N. Ito
Nagoya Math. J.
Vol. 37 (1970), 201–208

ON PERMUTATION GROUPS OF PRIME DEGREE p WHICH CONTAIN AT LEAST TWO CLASSES OF CONJUGATE SUBGROUPS OF INDEX p. II[1)]

NOBORU ITO[2)]

To Professor Katuzi Ono on his 60th birthday

Let p be a prime and let Ω be the set of p symbols $1, 2, \cdots, p$, called points. Let $\mathfrak{G}$ be a transitive permutation group on Ω such that

(I) $\mathfrak{G}$ contains a subgroup $\mathfrak{B}$ of index p which is not the stabilizer of a point.

$\mathfrak{B}$ has two point orbits, say D and $\Omega - D$ (cf. [3]). Let k be the number of points in D. Then $1 < k < p - 1$. Replacing D by $\Omega - D$, if need be, we can assume that $k \leqq \frac{1}{2}(p-1)$.

Now the only known transitive permutation groups of degree p satisfying the condition (I) are the following groups:

(i) Let $F(q)$ be the field of q elements. Let $V(r, q)$ $LF(r, q)$ and $SF(r, q)$ be the r-dimensional vector space, the r-dimensional projective special linear group and r-dimensional semilinear group over $F(q)$ respectively, where $r \geqq 3$ and $p = (q^r - 1)/(q-1)$. Let Π be the set of one-dimensional subspaces of $V(r, q)$. $SF(r, q)$ can be considered as a permutation group on Π. Identify Π with Ω. Then any subgroup $\mathfrak{G}$ of $SF(r, q)$ containing $LF(r, q)$ satisfies (I) with $k = (q^{r-1} - 1)/(q-1)$.

(ii) $\mathfrak{G} = LF(2, 11)$, where $p = 11$ and $k = 5$.

Now among the groups mentioned above only $LF(2, 11)$ satisfies the following condition:

Received Jan. 22, 1969

1) This paper is a continuation of ([7]) with the same title.

2) This research was partially supported by NSF Grant GP-6539.

(II) the restriction of $\mathfrak{B}$ to D is faithful.

In [6] we have proved that if the restriction of $\mathfrak{B}$ to D is not faithful, then $\mathfrak{G}$ is isomorphic to one of the groups mentioned in (i). In [7] we have proved that if $\mathfrak{G}$ satisfies (I) and (II), and if k is a prime, then $\mathfrak{G}$ is isomorphic to $LF(2,11)$.

In this note we prove the following

THEOREM: *Let* $\mathfrak{G}$ *be a group satisfying* (I) *and* (II). *Then* $k-1$ *is not a prime.*

Proof. (a) Let $\mathfrak{N}$ be a minimal normal subgroup of $\mathfrak{G}$. Since $\mathfrak{G}$ is 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. Since $\mathfrak{G}=\mathfrak{N}\mathfrak{B}$, $\mathfrak{N}: \mathfrak{N}\cap\mathfrak{B} = \mathfrak{G}: \mathfrak{B}=p$. Then since $\mathfrak{N}\cap\mathfrak{B}$ has two point orbits (cf. [3]), D and $\Omega-D$ are the point orbits of $\mathfrak{N}\cap\mathfrak{B}$. Therefore in order to prove the theorem we can assume the simplicity of $\mathfrak{G}$. So from now on let $\mathfrak{G}$ be simple.

(b) Let $Ns\mathfrak{P}$ denote the normalizer of $\mathfrak{P}$ in $\mathfrak{G}$. Since $\mathfrak{P}$ coincides with its own centralizer in $\mathfrak{G}$, $Ns\mathfrak{P}/\mathfrak{P}$ is a cyclic group of order dividing $p-1$. If $Ns\mathfrak{P}=\mathfrak{P}$, then by a transfer theorem of Burnside $\mathfrak{G}$ contains a normal Sylow p-complement. Since $\mathfrak{G}$ is simple, this implies that $\mathfrak{G}=\mathfrak{P}$, contradicting (I). Let pq be the order of $Ns\mathfrak{P}$. If $q=p-1$, then $Ns\mathfrak{P}$ contains an odd permutation contradicting the simplicity of $\mathfrak{G}$. Therefore $1<q<p-1$. Now the following results of Brauer concerning groups which contain self-centralizing subgroups of prime order can be applied for $\mathfrak{G}$ with p ([1]):

