8403
rights	
Note	

Osaka University Knowledge Archive : OUKA

<https://ir.library.osaka-u.ac.jp/>

Osaka University

A NOTE ON TRANSITIVE PERMUTATION GROUPS OF DEGREE p

BY

NOBORU ITO

Dedicated to Kenjiro Shoda on his sixtieth birthday

Let p and q be odd prime numbers such that $p=2q+1$. Let Ω be the set of symbols $1, \dots, p$ and let \mathfrak{G} be an insoluble transitive permutation group on Ω . Then by a famous theorem of Burnside \mathfrak{G} is doubly transitive on Ω . In particular the order of \mathfrak{G} is divisible by q . Let \mathfrak{Q} and $Ns\mathfrak{Q}$ denote a Sylow q -subgroup of \mathfrak{G} and its normalizer in \mathfrak{G} . Moreover let \mathfrak{H} be the maximal subgroup of \mathfrak{G} consisting of all the permutations of \mathfrak{G} each of which fixes the symbol 1 and let $LF_2(n)$ denote the linear fractional group over the field of n elements.

Now the purpose of this note is (i) to give a proof for an unpublished result of Wielandt in 1955:

Theorem 1. *If \mathfrak{H} is imprimitive on $\Omega - \{1\}$, then \mathfrak{G} is isomorphic to $LF_2(7)$ with $p=7$,*

and (ii) to prove the following theorem:

Theorem 2. *If $Ns\mathfrak{Q}$ has order $2q$, then \mathfrak{G} is isomorphic to either $LF_2(7)$ with $q=3$ or $LF_2(11)$ with $q=5$.*

§ 1. Proof of Theorem 1.

1. Let \mathfrak{P} and $Ns\mathfrak{P}$ denote a Sylow p -subgroup of \mathfrak{G} and its normalizer in \mathfrak{G} . We assume that $Ns\mathfrak{P}$ has order px . If $x=1$, then by the splitting theorem of Burnside \mathfrak{G} contains a normal subgroup of index p . Hence \mathfrak{H} is normal in \mathfrak{G} . Since \mathfrak{G} is transitive on Ω , we have that $\mathfrak{H}=1$ and $\mathfrak{G}=\mathfrak{P}$. Then \mathfrak{G} is soluble against our assumption. If $x=2$, let J be an involution in $Ns\mathfrak{P}$. Then the cycle structure of J consists of q transpositions. Since q is odd, J is an odd permutation. Let \mathfrak{G}^* be the subgroup of \mathfrak{G} consisting of all the even permutations of \mathfrak{G} . Then the index of \mathfrak{G}^* in \mathfrak{G} equals two. Since \mathfrak{G} is insoluble, \mathfrak{G}^* is also

* Supported partially by N. S. F. contract G-9654.

insoluble. But we have that $Ns\mathfrak{P} \cap \mathfrak{G}^* = \mathfrak{P}$. This is a contradiction as before. If $x = 2q$, then by a theorem of Wielandt ([5], (27. 1)) \mathfrak{G} is triply transitive on Ω . Hence \mathfrak{H} is doubly transitive and necessarily primitive on $\Omega - \{1\}$. This is against our assumption. Hence we can assume that $x = q$.

2. \mathfrak{G} is simple. Otherwise let \mathfrak{N} be a proper normal subgroup ($\neq 1$) of \mathfrak{G} . Then since \mathfrak{G} is doubly transitive on Ω , \mathfrak{N} is transitive on Ω . Therefore \mathfrak{N} contains \mathfrak{P} . Using Sylow's theorem we have that $\mathfrak{G} = Ns\mathfrak{P}\mathfrak{N}$. Therefore we have that $\mathfrak{P} \subseteq Ns\mathfrak{P} \cap \mathfrak{N} \subseteq Ns\mathfrak{P}$. Since $Ns\mathfrak{P} : \mathfrak{P} = q$ is a prime number, we have that $Ns\mathfrak{P} \cap \mathfrak{N} = \mathfrak{P}$. This implies the solubility of \mathfrak{N} and \mathfrak{G} as before. This contradiction shows the simplicity of \mathfrak{G} .

3. The order of \mathfrak{Q} is q and the cycle structure of every element ($\neq 1$) of \mathfrak{Q} consists of two q -cycles. Otherwise \mathfrak{Q} contains a q -cycle. Then by a classical theorem of Jordan \mathfrak{G} must be the alternating group of degree p , which is obviously triply transitive on Ω . This is a contradiction as before.

