PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 37, Number 2, February 1973

A PROPERTY OF THE GROUPS $P\Gamma L(m, q)$, $q \geqq 5$

PETER LORIMER

ABSTRACT. It is well known that the existence of a sharply doubly transitive set of permutations is equivalent to the existence of a projective plane. The natural representation of the group $P\Gamma L(m, q)$, $m \geqq 2$, is doubly transitive and it is proved here that this permutation group does not contain a sharply doubly transitive subset when $q \geqq 5$.

The basic problem of the existence of projective planes can be phrased in terms of sharply doubly transitive subsets of permutation groups. If G is a group of permutations on a set Σ and R is a subset of G we call R sharply doubly transitive on Σ if:

I. $1 \in R$.

II. If $\alpha, \beta, \gamma, \delta \in \Sigma$, $\alpha \neq \beta$, $\gamma \neq \delta$ there is a unique member $r \in R$ with $r(\alpha)=\gamma$, $r(\beta)=\delta$.

III. The relation $\sim$ defined on R by $r \sim s$ if $r=s$ or $r(\alpha) \neq s(\alpha)$ for every $\alpha \in \Sigma$ is an equivalence relation. Each equivalence class is sharply transitive on Σ, i.e. if $\alpha, \beta \in \Sigma$ each class contains a unique member r with $r(\alpha)=\beta$.

If Σ is a finite set III follows from I and II.

The group $P\Gamma L(m, q)$ has a natural representation as a doubly transitive group of degree $(q^m-1)/(q-1)$ on the points of the projective $m-1$ dimensional space $P(m-1, q)$ over the field of order q. If it had a sharply doubly transitive subset this could be used to define a projective plane of order $(q^m-1)/(q-1)$. However we will prove

THEOREM. *Let q be a power of a prime number, $q \geqq 5$ and m an integer, $m \geqq 2$. Then the group $P\Gamma L(m, q)$ represented as a permutation group on $P(m-1, q)$ does not have a sharply doubly transitive subset.*

The groups $P\Gamma L(2, q)$, $q=2, 3, 4$, all contain a sharply doubly transitive subset. These subsets correspond to the Desarguesian planes of orders 3, 4 and 5 respectively. For this reason the technique of proof used here fails to determine the nonexistence of such a subset for $P\Gamma L(m, q)$, $m>2$, $q=2, 3, 4$.

Received by the editors December 8, 1971.

AMS (MOS) subject classifications (1970). Primary 20B20, 50D35.

We use the notations of [1]. $P\Gamma L(m, q)$ will always have its representation as a permutation group on $P(m-1, q)$.

We will need the results of the following Lemma which we give here without proof.

LEMMA. *Let G be a permutation group on a finite set Σ which has n members and suppose that G has a sharply doubly transitive subset R. Then*

(1) *R has $n(n-1)$ members.*

(2) *The equivalence classes of R under $\sim$ each contain n members.*

(3) *R contains $n-1$ members which fix no symbol of Σ and $n(n-2)$ which fix one symbol. Only the identity in R fixes more than one symbol.*

(4) *If $r \in R$, $r^{-1}R$ is also a sharply doubly transitive subset of G.*

The proof splits into a number of cases which we will treat in separate sections.

1. $m=2, q\equiv 0(2)$. In this section we assume that $m=2$ and $q\equiv 0(2)$. Then $q=2^k$ for some positive integer k, $P\Gamma L(2, q)$ has order $k(q-1)q(q+1)$ and has $PSL(2, q)$ as a normal subgroup of index k. No member of $PSL(2, q)$ except 1 fixes three symbols of $P(1, q)$ and the members of $PSL(2, q)$ which fix one symbol are exactly the involutions. The Sylow 2-subgroups of $PSL(2, q)$ are elementary abelian of order q and the intersection of any two is 1. If a and b are involutions of different Sylow 2-subgroups of $PSL(2, q)$ then $a^{-1}b$ fixes zero or two members of $P(1, q)$.

Now let S be a sharply doubly transitive subset of $P\Gamma L(2, q)$ and put $S_1=S\cap PSL(2, q)$. Suppose that S_1 contains two members a and b which fix one symbol of $P(1, q)$. Then a and b are both involutions. As S is sharply doubly transitive, $a^{-1}b=ab$ cannot fix more than one symbol of $P(1, q)$. If it fixes one, ab is an involution and so $\{1, a, b, ab\}$ is a subgroup of $PSL(2, q)$. Then a and b would lie together in a Sylow 2-subgroup of $PSL(2, q)$. Otherwise $a^{-1}b$ fixes no symbol of $P(1, q)$ and so $a\sim b$. Suppose that not all the involutions of S_1 lie in one Sylow 2-subgroup of $PSL(2, q)$. If a and b are two which lie in different Sylow 2-subgroups we have $a\sim b$. If c is an involution of S_1, c cannot lie in a Sylow 2-subgroup with both a and b and so either $c\sim a$ or $c\sim b$. As $\sim$ is an equivalence relation we then have both $c\sim a$ and $c\sim b$. Hence all the involutions lie in one equivalence class of S under $\sim$ and so there are at most $q+1$ of them. If all the involutions of S_1 lie in one Sylow 2-subgroup there are at most $q-1$. Apart from involutions, S_1 can contain 1 and q members which fix no symbol of $P(1, q)$. Hence S_1 can contain at most $2(q+1)$ members.