The degree of an irreducible character X of $\mathfrak{G}$ is congruent to either 1, 0, -1 or $-\delta_p q$ modulo p, where δ_p is equal to ± 1. We say that X has p-type A, D, B, or C, according as the degree of X is congruent to 1, 0, -1, or $-\delta_{pq}$ modulo p 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 $(p-1)/q$. Let P be an element of order p of $\mathfrak{G}$. Then we have that $X(P)=1$, 0, -1, according as X has p-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 the values at P over all characters of p-type C equals δ_p.

(c) Without loss of generality, we may assume that D consists of the points $1, 2, \cdots, k$. Let G be an element of $\mathfrak{G}$. Then $G(D) = D$ if and only if G belongs to $\mathfrak{B}$. Since $\mathfrak{G}: \mathfrak{B} = p$, there exist exactly p distinct $G(D)'s$, which will be denoted by $D_1 = D, D_2, \cdots, D_p$. $D_i's$ are called blocks. Now let $\mathfrak{A}$ be the stabilizer of the point 1 in $\mathfrak{G}$ and A an element of $\mathfrak{A}$. Then $A(D) = D$ if and only if A belongs to $\mathfrak{A} \cap \mathfrak{B}$. Since D is an orbit of $\mathfrak{B}, \mathfrak{A} \cap \mathfrak{B}$ has index k in $\mathfrak{B}$ and hence in $\mathfrak{A}$. So there exist exactly k distinct $A(D)$'s, say $D_1, D_2, \cdots, D_k$. Every $D_i (i = 1, 2, \cdots, k)$ contains the point 1. By a theorem of Burnside we get from (I) that $\mathfrak{G}$ is nonsolvable and doubly transitive. So $\mathfrak{A}$ is transitive on $\Omega - \{1\}$. Hence every point $j \neq 1$ of Ω appears in the same number, say λ, of $D_i's (i = 1, 2, \cdots, k)$. Thus we get the following equality:

$$k^2 - k = \lambda(p-1). \tag{1}$$

Since $k \leqq \frac{1}{2}(p-1), \quad \lambda \leqq \frac{1}{2}(k-1)$.

Now assume that $k - 1 = l$ is a prime. Then by (1) l divides $p - 1$. Since $\mathfrak{G}$ is doubly transitive, the order of $\mathfrak{G}$ is divisible by $p-1$, and hence by l. Let $\mathfrak{L}$ be a Sylow l-subgroup of $\mathfrak{G}$ contained in $\mathfrak{A} \cap \mathfrak{B}$. Since $\mathfrak{B}$ is faithful on D by (II), the order of $\mathfrak{L}$ is equal to l and $\mathfrak{L}$ coincides with its own centralizer in $\mathfrak{G}$. Therefore the results of Brauer mentioned in (b) are applicable to $\mathfrak{G}$ with l in place of p.

(d) Let $\mathbf{1}_{\mathfrak{A} \cap \mathfrak{B}}$ be the principal character of $\mathfrak{A} \cap \mathfrak{B}$ and $\mathbf{1}^*_{\mathfrak{A} \cap \mathfrak{B}}$ the character of $\mathfrak{G}$ induced by $\mathbf{1}_{\mathfrak{A} \cap \mathfrak{B}}$. Let X_0 be the irreducible character of $\mathfrak{G}$ given by $X_0(G) = \alpha(G) - 1$, where G is an element of $\mathfrak{G}$ and $\alpha(G)$ denotes the number of points left fixed by G. By the reciprocity theorem of Frobenius we see that the multiplicity of X_0 in $\mathbf{1}^*_{\mathfrak{A} \cap \mathfrak{B}}$ is equal to the number of points orbits of $\mathfrak{A} \cap \mathfrak{B}$ less 1. Now by (c) $\mathfrak{B}$ is doubly transitive on D, and hence $\mathfrak{A} \cap \mathfrak{B}$ is transitive on $D - \{1\}$. Let $\mathfrak{A}_{k+1}$ be the stabilizer of the point $k+1$ in $\mathfrak{G}$. Then since $\Omega - D$ is an orbit of $\mathfrak{B}$, $\mathfrak{B} \cap \mathfrak{A}_{k+1}$ has index $p-k$ in $\mathfrak{B}$. Since k and $p-k$ are relatively prime, $\mathfrak{A} \cap \mathfrak{B} \cap \mathfrak{A}_{k+1}$ also has index $p-k$ in $\mathfrak{A} \cap \mathfrak{B}$. So $\mathfrak{A} \cap \mathfrak{B}$ is transitive on $\Omega - D$. Therefore X_0 appears in $\mathbf{1}^*_{\mathfrak{A} \cap \mathfrak{B}}$ with the multiplicity 2. Put