4. Let \mathfrak{R} be the subgroup of \mathfrak{G} consisting of all the permutations of \mathfrak{G} each of which fixes each of the symbols 1 and 2. Now since \mathfrak{H} is imprimitive on $\Omega - \{1\}$, \mathfrak{R} is not a maximal subgroup of \mathfrak{H} . Let \mathfrak{M} be a maximal subgroup of \mathfrak{H} containing \mathfrak{R} . Since $\mathfrak{H} : \mathfrak{R} = 2q$ two cases arise: (i) $\mathfrak{M} : \mathfrak{R} = q$ and $\mathfrak{H} : \mathfrak{M} = 2$ and (ii) $\mathfrak{M} : \mathfrak{R} = 2$ and $\mathfrak{H} : \mathfrak{M} = q$.

5. Case (i). Since \mathfrak{M} has index two in \mathfrak{H} and is intransitive on $\Omega - \{1\}$ $\Omega - \{1\}$ is divided into two domains of transitivity Ω_1 and Ω_2 of \mathfrak{M} each of which has length q . Let $Cs\mathfrak{Q}$ denote the centralizer of \mathfrak{Q} in \mathfrak{G} . Then we have that $Cs\mathfrak{Q} = \mathfrak{Q}$, because otherwise $Cs\mathfrak{Q}$ must contain a $2q$ -cycle, which is an odd permutation against the simplicity of \mathfrak{G} . Now using Sylow's theorem we can assume that \mathfrak{Q} is contained in \mathfrak{H} . Then \mathfrak{Q} is contained in \mathfrak{M} and we have that $\mathfrak{H} = Ns\mathfrak{Q}\mathfrak{M}$, whence follows that $Ns\mathfrak{Q} : \mathfrak{M} \cap Ns\mathfrak{Q} = 2$. Let \mathfrak{X} be a Sylow 2-subgroup of $Ns\mathfrak{Q}$. Then \mathfrak{X} is cyclic, because of $Cs\mathfrak{Q} = \mathfrak{Q}$. Anyway we have that $\mathfrak{X} \neq 1$. Let T be a generator of \mathfrak{X} . Then since \mathfrak{X} is not contained in \mathfrak{M} , T must permute Ω_1 with Ω_2 . Hence we have that $\alpha(T) = 1$, where $\alpha(X)$ denotes the number of symbols of Ω which are fixed by a permutation X of \mathfrak{G} . If T is an involution, then the cycle structure of T consists of q transpositions and T must be an odd permutation, contradicting the simplicity of \mathfrak{G} . Hence the order of T , say 2^r , is greater than two. Now we have that $\alpha(T^t) \leq 3$ for $T^t \neq 1$ (t is an integer.), because otherwise T^t fixes at least two symbols of either Ω_1 or Ω_2 . This means that T^t is commutative with the elements of \mathfrak{Q} , which is a contradiction since $Cs\mathfrak{Q} = \mathfrak{Q}$. Since $2q \not\equiv 0 \pmod{4}$ the cycle structure of T must contain a transposition. Hence if t is even and $T^t \neq 1$ we have that $\alpha(T^t) = 3$.

Therefore the cycle structure of T consists of one transposition and $(2q-2/2^r)2^r$ -cycles. Since T must be an even permutation, we have that $2q-2/2^r$ is odd. Anyway we obtain the following equality:

$$(I) \quad 2q = 2 + 2^r(2q - 2/2^r),$$

where $(2q-2/2^r)$ is an odd number. On the other hand, T is contained in $Ns\Omega$ and $Cs\Omega = \Omega$. Therefore we obtain the following congruence:

$$(II) \quad q \equiv 1 \pmod{2^r}.$$

(I) and (II) give us a contradiction. Hence the case (i) cannot occur.

