RENDICONTI
del
SEMINARIO MATEMATICO
della
UNIVERSITÀ DI PADOVA

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 $\mathfrak{G}$ be a transitive permutation group on $F(p)$ 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 $F(p) - D$ (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 $\mathfrak{G}$ 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 $\mathfrak{G}$ of degree p satisfyng 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 $p = \dfrac{q^r - 1}{q - 1}$. 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 $F(p)$. Then any subgroup $\mathfrak{G}$ of $SF(r, q)$ containing $LF(r, q)$ satisfies (I) with parameters $k = \dfrac{q^{r-1} - 1}{q - 1}$ and $\lambda = \dfrac{q^{r-2} - 1}{q - 1}$.

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

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

(II) the restriction of $\mathfrak{B}$ 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 $\mathfrak{G}$ be a group satisfying (I) and (II). If k is a prime, then $\mathfrak{G} \cong LF(2, 11)$.

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

$$\lambda (p - 1) = k (k - 1). \text{ [1]} \tag{1}$$

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

$$p - 1 = kN, \tag{2}$$

which implies by (1) that

$$k - 1 = \lambda N. \tag{3}$$

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

$$N \equiv 0 \pmod q. \tag{4}$$

[1]) For the theory of difference sets see [7].

In the latter case, since k is prime,

$$k = q. \tag{5}$$

(c) The restriction of $\mathfrak{B}$ to D is doubly transitive.

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

$$q(1 + np) = k\zeta. \tag{6}$$

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

$$q(aNk + a - N) = \zeta. \tag{7}$$

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

(d) Let $\mathfrak{K}$ be a Sylow k-subgroup of $\mathfrak{G}$ contained in $\mathfrak{B}$. By assumption (II) the restriction of $\mathfrak{K}$ to D is faithful. Thus $\mathfrak{K}$ is of order k. If $\mathfrak{K}$ leaves fixed at least two points, then since $\mathfrak{G}$ is doubly transitive on $F(p)$, the index of $\mathfrak{K}$ in $\mathfrak{G}$ 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 $Ns\mathfrak{K}$ be the normalizer of $\mathfrak{K}$ in $\mathfrak{G}$. Since clearly D is the only block left fixed by $\mathfrak{K}$, $Ns\mathfrak{K}$ is contained in $\mathfrak{B}$. By assumption (II) $\mathfrak{K}$ coincides with its own centralizer. Thus the order of $Ns\mathfrak{K}$ equals $k\zeta$, where ζ is a divisor of $k - 1$.

(e) Let $\mathfrak{A}(i)$ be the stabilizer of i in $\mathfrak{G}$. If $\mathfrak{G} \not\cong LF(2, 11)$,[2] then the restriction of $\mathfrak{B} \cap \mathfrak{A}(i)$ to D is doubly transitive.

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

Now let $\mathfrak{B}'$ be a minimal normal subgronp of $\mathfrak{B}$. Then $\mathfrak{B}'$ is a direct product of mutually isomorphic simple groups. Since the restriction of $\mathfrak{B}$ to D is doubly transitive, the restriction of $\mathfrak{B}'$ to

[2]) Read: $\mathfrak{G}$ is not isomorphic to ...

D is transitive. Since $\mathfrak{K}$ has order k, $\mathfrak{B}'$ is simple. By Sylow's Theorem $\mathfrak{B} = \mathfrak{B}'(Ns\mathfrak{K})$. Thus $\mathfrak{B}'$ has order $(p-k)k\zeta'$, where ζ' 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]) $\mathfrak{G}$ 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 (α) $N=2, \mathfrak{B}'=LF(2,k)$ or (β) $N=\frac{k-1}{2}$, $\mathfrak{B}'=LF(2,k-1)$, $k-1=2^u$.