S has $q(q+1)$ members and $PSL(2, q)$ has k cosets in $P\Gamma L(2, q)$ so that one of these cosets has at least $(1/k)q(q+1)$ members of S. Suppose that one such is $sPSL(2, q)$ where $s \in S$. Then $PSL(2, q)$ has at least $(1/k)q(q+1)$

members of $s^{-1}S$ and by the Lemma this is also a sharply doubly transitive subset of $P\Gamma L(2, q)$. Hence $(1/k)q(q+1) \leqq 2(q+1)$ and so $2k \geqq q = 2^k$. The only solutions of this equation are $k=1$ and $k=2$ and these cases are excluded in the statement of the Theorem.

This proves the Theorem in the cases under consideration.

2. $m=2, q \equiv 1(2)$. We now suppose that $m=2$ and $q=p^k$ where p is an odd prime number.

Let S be a sharply doubly transitive subset of $P\Gamma L(2, q)$.

The members of $P\Gamma L(2, q)$ which interchange the members 0 and ∞ of $P(1, q)$ are the transformations

$$x \rightarrow \frac{a}{x^\sigma}$$

where $a \neq 0$ and σ is an automorphism of the field $GF(q)$ with q elements, $\infty^\sigma = \infty$. As q is odd $GF(q)$ contains a member $w \neq 1$ with $ww^\sigma = 1$. If the above transformation fixes a symbol x it also fixes xw. Now S contains a member, say r, which interchanges 0 and ∞ and as r can fix at most one symbol of $P(1, q)$ we deduce that r fixes no symbol of $P(1, q)$. Because of the double transitivity of $P\Gamma L(2, q)$ the same is true with any two members of $P(1, q)$ in place of 0 and ∞. Now if α, β are two members of $P(1, q)$, R contains a member which interchanges α and β. Thus the $\frac{1}{2}q(q+1)$ transpositions $(\alpha\beta)$ occur among the cycles in the decomposition of the members of S into disjoint cycles. But from the above these all occur among the q members of S which fix no symbols of $P(1, q)$. Hence the latter must all be involutions. In a sharply doubly transitive subset T we will denote by T^* the subset containing 1 and the members of T which fix no symbols. S^* consists of 1 and involutions. Suppose $s \in S^*$. Then $s^{-1}S$ is a sharply doubly transitive subset of $P\Gamma L(2, q)$ and because $\sim$ is an equivalence relation $(s^{-1}S)^* = s^{-1}S^*$. If $t \in S^*$, $t \neq s$, then $st = s^{-1}t$ is an involution and hence $st = ts$. The members of S^* thus generate a subgroup of $P\Gamma L(2, q)$ which is an elementary abelian 2-group of order not less than $q+1$. As the Sylow 2-subgroups of the groups $PGL(2, q)$ are dihedral and the involutions of $P\Gamma L(2, q) - PGL(2, q)$ all lie in one coset we can only have the possibilities $q+1 = 4, 6$, or 8. In each case q is a prime number so that $P\Gamma L(2, q) = PGL(2, q)$. Hence we only have the case $q=3$ which is excluded from the statement of the Theorem.

This proves Theorem 1 in the case under discussion.

3. $m > 2$. In this section we complete the proof of Theorem 1. Throughout we assume that $m > 2$ and $q \geqq 5$. V will denote a vector space of dimension m over $GF(q)$ and $P(m-1, q)$ will be the set of one dimensional

subspaces of V. If $v \in V$ we denote the member of $P(m-1, q)$ containing v by $\langle v\rangle$.

Suppose u and v are two linearly independent members of V which will be fixed for the remainder of the proof. We make the following definitions:

V_1 is the subspace of V spanned by u and v;

$W=\{\langle w\rangle; w \in V_1\}$;

H is the stabilizer of $\langle u\rangle$ and $\langle v\rangle$ in $P\Gamma L(m, q)$;

K is the pointwise stabilizer of W in $P\Gamma L(m, q)$;

L is the global stabilizer of W in $P\Gamma L(m, q)$.

In a straightforward manner we obtain $K \subseteq H$ and $L=N(K)$ the normalizer of K. From the general properties of projective linear groups we also have $H \subseteq L$. As L is the global stabilizer of W, L inherits a representation as a permutation group on W. This representation has kernel K and if we take $W=P(1, q)$ we may take the image of L under this representation as $P\Gamma L(2, q)$. In particular, L is doubly transitive on W.

Now suppose that $P\Gamma L(m, q)$ has a sharply doubly transitive subset R. As L is doubly transitive on W and $H \subseteq L$ it follows that $R \cap L$ is doubly transitive on W. Hence the image of $R \cap L$ under the above permutation representation is a sharply doubly transitive subset of $P\Gamma L(2, q)$. As $q \geqq 5$ this contradicts the results of §§1 and 2 so that no such subset R can exist.

This completes the proof of the Theorem.

Reference

1. B. Huppert, *Endliche Gruppen*. I, Die Grundlehren der math. Wissenschaften, Band 134, Springer-Verlag, Berlin and New York, 1967. MR **37** #302.

Department of Mathematics, University of Auckland, Auckland, New Zealand