6. Case (ii). Since $\mathfrak{M}:\mathfrak{R}=2$, the length of the domain Γ of transitivity of \mathfrak{M} containing the symbol 2 of Ω must be two. Let us assume that Γ consists of two symbols 2 and 3 of Ω . Then since \mathfrak{R} is normal in \mathfrak{M} , \mathfrak{R} must fix also the symbol 3. Now let Φ denote the set of symbols of Ω which are fixed by \mathfrak{R} . Then the length f of Φ is at least three. By a theorem of Witt ([5], (9. 4)) the normalizer $Ns\mathfrak{R}$ of \mathfrak{R} in \mathfrak{G} is doubly transitive on Φ . In our case then $Ns\mathfrak{R}$ clearly has order $f(f-1)$. Since $f(f-1)$ must divide $2pq$ and f is smaller than p , we must have that $f=q$ and $f-1=2$. Thus we obtain that $q=3$ and $p=7$. Now it is easy to show that \mathfrak{G} is isomorphic to $LF_2(7)$.

§ 2. Proof of Theorem 2.

If $Ns\Omega$ is cyclic, then \mathfrak{G} contains by the splitting theorem of Burnside a normal subgroup \mathfrak{N} of index q . Since $Ns\mathfrak{N} \cap \mathfrak{N}$ has order at most $2p$, \mathfrak{N} and \mathfrak{G} must be soluble as before in § 1.1 against our assumption. Hence $Ns\Omega$ must be a dihedral group of order $2q$. Therefore Theorem 2 is a special case of the following

Theorem 3. *Let n be an integer such that $n=2q+1$, where q is an odd prime number. Let Ω be the set of symbols $1, \dots, n$ and let \mathfrak{G} be an insoluble doubly transitive permutation group on Ω . Let Ω be a Sylow q -subgroup of \mathfrak{G} and $Ns\Omega$ be the normalizer of Ω in \mathfrak{G} . If $Ns\Omega$ is a dihedral group of order $2q$, then \mathfrak{G} is isomorphic to either $LF_2(7)$ with $q=3$ or $LF_2(11)$ with $q=5$.*

Proof of Theorem 3.

1. \mathfrak{G} is simple. Otherwise let \mathfrak{N} be a maximal normal subgroup ($\neq 1$) of \mathfrak{G} . If \mathfrak{N} contains Ω , then we have that $\mathfrak{N} \cap Ns\Omega = \Omega$, since $Ns\Omega:\Omega=2$ and by Sylow's theorem $(Ns\Omega)\mathfrak{N} = \mathfrak{G}$. Hence by the splitting theorem of Burnside \mathfrak{N} contains a normal subgroup \mathfrak{N}^* of index q . Since $Ns\Omega$ is a dihedral group of order $2q$, every element ($\neq 1$) of \mathfrak{N}^*

is not commutative with any element ($\neq 1$) of Ω . Therefore \mathfrak{N}^* is nilpotent by a theorem of Thompson [4]. Then \mathfrak{N} and \mathfrak{G} become soluble against our assumption. If the order of \mathfrak{N} is prime to q , then let us consider the subgroup $\mathfrak{N}\Omega$. Again by a theorem of Thompson \mathfrak{N} becomes nilpotent. Let \mathfrak{N}^* be a minimal normal subgroup of \mathfrak{G} contained in \mathfrak{N} . Since \mathfrak{G} is doubly transitive on Ω , every normal subgroup ($\neq 1$) of \mathfrak{G} is transitive on Ω . Therefore \mathfrak{N}^* must be an elementary abelian p -group for some prime number p and we have the following factorisation of $\mathfrak{G} : \mathfrak{G} = \mathfrak{N}^* \mathfrak{H}$, $\mathfrak{N}^* \cap \mathfrak{H} = 1$, where \mathfrak{H} denotes the maximal subgroup of \mathfrak{G} consisting of all the permutations of \mathfrak{G} each of which fixes the symbol 1. Since \mathfrak{N} is nilpotent, \mathfrak{N}^* is contained in the center of \mathfrak{N} . Since \mathfrak{H} does not contain any normal subgroup ($\neq 1$) of \mathfrak{G} , we have that $\mathfrak{N} \cap \mathfrak{H} = 1$ and $\mathfrak{N} = \mathfrak{N}^*$. On the other hand, since \mathfrak{G} is insoluble, \mathfrak{H} must be insoluble. Moreover since \mathfrak{N} is also a maximal normal subgroup of \mathfrak{G} , \mathfrak{H} is simple. Let p^ν be the order of \mathfrak{N} . Then we have the equality

$$n = 2q + 1 = p^\nu.$$

Since \mathfrak{H} is insoluble, we have that ν is greater than one. Hence we have that $p=3$ and $q=\frac{1}{2}(3^\nu-1)$. In particular we have that ν is greater than two. Then \mathfrak{H} is isomorphic to a subgroup of the ν -dimensional special linear group $SL_\nu(3)$ over the field of three elements. But then $Ns\Omega$ has order $\nu q > 2q$ [3]. This is a contradiction. Hence \mathfrak{G} must be simple.

