NOBORU ITO

On permutation groups of prime degree $p$
which contain (at least) two classes of conjugate
subgroups of index $p$

Rendiconti del Seminario Matematico della Università di Padova,
tome 38 (1967), p. 287-292

<http://www.numdam.org/item?id=RSMUP_1967__38__287_0>
ON PERMUTATION GROUPS OF PRIME DEGREE p WHICH CONTAIN (AT LEAST) TWO CLASSES OF CONJUGATE SUBGROUPS OF INDEX p

NOBORU ITO *)

Let $p$ be a prime and let $F(p)$ be the field of $p$ elements, called points. Let $G$ be a transitive permutation group on $F(p)$ such that

(I) $G$ contains a subgroup $H$ of index $p$ which is not the stabilizer of a point.

$H$ has two point orbits, say $D$ and $F(p) - D$ (cf. [3]). Let $k$ be the number of points in $D$. Then $1 < k < p - 1$. Furthermore $D = D(p, k, \lambda)$ can be considered as a difference set modulo $p$ such that the automorphism group $A(D)$ of $D$ contains $G$ as a subgroup (cf. [5]).

Replacing $D$ by $F(p) - D$, if need be, we always can assume that $k \leq \frac{1}{2} (p - 1)$.

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

(i) Let $F(q)$ be the field of $p$ elements. Let $V(r, q)$, $LF(r, q)$ and $SF(r, q)$ be the $r$-dimensional vector space, the $r$-dimensional projective special linear and semilinear groups over $F(q)$ respectively.

*) This research was partially supported by National Science Foundation Grant GP-6539.

Indirizzo dell'A.: Depart. of Mathematics, University of Illinois at Chicago Circle, Box 4348, Chicago, Ill. 60680 USA.
where \( r \geq 3 \) and \( p = \frac{q^r - 1}{q - 1} \). Let \( \Pi \) be the set of one dimensional subspaces of \( V(r, q) \). \( SF(r, q) \) can be considered as a permutation group on \( \Pi \). Identify \( \Pi \) with \( F(p) \). Then any subgroup \( \mathcal{G} \) of \( SF(r, q) \) containing \( LF(r, q) \) satisfies (I) with parameters \( k = \frac{q^{r-1} - 1}{q - 1} \) and \( \lambda = \frac{q^{r-2} - 1}{q - 1} \).

(ii) \( \mathcal{G} = LF(2, 11) \), where \( p = 5 \) and \( \lambda = 2 \).

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

(II) the restriction of \( \mathcal{B} \) to \( D \) is faithful (cf. [5]).

Thus it is natural to ask whether this is the only group satisfying (I) and (II). The purpose of this note is to make a first step towards the solution. We prove the following theorem.

Let \( \mathcal{G} \) be a group satisfying (I) and (II). If \( k \) is a prime, then \( \mathcal{G} \cong LF(2, 11) \).

**Proof.** (a) First of all, we recall the following fundamental equality for the difference set

\( \lambda (p - 1) = k (k - 1) \).

Since \( k \) is a prime by assumption, from (1) we see that \( k \) divides \( p - 1 \). Put

\( p - 1 = kN \),

which implies by (1) that

\( k - 1 = \lambda N \).

(b) Let \( \mathcal{P} \) be a Sylow \( p \)-subgroup of \( \mathcal{G} \) and let \( N_{\mathcal{P}} \mathcal{P} \) be the normalizer of \( \mathcal{P} \) in \( \mathcal{G} \). Then since \( \mathcal{G} = \mathcal{P}\mathcal{B} \), \( N_{\mathcal{P}} \mathcal{P} = \mathcal{P}\mathcal{Q} \) with \( \mathcal{Q} = \mathcal{B} \cap N_{\mathcal{P}} \mathcal{P} \). \( \mathcal{Q} \) is cyclic of order \( q \), where \( q \) is a divisor of \( p - 1 \). Clearly \( \mathcal{Q} \) leaves \( D \) fixed. Also clearly \( \mathcal{Q} \) leaves only one point fixed. Thus either \( k \equiv 1 \) (mod \( q \)) or \( k \equiv 0 \) (mod \( q \)). In the former case, by (2)

\( N \equiv 0 \) (mod \( q \)).