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

Suppose that (β) 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

$$(k-2)\zeta+q\equiv 0 \pmod p. \tag{8}$$

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

$$q\geq k. \tag{9}$$

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

$$\zeta=\frac{k-1}{2}. \tag{10}$$

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

$$n = \frac{k-3}{2}. \tag{11}$$

Now let $\mathfrak{G}'$ be a minimal normal subgroup of $\mathfrak{G}$. Then $\mathfrak{G}'$ has order $pq(1 + n'p)$ with $n' \leq n$. Hence again by a theorem of Brauer ([1], Theorem 10) $n' = 1$ and $\mathfrak{G}' \cong LF(2, p)$. Then $k = q = \frac{p-1}{2}$. Thus $k = 5, p = 11$, and $\mathfrak{G} = \mathfrak{G}' \cong LF(2, 11)$.

(*f*) The line through two distinct points i and j is the intersection of all the bloks containing both i and j (cf. [2]). Since $\mathfrak{G}$ 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

$$N \equiv 0 \pmod{s(s-1)}. \tag{12}$$

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

$$s \leq N - 1. \tag{13}$$

In fact, the number of lines is equal to

$$\binom{p}{2} \Big/ \binom{s}{2} = p(p-1)/s(s-1) = pkN/s(s-1).$$

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

(*g*) Assume that $\mathfrak{G} \not\cong LF(2, 11)$. Let 0 and 1 be two distinct points of D. Let $\mathfrak{A}(0)$ abd $\mathfrak{A}(1)$ be the stabilizers of 0 and 1 in $\mathfrak{G}$ respectively. Then by (*e*) we see at once that $\mathfrak{A}(0) \cap \mathfrak{A}(1) \cap \mathfrak{B} : \mathfrak{A}(0) \cap \mathfrak{A}(1) \cap \mathfrak{B} \cap \mathfrak{A}(1) = p - k$. Thus the orbit of $\mathfrak{A}(0) \cap \mathfrak{A}(1)$ containing i contains $F(p) - D$. Clearly this is the case for every block containing both 0 and 1. Thus the orbit of $\mathfrak{A}(0) \cap \mathfrak{A}(1)$ containing i coincides with the line determined by 0 and 1. Now considering the index of $\mathfrak{A}(0) \cap \mathfrak{A}(1) \cap \mathfrak{B} \cap \mathfrak{A}(i)$ in $\mathfrak{A}(0) \cap \mathfrak{A}(1)$ we obtain

$$\lambda(p - k) = t(p - s), \tag{14}$$

where t is the index of $\mathfrak{A}(0) \cap \mathfrak{A}(1) \cap \mathfrak{B} \cap \mathfrak{A}(i)$ in $\mathfrak{A}(0) \cap \mathfrak{A}(1) \cap \mathfrak{A}(2)$. From (14) we obtain

$$k = (\lambda - t)p + ts. \tag{15}$$

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

$$\lambda - t + ts = k. \tag{16}$$

From (2), (15), (16) we obtain

$$k = (k - ts)p + ts = (k - ts)(kN + 1) + ts = (k - ts)kN + k,$$

which implies that

$$p = \lambda + tsN. \tag{17}$$

But by (3) and (13) $p = \lambda + tsN < \lambda + \lambda sN < \lambda + sk \leq \lambda + (N-1)k < p$. This contradiction establishes $\mathfrak{G} \cong LF(2, 11)$.

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 - A. Wagner, *Some characterizations of finite projective spaces*, Arch. Math. 11 (1960), 465-469.

[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, *Transitive permutation groups of degree $p = 2q + 1$, p and q being prime numbers III*, Trans. Amer. Math. Soc. 116 (1965), 151-166.

[5] N. Ito, *On a class of doubly, but not triply transitive permutation groups*, to appear in Arch. Math.

[6] T. G. Ostrom - A. Wagner, *On projective and affine planes with transitive collineation groups*, Math. Zeitschr. 7 (1959), 186-199.

[7] H. J. Ryser, *Combinatorial mathematics*, MAA (1963).

Manoscritto pervenuto in redazione il 17 marzo 1967