PACIFIC JOURNAL OF MATHEMATICS
Vol. 46, No. 1, 1973

A PROPERTY OF THE GROUPS Aut $PU(3, q^2)$

PETER LORIMER

The automorphism group Aut $PU(3, q^2)$ of the projective unitary group $PU(3, q^2)$ has a natural doubly transitive representation on $q^3 + 1$ symbols. If this group contained a sharply doubly transitive subset, it would serve to define a projective plane with $q^3 + 2$ points on a line.

However it is the purpose of this note to prove that Aut $PU(3, q^2)$ does not have such a subset when $q > 2$.

The group $PU(3, 4)$ is a sharply doubly transitive group and so forms a sharply doubly transitive subset of Aut $PU(3, 4)$. This subset corresponds to the projective plane defined by the near field of order 9.

Our result is

THEOREM. *Let q be a power of a prime number, $q > 2$. Then the group* Aut $PU(3, q^2)$ *represented in the usual way as a doubly transitive group of degree $q^3 + 1$ does not have a sharply doubly transitive subset.*

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 exactly one member r with $r(\alpha) = \beta$.

For the relation between projective planes and sharply transitive sets see [1, p. 140]. If Σ is finite III follows from II. The elementary properties of sharply doubly transitive sets are given by the following lemma which we state 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 R 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.*

If $q \geqq 5$ the theorem follows easily from the results of [3] but the cases $q = 3$ and 4 must be treated separately. In §1 we gather the results that we need about the groups Aut $PU(3, q^2)$ and the following sections give the proofs necessary for the different cases.

1. The groups Aut $PU(3, q^2)$. In our discussion of these groups we will be guided by [2, pages 233–250]. The notations established in this section will be used in the rest of the paper.

Let q be a prime power, K the field of order q^2 and τ the unique involutory automorphism of K. Let V be a 3-dimensional vector space over K and w_1, w_2, w_3 a basis of V. Define a hermitian form on V by

$$(w_2, w_2) = (w_1, w_3) = 1$$
$$(w_1, w_1) = (w_3, w_3) = (w_1, w_2) = (w_2, w_3) = 0$$

Then we may take the unitary group $U(3, q^2)$ as the group of linear transformations of V leaving this form invariant.

The 1-dimensional subspaces of V form the points and the 2-dimensional subspaces the lines of the projective plane $P(2, q^2)$ over K. $U(3, q^2)$ has its induced representation $PU(3, q^2)$ as a permutation group on the points and lines of $P(2, q^2)$ and we may take Aut $PU(3, q^2)$ as the normal extension of $PU(3, q^2)$ by the field automorphisms of K.

If $v \in V$ and $(v, v) = 0$, v is called an isotropic vector. The isotropic vectors form $q^3 + 1$ points of $P(2, q^2)$ and we will call these points isotropic points and denote the set of them by A. Aut $PU(3, q^2)$ acts faithfully and doubly transitively on A. This is the representation of Aut $PU(3, q^2)$ referred to in the theorem.

If $v \in V$, $v \neq 0$, we will denote the point of $P(2, q^2)$ which contains v by $\langle v \rangle$ and if $u \notin \langle v \rangle$ we denote the line of $P(2, q^2)$ which contains both u and v by $\langle u, v \rangle$.

If l is a line of $PU(3, q^2)$ which contains 2 isotropic points then it contains exactly $q + 1$. If L is the stabilizer of l in Aut $PU(3, q^2)$ L has a representation as a permutation group on the $q + 1$ isotropic points of l and this representation may be taken as Aut $PU(2, q^2)$ acting on these points. The representation is thus permutation isomorphic to Aut $PGL(2, q) = P\Gamma L(2, q)$, see [2, p. 237].

It is now necessary to consider this representation in more detail. As Aut $PU(3, q^2)$ is doubly transitive on A it is sufficient to consider the line $l = \langle w_1, w_3 \rangle$. We define the following subgroups of Aut $PU(3, q^2)$:

L is the stabilizer of l;

H is the stabilizer of both $\langle w_1 \rangle$ and $\langle w_3 \rangle$;

M is the stabilizer of all isotropic points $\langle w \rangle$ with $\langle w \rangle \in l$.

In a straightforward manner we find that $M \subseteqq H$ and that M is the kernel of the representation of L on the $q+1$ isotropic points of l. From the properties of the linear group $U(3, q^2)$ we also find that if $\langle u\rangle$, $\langle v\rangle$ are two isotropic vectors of l then L consists precisely of those members f of Aut $PU(3, q^2)$ with $f\langle u\rangle, f\langle v\rangle \in l$. In particular $H \subseteqq L$ and L is doubly transitive on the isotropic points of l.

Considering now a possible sharply doubly transitive subset R of Aut $PU(3, q^2)$. We can prove the following.