\(^1\) For the theory of difference sets see [7].
In the latter case, since \( k \) is prime,

\begin{equation}
(5) \quad k = q.
\end{equation}

(c) The restriction of \( H \) to \( D \) is doubly transitive.

Otherwise, by assumption (II) and by a theorem of Burnside \( H \) is metacyclic of order \( k \zeta \), where \( \zeta \) is a proper divisor of \( k - 1 \). Hence the order \( g \) of \( G \) is equal to \( pk\zeta \). On the other hand, by Sylow’s Theorem, \( g = pq(1 + np) \), where \( n \) is positive, since \( G \) is clearly nonsolvable. Thus

\begin{equation}
(6) \quad q(1 + np) = k\zeta.
\end{equation}

If \( k = q \), then from (6) \( 1 + p \leq 1 + np = \zeta \). This is a contradiction. Thus \( 1 + np \equiv 1 + n \equiv 0 \pmod{k} \). Put \( n = ak - 1 \). Then from (2) and (6) we obtain

\begin{equation}
(7) \quad q(aNk + a - N) = \zeta.
\end{equation}

Since \( N > 1 \) and \( k > 1 \), \( Nk \geq N + k \). Thus from (7) \( k < \zeta \). This is a contradiction.

(d) Let \( k \) be a Sylow \( k \)-subgroup of \( G \) contained in \( H \). By assumption (II) the restriction of \( k \) to \( D \) is faithful. Thus \( k \) is of order \( k \). If \( k \) leaves fixed at least two points, then since \( G \) is doubly transitive on \( F(p) \), the index of \( k \) in \( G \) is divisible by \( p - 1 \). This contradicts (2). Thus \( K \) leaves fixed exactly one point, say \( i \). Then \( i \) belongs to \( F(p) - D \). Let \( Ns_k \) be the normalizer of \( k \) in \( G \). Since clearly \( D \) is the only block left fixed by \( k \), \( Ns_k \) is contained in \( H \). By assumption (II) \( k \) coincides with its own centralizer. Thus the order of \( Ns_k \) equals \( k\zeta \), where \( \zeta \) is a divisor of \( k - 1 \).

(e) Let \( A(i) \) be the stabilizer of \( i \) in \( G \). If \( G \cong LF(2, 11) \), then the restriction of \( H \cap A(i) \) to \( D \) is doubly transitive.

Otherwise, by assumption (II) and by a theorem of Burnside \( H \cap A(i) \) is contained in \( Ns_k \). Since \( Ns_k \) leaves \( i \) fixed, \( Ns_k = H \cap A(i) \). Thus \( \zeta \) is a proper divisor of \( k - 1 \). Since \( B:H \cap A(i) = p - k \), the order of \( B \) is equal to \( (p - k)k\zeta \).

Now let \( B' \) be a minimal normal subgroup of \( B \). Then \( B' \) is a direct product of mutually isomorphic simple groups. Since the restriction of \( B \) to \( D \) is doubly transitive, the restriction of \( B' \) to
D is transitive. Since $k$ has order $k$, $H'$ is simple. By Sylow's Theorem $H = H' (N \triangleleft K)$. Thus $H'$ has order $(p - k) k'\zeta'$, where $\zeta'$ is a divisor of $k - 1$.

Now by (2) $p - k = (N - 1) k + 1$. If $\lambda = 1$, then by a theorem of Ostrom-Wagner ([6]) $G$ does not satisfy the assumption (II). Hence by (3) $N - 1 = \frac{k - 1}{\lambda} - 1 \leq \frac{k - 3}{2}$. Therefore by a theorem of Brauer ([1], Theorem 10) either (a) $N = 2$, $H' = LF(2, k)$ or (b) $N = \frac{k - 1}{2}$, $H' = LF(2, k - 1)$, $k - 1 = 2^n$.

By a previous result ([3]) $G$ cannot be triply transitive on $F(p)$. If (a) occurs and if $p > 11$, then by a previous result ([4]) $G$ is quadruply transitive on $F(p)$. Thus $p = 11$. Then it is easy to check that $G = LF(2, 11)$.