$$\mathbf{1}^*_{\mathfrak{A} \cap \mathfrak{B}} = \mathbf{1}_{\mathfrak{G}} + 2X_0 + Y, \tag{2}$$

where $\mathbf{1}_{\mathfrak{G}}$ denotes the principal character of $\mathfrak{G}$ and $\boldsymbol{Y}$ is a (in general, reducible) character of degree $(k-2)p+1$. Since $\mathbf{1}^{*}_{\mathfrak{A}\cap\mathfrak{B}}(P)=0$, $\mathbf{1}_{\mathfrak{G}}(P)=1$ and $\boldsymbol{X}_0(P)=-1$, $\boldsymbol{Y}(P)=1$. Therefore by the results of Brauer mentioned in (b) either a character $\boldsymbol{X}$ of p-type A or a character $\boldsymbol{X}$ of p-type C with $\boldsymbol{X}(E)\equiv -q \pmod p$ appears as an irreducible component of $\boldsymbol{Y}$, where E denotes the identity element of $\mathfrak{G}$.

First assume that a character $\boldsymbol{X}=\boldsymbol{A}_2$ of p-type A appears as an irreducible component of $\boldsymbol{Y}$. Put $\boldsymbol{A}_2(E)=ap+1$. Since $\mathfrak{G}$ is simple, $a\neq 0$.

If $\boldsymbol{A}_2$ has 1-type A, then $ap+1\equiv 1 \pmod l$, $a\equiv 0 \pmod l$ and $ap+1 \geqq lp+1=(k-1)p+1$. This is a contradiction, since $\boldsymbol{Y}(E)=(k-2)p+1$ and $\boldsymbol{A}_2(E)\leqq \boldsymbol{Y}(E)$.

If $\boldsymbol{A}_2$ has l-type D, then $ap+1\equiv 0 \pmod l$. Since $p\equiv 1 \pmod l$, $a\equiv -1 \pmod l$. This implies that $\boldsymbol{Y}=\boldsymbol{A}_2$.

If $\boldsymbol{A}_2$ has l-type B, then $ap+1\equiv -1 \pmod l$, $a\equiv -2 \pmod l$ and $a=l-2$. Then using the results of Brauer mentioned in (b) we see that the decomposition of $\boldsymbol{Y}$ into irreducible components has the following form: $\boldsymbol{Y}=\boldsymbol{A}_2+\boldsymbol{D}$, where $\boldsymbol{D}$ is an irreducible character of degree p of $\mathfrak{G}$.

(e) Let $\mathfrak{M}$ be a Sylow l-complement of the normalizer of $\mathfrak{L}$ in $\mathfrak{G}$. Then $\mathfrak{M}$ is cyclic of order, say m, dividing $l-1$. Let M be a generator of $\mathfrak{M}$. M restricted to D leaves the point 1 and another point, say 2 fixed, and consists of $(l-1)/m$ m-cycles. Let L be a generator of $\mathfrak{L}$. Then by the results of Brauer mentioned in (b) we get that $\boldsymbol{X}_0(L)=0$, and hence that $\alpha(L)=1$.