PROPOSITION. *Let R be a sharply doubly transitive subset of* Aut $PU(3, q^2)$. *Then the members $rM, r \in R \cap L$, of L/M form a sharply doubly transitive subset of L/M in its representation on the isotropic points of l.*

Proof. It is sufficient to notice that if $\langle u\rangle$, $\langle v\rangle$ are two isotropic vectors of l then $R \cap L$ contains all those members r of R with $r\langle u\rangle$, $r\langle v\rangle \in l$.

2. $q \geqq 5$. The results of [3] enable us to prove our theorem when $q \geqq 5$.

Suppose that Aut $PU(3, q^2)$ has a sharply doubly transitive subset R. Using the proposition in §1 we obtain a sharply doubly transitive subset of the group L/M. As this group is permutation isomorphic to $P\Gamma L(2, q)$ we obtain a sharply doubly transitive subset of $P\Gamma L(2, q)$. This contradicts the results of [3] when $q \geqq 5$.

As the groups $P\Gamma L(2, 3)$ and $P\Gamma L(2, 4)$ each contain a sharply doubly transitive subset this proof does not work for $q = 3$ or $q = 4$ and it is necessary to treat these cases separately. We do this in the next two sections.

3. $q = 3$. In this section we treat the group Aut $PU(3,9)$. $PU(3,9)$ has order 28.27.8 and has index 2 in Aut $PU(3, 9)$. K has 9 members and we may take them as the elements $a + ib$ where $a, b = 0, 1, -1$, the members of the field of order 3 and $i^2 + 1 = 0$. The one automorphism τ of K is given by $\tau(a + ib) = a - ib$ or equivalently $\tau(x) = x^3$ for all $x \in K$. The set A of isotropic points has 28 members.

The stabilizer of the two points $\langle w_1\rangle$ and $\langle w_3\rangle$ of l has order 16. Thus Aut $PU(3, 9)$ has 16 members which interchange $\langle w_1\rangle$ and $\langle w_3\rangle$. Following [2, p. 242] we may take these as the transformations $T(\sigma, k)$, $\sigma = 1, \tau, k \in K - \{0\}$ defined by

$$(x, y, z) \longrightarrow (kz^\sigma, k^2y^\sigma, k^{-3}x^\sigma) .$$

Suppose now that Aut $PU(3, 9)$ has a sharply doubly transitive subset

R. Then R contains exactly one member r which interchanges $\langle w_1\rangle$ and $\langle w_3\rangle$. As the stabilizer of $\langle w_1\rangle$ and $\langle w_3\rangle$ has order 16, r is a 2-element. If it fixed one member of A it would have to fix another as A has 28 members. From the lemma in the introduction it follows that r fixes no members of A, i.e., $r \sim 1$. Denote the class of 1 under this relation by R^*. R^* contains 28 members and because of the double transitivity of Aut $PU(3, 9)$ the above shows that when we decompose the members of R^* into disjoint cycles we obtain (1/2)28.27 transpositions. Thus the 27 nonidentity members of R^* must all be involutions. In particular, r is an involution.

We now proceed to show that every involution interchanging $\langle w_1\rangle$ and $\langle w_3\rangle$ fixes at least two isotropic points and hence show that r cannot exist.

Any involution interchanging $\langle w_1\rangle$ and $\langle w_3\rangle$ is conjugate to one of $T(1, 1)$, $T(\tau, 1)$ or $T(\tau, 1+i)$. $T(1, 1)$ fixes $\langle(1, -1, 1)\rangle$ and $\langle(1, 1, 1)\rangle$, $T(\tau, 1)$ fixes $\langle(1, 0, i)\rangle$ and $\langle(1, 0, -i)\rangle$ and $T(\tau, 1+i)$ fixes $\langle(1-i, 1-i, i)\rangle$ and $\langle(1-i, -1+i, i)\rangle$. In each case we have two isotropic vectors so that none of these can be r.

Thus no r interchanging $\langle w_1\rangle$ and $\langle w_3\rangle$ can exist and this proves the result when $q = 3$.

4. $q = 4$. Finally we treat the case $q = 4$.

The group Aut $PU(3, 16)$ has order $65\cdot 64\cdot 15\cdot 4$ and has $PU(3, 16)$ as a subgroup of index 4. In this case there are 65 isotropic points in $P(2, 16)$ and we are interested in the representation on the set A containing these 65 points. We let w_1, w_3, l, H, L, and M be as in Section 1. The line l containing $\langle w_1\rangle$ and $\langle w_3\rangle$ contains 5 isotropic points and we will denote the set of them by l^*.