Suppose that (b) occurs. Then by (3) $\lambda = 2$. Now from $g = pq(1 + np) = p(p - k) k\zeta$ it follows that

$$k^2 \zeta + q \equiv 0 \pmod{p}.$$ 

By (2) $k^2 \equiv k - 2 \pmod{p}$. Thus

$$(k - 2) \zeta + q \equiv 0 \pmod{p}.$$ 

Since $p = \left(\frac{k - 1}{2}\right) k + 1$ and $\zeta \leq \frac{k - 1}{2}$, we obtain from (8)

$$\frac{(k - 2)(k - 1)}{2} + q \geq \frac{k(k - 1)}{2} + 1,$$

which implies that

$$q \geq k.$$ 

Then by (4) and (5) $q = k$. Now again from $g + pq(1 + np) = p(p - k) k$ it follows that

$$k\zeta + 1 \equiv 0 \pmod{p},$$

which implies that

$$\zeta = \frac{k - 1}{2}.$$


On permutation groups of prime degree $p$ which contain etc. 291

From (10), $g = pq (1 + np) = p (p - k) k \zeta$ and $\lambda = 2$ it follows that

\[ n = \frac{k - 3}{2}. \]

Now let $G'$ be a minimal normal subgroup of $G$. Then $G'$ has order $pq (1 + n'p)$ with $n' \leq n$. Hence again by a theorem of Brauer ([1], Theorem 10) $n' = 1$ and $G' \cong LF(2, p)$. Then $k = q = \frac{p - 1}{2}$.

Thus $k = 5, p = 11$, and $G = G' \cong LF(2, 11)$.

(f) The line through two distinct points $i$ and $j$ is the intersection of all the blocks containing both $i$ and $j$ (cf. [2]). Since $G$ is doubly transitive on $F(p)$, every line contains the same number of points. Let $s$ be the number of points on a line. Then

\[ N \equiv 0 \pmod{s(s - 1)}. \]

In particular, if $N \geq 4$, then

\[ s \leq N - 1. \]

In fact, the number of lines is equal to

\[ \binom{p}{2} \binom{s}{2} = \frac{p (p - 1)}{2} \frac{s (s - 1)}{2} = \frac{p k N}{s} (s - 1). \]

Since $p$ and $k$ are primes and since $\lambda \geq s$, we obtain (12).

(g) Assume that $G \cong LF(2, 11)$. Let 0 and 1 be two distinct points of $D$. Let $A(0)$ and $A(1)$ be the stabilizers of 0 and 1 in $G$ respectively. Then by (e) we see at once that $A(0) \cap A(1) \cap B: A(0) \cap A(1) \cap B \cap A(1) = p - k$. Thus the orbit of $A(0) \cap A(1)$ containing $i$ contains $F(p) - D$. Clearly this is the case for every block containing both 0 and 1. Thus the orbit of $A(0) \cap A(1)$ containing $i$ coincides with the line determined by 0 and 1. Now considering the index of $A(0) \cap A(1) \cap B \cap A(i)$ in $A(0) \cap A(1)$ we obtain

\[ \lambda (p - k) = \ell (p - s), \]
where $t$ is the index of $A(0) \cap A(1) \cap B \cap A(i)$ in $A(0) \cap A(1) \cap A(2)$. From (14) we obtain
\begin{equation}
(15) \quad k = (\lambda - t)p + ts.
\end{equation}
Since by (13) $ts < \lambda N < k$, $\lambda - t$ is positive. From (2) and (15) it follows that
\[ \lambda - t + ts \equiv 0 \pmod{k}, \]
which implies that
\begin{equation}
(16) \quad \lambda - t + ts = k.
\end{equation}
From (2), (15), (16) we obtain
\[ k = (k - ts)p + ts = (k - ts)(kN + 1) + ts = (k - ts)kN + k, \]
which implies that
\begin{equation}
(17) \quad p = \lambda + tsN.
\end{equation}
But by (3) and (13) $p - \lambda + tsN < \lambda + \lambda sN < \lambda + sk \leq \lambda + (N - 1)k < p$. This contradiction establishes $G \cong LF(2, 11)$.

\section*{BIBLIOGRAPHY}


Manoscritto pervenuto in redazione il 17 marzo 1967