Let b be the permutation representation of $\mathfrak{G}$ on the set W of blocks $D_1, D_2, \cdots, D_p$. L leaves the point 1 fixed, and hence $b(L)$ leaves the set $\varDelta$ of blocks $D_1, D_2, \cdots, D_k$ containing the point 1 fixed. Since $\alpha(L)=1$, D_1 is the only block of W left fixed by $b(L)$ (cf. [2], p. 22). Therefore $b(L)$ restricted to $\varDelta$ leaves the block D_1 fixed, and consists of one l-cycle. Hence $b(M)$ restricted to $\varDelta$ leaves the block D_1 and another block, say D_2 fixed and consists of $(l-1)/m$ m-cycles. By (c) there exist exactly λ blocks of $\varDelta$ which contain the point 2. The set of these λ blocks are left fixed by $b(M)$. Thus

$$\lambda\equiv 1 \pmod m \quad \text{or} \quad \lambda\equiv 2 \pmod m, \tag{3}$$

according as D_2 contains the point 2 or not. If $\lambda=1$, then by a theorem of Ostrom-Wagner ([2], p. 214) $\mathfrak{G}$ does not satisfy the condition (II). Thus λ is bigger than 1. Then by (3) we get that either $\lambda = 2$ or

$$\begin{aligned}(4)\qquad ((l-1)/m)+2 &\geqq ((l-1)/(\lambda-1))+2 \\ &= (1+2\lambda-3)/(\lambda-1) \\ &\geqq (l+1)/(\lambda-1).\end{aligned}$$

(f) Assume that λ is bigger than 2. If A_2 has l-type C, then by the results of Brauer mentioned in (b) there exist $(l-1)/m$ characters of $\mathfrak{G}$ algebraically conjugate to A_2. Here if q is relatively prime to l, then q divides $(p-1)/l = (l+1)/\lambda$. By the results of Brauer mentioned in (b) there exist exactly q characters of p-types A or B of $\mathfrak{G}$. But we have already $((l-1)/m)+2$ characters of p-types A or B of $\mathfrak{G}$, namely $\mathbf{1}_{\mathfrak{G}}$, $\boldsymbol{X}_0$ and the algebraically conjugate family of A_2. By (4) this is a contradiction. Thus l divides q. Then since there exists an element of order q in $\mathfrak{G}$ and since $\mathfrak{L}$ coincides with its own centralizer in $\mathfrak{G}$, we obtain that $q = l$.

(g) We claim that if either $\lambda = 2$ or $q = l$, then $\mathfrak{B}$ restricted to D is triply transitive.

If $\mathfrak{B}$ restricted to D is not triply transitive, $\mathfrak{A}\cap\mathfrak{B}$ restricted to $D-\{1\}$ is not doubly transitive. If $m = 1$, then by a transfer theorem of Burnside $\mathfrak{G}$ contains a normal Sylow l-complement, contradicting the simplicity of $\mathfrak{G}$. So m is bigger than 1, and by a theorem of Burnside $\mathfrak{A}\cap\mathfrak{B}$ restricted to $D-\{1\}$ is a Frobenius group of order lm. Since $k = l+1$ is even, by a previous result ([4]) we get that $m = \frac{1}{2}(k-2)$. Hence the order g of $\mathfrak{G}$ is equal to $\frac{1}{2}pk(k-1)(k-2)$. Sylow's theorem gives $g = pq(1+xp)$, where x is a positive integer, and so we get that

$$(5)\qquad \frac{1}{2}k(k-1)(k-2) = q(1+xp).$$

First assume that $\lambda = 2$. Then from (5) it follows that

$$(p-1)(k-2) = q(1+xp).$$

Hence $2 \equiv q+k \pmod{p}$. Since $k \leqq \frac{1}{2}(p-1)$ and $q \leqq \frac{1}{2}(p-1)$, this is a contradiction.

Next assume that $q = l$. Then from (5) it follows that

(6) $$\frac{1}{2}k(k-2) = 1 + xp.$$

Hence $2x + 3 \equiv 0 \pmod{l}$. Put $2x = yl - 3$. Then y is a positive integer. From (6) it follows that $(yl-3)p = l^2 - 3$. Since $p \geqq 2k + 1 = 2l + 3$, this is a contradiction.