2. In the first place let us assume that \mathfrak{H} is imprimitive on $\Omega - \{1\}$. Let \mathfrak{K} be the subgroup of \mathfrak{G} consisting of all the permutations each of which fixes each of the symbols 1 and 2 of Ω . Then \mathfrak{K} is not a maximal subgroup of \mathfrak{H} . Let \mathfrak{M} be a maximal subgroup of \mathfrak{H} containing \mathfrak{K} . Since $\mathfrak{H} : \mathfrak{K} = 2q$, we have two cases: (i) $\mathfrak{H} : \mathfrak{M} = 2$, $\mathfrak{M} : \mathfrak{K} = q$ and (ii) $\mathfrak{H} : \mathfrak{M} = q$, $\mathfrak{M} : \mathfrak{K} = 2$.

3. Case (i). Using Sylow's theorem we can assume that Ω is contained in \mathfrak{H} . Then Ω is contained in \mathfrak{M} . Hence by Sylow's theorem we have that $(Ns\Omega)\mathfrak{M} = \mathfrak{H}$. Since $Ns\Omega : \Omega = 2$, we have then that $Ns\Omega \cap \mathfrak{M} = \Omega$. By the splitting theorem of Burnside \mathfrak{M} contains a normal subgroup of index q , which necessarily coincides with \mathfrak{K} . Since \mathfrak{H} is transitive on $\Omega - \{1\}$, we have that $\mathfrak{K} = 1$. Then it is easy to show the solubility of \mathfrak{G} against our assumption. Thus Case (i) cannot occur.

4. Case (ii). If \mathfrak{H} is simple, then by a previous result ([2], Theorem II) \mathfrak{H} becomes primitive on $\Omega - \{1\}$. Hence in our case \mathfrak{H} cannot be simple. Let \mathfrak{N} be a maximal normal subgroup of \mathfrak{H} . If the order of \mathfrak{N} is divisible by q , then \mathfrak{N} has index two in $\mathfrak{H}\mathfrak{N} \cap Ns\Omega = \Omega$, because $Ns\Omega$ is a dihedral group of order $2q$ and we have that $\mathfrak{H} = \mathfrak{N}Ns\Omega$ by Sylow's theorem. Now by the splitting theorem of Burnside \mathfrak{N} contains a normal

subgroup \mathfrak{N}^* of index q . Since \mathfrak{G} is transitive on $\Omega - \{1\}$ \mathfrak{N}^* is semi-transitive on $\Omega - \{1\}$ ([5], 11). Hence the length of domains of transitivity of \mathfrak{N}^* from $\Omega - \{1\}$ equals two and \mathfrak{N}^* is an elementary abelian 2-subgroup. Let us consider the subgroup $\mathfrak{N}\mathfrak{N}^*$. Since $Ns\mathfrak{N}$ is a dihedral group of order $2q$, every element ($\neq 1$) of \mathfrak{N}^* is not commutative with any element ($\neq 1$) of \mathfrak{N} . Hence we see in particular that the order of \mathfrak{N}^* is congruent to 1 modulo q .

Since \mathfrak{G} is simple and $Ns\mathfrak{N}$ is a dihedral group of order $2q$, we see, using a method of Brauer-Fowler ([2], § 1.3), that there is only class of conjugate involutions in \mathfrak{G} . Now let us consider the subgroup $Ns\mathfrak{N}$. Every element of $Ns\mathfrak{N}$ of order q has a cycle structure consisting of two q -cycles. Then it is easy to show that every involution in $Ns\mathfrak{N}$ fixes just three symbols of Ω .