H has a normal Sylow 5-subgroup consisting of the transformations arising from the matrices $S(k, \alpha)$ in $U(3, 16)$ for $\alpha, k \in K$ $\alpha^5 = k^5 = 1$ where $S(k, \alpha)$ is the matrix

$$\begin{pmatrix} k & \cdot & \cdot \\ \cdot & \alpha & \cdot \\ \cdot & \cdot & k \end{pmatrix}$$

relative to the basis w_1, w_2, w_3. Such a matrix fixes every point on the (projective) line l and also fixes the point $\langle w_2\rangle$. Now consider the lines through $\langle w_2\rangle$ in $P(2, 16)$. There are 17 of them and each meets l in a point fixed by $S(k, \alpha)$. Thus $S(k, \alpha)$ fixes each of these lines. If $w \in l^*$, $w + \alpha w_2$ has length α^5 and so the line through $\langle w\rangle$ and $\langle w_2\rangle$ contains exactly one isotropic point, namely $\langle w\rangle$. As l^* contains 5 points the remaining 60 isotropic points are distributed among the other 12 lines through w_2 and as no line can contain more than 5 isotropic points it follows that each of these lines contains exactly 5.

Now consider the Sylow 5-subgroups of $PU(3, 16)$. They have order 25 and so are abelian. As any 5-element fixing 2 isotropic points is conjugate to a matrix $S(k, \alpha)$, such a 5-element fixes exactly 5 isotropic points and moves the other 60 points in orbits of length 5. If $PU(3, 16)$ contained an element of order 25 it would have to fix no isotropic point and yet have its 5th power fixing exactly 5 such points. This is not possible so that the Sylow 5-subgroups are elementary abelian.

If a is a 5-element of $M \cap PU(3, 16)$ and b is a 5-element of $PU(3, 16)$ it follows that a and b lie in a Sylow 5-subgroup together if and only if $ab = ba$. Reference to the end of § 1 shows that $L/M \cong P\Gamma L(2, 4)$ and as L contains a Sylow 5-subgroup of $PU(3, 16)$ and M has order 5, L contains the same number of Sylow 5-subgroups as $P\Gamma L(2, 4)$, namely 6. Any two intersect in M so that each 5-element of M commutes with exactly 124 5-elements of L and clearly commutes with no other 5-element of $PU(3, 16)$. Again let a be a 5-element of M. We showed in the last paragraph that a fixes 12 lines which contain 5 isotropic points each and it can clearly not fix any more such lines. Hence for 12 lines a lies in the normalizer of the stabilizer of the 5 isotropic points on the line. It thus commutes with each of the 4 5-elements which fix all these points. Hence a commutes with $12 \cdot 4 = 48$ 5-elements outside M which fix exactly 5 isotropic vectors and so commutes with $120-48 = 72$ 5-elements which fix no isotropic vector. As L contains 6 Sylow 5-subgroups it follows that each Sylow 5-subgroup contains 12 members which fix no isotropic point.

We now suppose that R is a sharply doubly transitive subset of Aut $PU(3, 16)$. From the results at the end of § 1 we see that $R \cap L$ contains 20 members and because $P\Gamma L(2, 4)$ contains only one type of sharply doubly transitive subset, namely that corresponding to the set of semilinear transformation $x \to ax + b$, $a \neq 0$ over the field of order 5, it follows that $R \cap L$ contains 4 members which have in their decomposition into disjoint cycles, a cycle of order 5 on the isotropic points of l^*. If r is one of these and r fixes an isotropic point, say u, then r^5 fixes 6 isotropic points, namely u and the 5 members of l^*. But only the identity in Aut $PU(3, 16)$ fixes more than 5 isotropic points and so $r^5 = 1$. But each element of order 5 fixes either 5 or no isotropic points and as no member of R except 1 can fix more than one point we obtain a contradiction. Hence r fixes no isotropic points or $r \sim 1$. If we denote the equivalence class containing 1 by R^* it follows that we obtain $(65 \cdot 64)/(5 \cdot 4) \cdot 4$ 5-cycles when we decompose the members of R^* into disjoint cycles. As R^* contains only 64 members apart from 1 each of these must decompose into 13 5-cycles, i.e., each must be an element of order 5 and moreover the isotropic points in each 5-cycle which occurs must lie together on one line in $P(2, 16)$.

Let r be a member of R^*-{1} and denote the set of 5-elements of Aut $PU(3, 16)$ which fix 5 points of A by Q. Suppose that r lies in α Sylow 5-subgroups. The intersection of any two of them can only consist of r and its powers so that no member of Q lies in two of them. Each contains 12 members of Q so that r commutes with 12 α members of Q. On the other hand we have shown that r fixes 13 lines containing 5 isotropic vectors each and as $PU(3, 16)$ is transitive on such lines it follows from the above analysis that r commutes with the 4 5-elements that fix the points of each line and r commutes with no other member of Q. Thus r commutes with 13.4 members of Q and so $13.4 = 12\alpha$. As α is an integer we have a contradiction.

This establishes the result when $q = 4$ and so proves the theorem.

REFERENCES

1. P. Dembowski, *Finite Geometries*, Springer-Verlag, Berlin 1968.
2. B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin 1967.
3. P. Lorimer, *A Property of the Groups* $P\Gamma L(m, q)$. $q \geqq 5$. To appear Proc. Amer. Math. Soc.

Received January 28, 1972 and in revised form June 22, 1972.

UNIVERSITY OF AUCKLAND