(h) Assume that $\mathfrak{B}$ restricted to D is triply transitive. Then $\mathfrak{A} \cap \mathfrak{B}$ is doubly transitive on $D - \{1\}$. Put $d_i = (D - \{1\}) \cap D_i$ for $i = 2, 3, \cdots, k$. Then by (c) every d_i contains exactly $\lambda - 1$ points, and also by (c) there exist $\lambda - 1$ of d_i's, say $d_2, d_3, \cdots, d_\lambda$ which contain the point 2. Let $\mathfrak{A}_2$ be the stabilizer of the point 2 in $\mathfrak{G}$. Since $\mathfrak{A} \cap \mathfrak{A}_2 \cap \mathfrak{B}$ is transitive on $D - \{1, 2\}$, every point $\neq 1, 2$ of D appears in the same number, say μ, of d_i's$(i = 2, 3, \cdots, \lambda)$. Thus we obtain that

(7) $$(\lambda - 1)^2 = (\lambda - 1) + \mu(k-2).$$

Put $p - 1 = nl$. Then by (1) $k = n\lambda$. Hence from (7) it follows that $2\mu + 2 = 0 \pmod{\lambda}$. Put $2\mu + 2 = \nu\lambda$. Then ν is a positive integer. Then again from (7) it follows that

$$(2\lambda - 2)(\lambda - 2) = (\nu\lambda - 2)(n\lambda - 2).$$

Since n is even, this implies that $\nu = 1$ and $n = 2$. Thus $p = 2l + 1$. By a previous result ([5]) $\mathfrak{G}$ is triply transitive on Ω, which is a contradiction ([3]). Therefore $\mathfrak{B}$ restricted to D cannot be triply transitive. In particular by (f) $\boldsymbol{A}_2$ cannot be of l-type C.

(i) By (g) we have that $g = \frac{1}{2}pk(k-1)(k-2)$. If $\boldsymbol{A}_2$ is of l-type B, then by (d) $\boldsymbol{A}_2(E) = (k-3)p + 1$. Since $\boldsymbol{A}_2(E)$ divides g, we obtain that $\frac{1}{2}k(k-2) \equiv 0 \pmod{(k-3)p+1}$. Since $p \geqq 2k + 1$, this is impossible.

(j) If $\boldsymbol{A}_2$ is of l-type D, then by (d) $\boldsymbol{A}_2 = \boldsymbol{Y}$ and hence

(8) $$\mathbf{1}^*_{\mathfrak{A}\cap\mathfrak{B}} = \mathbf{1}_{\mathfrak{G}} + 2\boldsymbol{X}_0 + \boldsymbol{A}_2.$$

Let Π be the set of all pairs (i, D_j) such that the point i belongs to the block D_j. There exist pk pairs of this kind. Obviously $\mathfrak{G}$ can be considered as a permutation group on Π, and then $\mathfrak{A} \cap \mathfrak{B}$ is the stabilizer of the pair $(1, D_1)$ in $\mathfrak{G}$. By (8) the norm of $\mathbf{1}^*_{\mathfrak{A}\cap\mathfrak{B}}$ is equal to 6, and this is equal to the number of orbits of $\mathfrak{A} \cap \mathfrak{B}$ on Π. But it is easy to check that the following 7 sets of pairs are disjoint, non-empty and left fixed by $\mathfrak{A}\cap\mathfrak{B}$, which is a contradiction: $O_1=\{(1,D_1)\}$, $O_2=\{(i,D_1),\ i\neq 1\}$, $O_3=\{(1,D_i),\ i\neq 1\}$, $O_4=\{(i,D_j),\ 1\neq i\in D_1,\ j\neq 1 \text{ and } 1\in D_j\}$, $O_5=\{(i,D_j),\ i\notin D_1 \text{ and } 1\in D_j\}$, $O_6=\{(i,D_j),\ i\in D_1 \text{ and } 1\notin D_j\}$ and $O_7=\{(i,D_j),\ i\notin D_1 \text{ and } 1\notin D_j\}$.