Since $\mathfrak{M}:\mathfrak{R}=2$, the length of the domain Γ of transitivity of \mathfrak{M} containing the symbol 2 of Ω must be two. Let us assume that Γ consists of two symbols 2 and 3 of Ω . Then since \mathfrak{R} is normal in \mathfrak{M} , \mathfrak{R} must fix also the symbol 3. Let \mathfrak{X} be a Sylow 2-subgroup of \mathfrak{R} . Then \mathfrak{X} must be semi-regular on $\Omega - \{1, 2, 3\}$ ([5], § 4). Therefore the order of \mathfrak{X} is a divisor of $2q-2$. Since the orders of \mathfrak{X} and \mathfrak{N}^* are same, we see that the order of \mathfrak{X} equals $q+1$ and that $2q-2=q+1$. Thus we obtain that $q=3$. Now it is easy to show that \mathfrak{G} is isomorphic to $LF_2(7)$.

If the order of \mathfrak{N} is prime to q , then as before (see No. 1 of this proof) by a theorem of Thompson [4] \mathfrak{N} itself becomes a nilpotent, therefore, an elementary abelian 2-group and the order of \mathfrak{N} is congruent to 1 modulo q . If \mathfrak{N} has index q in \mathfrak{G} , then we must have that $Ns\mathfrak{N}=\mathfrak{N}$ against our assumption. Since the factor group $\mathfrak{G}/\mathfrak{N}$ is simple, the order of $\mathfrak{G}/\mathfrak{N}$ is divisible by 4. Hence the order of \mathfrak{N} is at most a half of that of \mathfrak{X} . Thus we obtain an absurd inequality $q-1 \geq q+1$.

5. So we can assume that \mathfrak{G} is primitive on $\Omega - \{1\}$. Then \mathfrak{G} is simple. Otherwise let \mathfrak{N} be a proper normal subgroup ($\neq 1$) of \mathfrak{G} . Since \mathfrak{G} is primitive on $\Omega - \{1\}$, \mathfrak{N} is transitive on $\Omega - \{1\}$. Hence the order of \mathfrak{N} is divisible by $2q$. Since $Ns\mathfrak{N}$ is a dihedral group of order $2q$ and $\mathfrak{G}=\mathfrak{N}Ns\mathfrak{N}$ by Sylow's theorem, we must have that $\mathfrak{G}:\mathfrak{N}=2$ and $\mathfrak{N} \cap Ns\mathfrak{N}=\mathfrak{N}$. Then by the splitting theorem of Burnside \mathfrak{N} contains a characteristic subgroup \mathfrak{N}^* of index q . If $\mathfrak{N}^* \neq 1$, then the order of \mathfrak{N}^* is divisible by $2q$. Therefore we obtain that $\mathfrak{N}^*=1$, which implies the solubility of \mathfrak{G} against our assumption.

6. If \mathfrak{G} is doubly transitive on $\Omega - \{1\}$, then by a previous result ([2], Theorem I), \mathfrak{G} is isomorphic to $LF_2(r)$ with $2q=r+1$, and hence only the identity element of \mathfrak{G} fixes at least three symbols of $\Omega - \{1\}$. Therefore \mathfrak{G} is triply transitive on Ω and only the identity element fixes

at least four elements of Ω . Now using a theorem of Gorenstein-Hughes [1] we obtain that $2q+1=2^v+1$. This is a contradiction, since q is an odd prime number.

7. If \mathfrak{G} is not doubly transitive on $\Omega - \{1\}$, then also by a previous result ([2], Theorem II) \mathfrak{G} is isomorphic to the icosahedral group with $q=5$. Thus we have obtained that $n=11$ and the order of \mathfrak{G} is 660. Now it is easy to show that \mathfrak{G} is isomorphic to $LF_2(11)$.

UNIVERSITY OF ILLINOIS AND NAGOYA UNIVERSITY

(Received April 6, 1962)

Bibliography

- [1] D. Gorenstein and D. R. Hughes: *Tripily transitive groups in which only the identity fixes four letters*, Illinois J. Math. **5** (1961), 486-491.
- [2] N. Ito: *On transitive simple permutation groups of degree $2p$* , Math. Z. **78** (1962), 453-468.
- [3] N. Ito: *A note on $SL_r(q)$* , to appear in Arch. d. Math.
- [4] J. Thompson: *Finite groups with fixed-point-free automorphisms of prime order*, Proc. Nat. Acad. Sci. U.S.A. **45** (1959), 578-581.
- [5] H. Wielandt: *Permutationsgruppen*, Vorlesungsausarbeitungen von J. André, Tübingen, 1955.