(k) Finally we can assume that a character $\boldsymbol{X}$ of p-type C with $\boldsymbol{X}(E)\equiv -q \pmod p$ appears in $\boldsymbol{Y}$. By the results of Brauer mentioned in (b) there exist $(p-1)/q$ characters $\boldsymbol{C}_1=\boldsymbol{X}, \boldsymbol{C}_2, \cdots, \boldsymbol{C}_{(p-1)/q}$ of $\mathfrak{G}$ which are algebraically conjugate to $\boldsymbol{X}$. Since $\boldsymbol{Y}$ is rational, every $\boldsymbol{C}_i$ appears in $\boldsymbol{Y}$ with the same multiplicity γ. Put

$$\boldsymbol{Y}=\gamma\sum_{i=1}^{(p-1)/q}\boldsymbol{C}_i+\cdots. \tag{9}$$

Put $\boldsymbol{X}(E)=cp-q$. Then c is a positive integer. From (9) we obtain that

$$\gamma((p-1)/q)(cp-q)\leqq(k-2)p+1. \tag{10}$$

By (g) and (h) we see that q divides $n=(p-1)/1$, since otherwise we get that $q=l$ and that $\mathfrak{B}$ restricted to D is triply transitive. Thus from (10) we obtain that

$$\gamma(k-1)(n/q)(cp-q)\leqq(k-2)p+1. \tag{11}$$

(11) obviously implies that $\gamma=1$, $n=q$, $c=1$ and that

$$\boldsymbol{Y}=\sum_{i=1}^{(p-1)/q}\boldsymbol{C}_i. \tag{12}$$

Since 1 and D_1 are only point and block left fixed by L respectively, we get that $\mathbf{1}^*_{\mathfrak{A}\cap\mathfrak{B}}(L)=1$. Hence by the results of Brauer mentioned in (b) we obtain (from (2) and (12)) that $\boldsymbol{C}_1(L)=0$. Thus $\boldsymbol{X}$ has l-type D, and $p\equiv q \pmod l$. Since $p\equiv 1 \pmod l$, $q=n\equiv 1 \pmod l$. Since q is bigger than 1, $n\geqq l+1$. Then $p-1=ln\geqq l(l+1)$. Therefore by (1) we get that $\lambda=1$, which is a contradiction (see (e)).

Remark. Assume that $\mathfrak{G}$ satisfies (I) and (II). If $k\geqq\frac{1}{2}(p-1)$, then by a theorem of Joran ([8]) we get that either $p=2(k-1)+1$ or $p=2(k-1)+3$. If $p=2(k-1)+1$, then by a previous result ([5]) we get that $p=11$ and $\mathfrak{G}\cong LF(2,11)$. If $p=2(k-1)+3$, then by (1) we get that $k=3$, $p=7$ and $\mathfrak{G}\cong LF(2,7)$ contradicting the assumption (II).

Bibliography

[1] R. Brauer, On permutation groups of prime degree and related classes of groups, Ann. of Math. (2) **44** (1943), 57–79.

[2] P. Dembowski, Finite geometries, Berlin Heiderberg New York 1968.

[3] N. Ito, Über die Gruppen $PSL_n(q)$, die eine Untergruppe von Primzahlindex enthalten. Acta Sci. Math. Szeged **21,** (1960), 206–217.

[4] N. Ito, On a class of doubly transitive permutation groups, Illinois J. Math. **6** (1962), 341–352.

[5] N. Ito Transitive permutation groups of degree $p=2q+1$, p and q being prime numbers. II, Trans. Amer. Math. Soc. **113** (1964), 454–487.

[6] N. Ito, On a class of doubly, but not triply transitive permutation groups, Arch. Math. **18** (1967), 564–570.

[7] N. Ito, On permutation groups of prime degree p which contain (at least) two classes of conjugate subgroups of index p, Rendiconti Sem. Mat. Padova **38** (1967), 287–292.

[8] H. Wielandt, Finite permutation groups, New York (1964).

Department of Mathematics
University of Illinois at Chicago Circle
Chicago, Illinois, 60680, USA