Projective Planes with a Condition on Projectivities

Peter Lorimer

University of Auckland, Auckland, New Zealand[1]

Introduction

Let π be a projective plane, L, M two lines of $\pi, \sum$ the set of points on L excluding the point of intersection of L and M, and I a point of π lying on neither L nor M. If J is any point of π not lying on L or M we can define a permutation r of $\sum$ by first projecting L onto M through I and then projecting M back onto L through J. We denote the set of permutations r obtained from every such J by R. R has the following properties which are characteristic of projective planes.

I $1 \in R$

II If $\alpha, \beta, \gamma, \delta \in \sum$, $\alpha \neq \beta$, $\gamma \neq \delta$ there is a unique member r of R with the properties $r(\alpha) = \gamma$, $r(\beta) = \delta$

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

A set R of permutations on a set $\sum$ which satisfies I, II and III will be called sharply doubly transitive and if G is a group of permutations on $\sum$ which contains R we call R a sharply doubly transitive subset of G.

A consequence of the axiom of Pappus in a projective plane is that any projectivity of a line which transposes two points of the line must act as an involution on the line. The converse of this result follows from a theorem of J. Tits [4]. The unrestricted group of projectivities on a line in a projective plane acts triply transitively on the points of that line and it is a simple consequence of the result of Tits that a triply transitive group in which only involutions transpose symbols must be a group $PGL(2, F)$ of all bilinear transformations

[1] This research was partially supported by National Science Foundation grant GP-11342 at the University of Notre Dame.

$$x \to \frac{ax+b}{cx+d} \qquad ad - bc \neq 0$$

over a field F. This is enough to ensure that Pappus' Theorem holds in the plane. Here we investigate the less restrictive situation suggested in the first paragraph.

Our main result is

THEOREM 1. *Let G be a group of permutations on a finite set $\sum$. Suppose that G contains a sharply doubly transitive subset R and satisfies*

IV *If $g \in G$, $\sigma \in \sum$, $g(\sigma) \neq \sigma$ but $g^2(\sigma) = \sigma$ then $g^2 = 1$.*

Then G has a normal regular subgroup V and

(i) *if $\sigma \in \sum$ the stabilizer of σ in G contains a subset R_σ such that $R = VR_\sigma$*

(ii) *the stabilizer in G of any two elements of $\sum$ is an elementary abelian 2-group (possibly 1).*

The proof relies heavily on M. Aschbacher's classification of finite doubly transitive groups in which the stabilizer of any two points is abelian.

Our result has the following consequence for the theory of projective planes

THEOREM 2. *Let π be a finite projective plane and let $L, M, \sum, I$ and R be as in the first paragraph above. If R generates the subgroup G of the symmetric group on $\sum$ and G satisfies IV then π is the dual of a translation plane.*

The proof is direct and will not be given here.

Proof of Theorem 1

We now suppose that G satisfies the hypotheses of Theorem 1. If $\alpha, \beta \in \sum$ and K is any subgroup of G we write K_α for the stabilizer of α in K and $K_{\alpha\beta}$ for the stabilizer of α and β in K.

We note first that G is clearly doubly transitive on $\sum$.

Let α, β be any two fixed symbols of $\sum$. As G is doubly transitive G contains a member a which interchanges α and β. By assumption we then have $a^2 = 1$. If $h \in G_{\alpha\beta}$, ah also interchanges α and β so that $(ah)^2 = 1$. Hence every member of $aG_{\alpha\beta}$ is an involution and so $G_{\alpha\beta}$ is abelian. We can now apply Aschbacher's result [1] and deduce that one of the following is true

(1) G has a normal regular subgroup.

(2) $G = L_3(2)$.

(3) $G = R(3)$ the smallest Ree group.

(4) G has a unique minimal normal subgroup $M(G)$ with $G \subseteq \operatorname{Aut} M(G)$ and $M(G) = L_2(q)$, $U_3(q)$, $Sz(q)$ or $R(q)$.

By equality in each case we mean that G or $M(G)$ is permutation isomorphic to the given group where the latter has its usual representation as a doubly transitive permutation group. However there is no loss in generality by assuming that this relation is equality.

Our immediate task now is to show that conclusions (2), (3) and (4) cannot hold unless (1) also holds.

$L_3(2)$ contains the matrix

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

which interchanges the vectors

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

but is not an involution. Thus $G \neq L_3(2)$.

$R(3)$ has order $28 \cdot 27 \cdot 2$ and degree 28. Every involution of $R(3)$ fixes four symbols. Suppose that $G = R(3)$. R contains a member interchanging two symbols of $\sum$ and $r^2 = 1$. Thus r fixes four symbols of $\sum$ which is impossible as 1 is the only member of r fixing two symbols of $\sum$. Hence $G \neq R(3)$.

Now suppose that case (4) of Aschbacher's result applies. We notice first that in each case $M(G)$ is doubly transitive on $\sum$. In each case the stabilizer $M(G)_\alpha$ of α in $M(G)$ has a characteristic subgroup, say Q_α which is regular on $\sum - \{\alpha\}$. As $M(G)$ is doubly transitive on $\sum$ we have $G = G_{\alpha\beta}M(G)$. If a is a member of G which interchanges α and β each coset of $M(G)$ in G contains a member of $aG_{\alpha\beta}$. As all the members of this set are involutions it follows that $G/M(G)$ is an elementary abelian 2-group.

We now consider the different possibilities for $M(G)$ in turn.

Suppose that $M(G) = L_2(q)$. Let x be any member of $G_{\alpha\beta}$. Then x normalises Q_α. Suppose $h \in Q - \{1\}$. From the properties of Aut $L_2(q)$ there is a member y of $PGL(2, q)_{\alpha\beta}$ with the property $h^x = h^y$. Put $z = xy^{-1}$ so that $h^z = h$. Now let w be any member of $L_2(q)_{\alpha\beta}$. As both $G_{\alpha\beta}$ and $PGL(2, q)_{\alpha\beta}$ are abelian and contain $L_2(q)_{\alpha\beta}$ we have $(h^w)^z = h^w$. $L_2(q)_{\alpha\beta}$ contains either $q - 1$ or $\frac{1}{2}(q - 1)$ members and none of these commutes with a member of Q_α. Hence z centralizes either q or $\frac{1}{2}(q + 1)$ members of Q_α. As $\frac{1}{2}(q + 1) > \frac{1}{2}q$ we find that in either case z centralizes Q_α. As z centralizes $L_2(q)_{\alpha\beta}$ it now follows that z centralizes $L_2(q)_\alpha$. $G/M(G)$ is an elementary abelian 2-group so that $z^2 \in M(G)$. Thus z^2 lies in the centre of $L_2(q)_\alpha$ and so $z^2 = 1$. Let a be a member of $L_2(q)$ which interchanges α and β. Then az also interchanges α and β so we have both $a^2 = 1$ and $(az)^2 = 1$. Thus z centralizes a. As $L_2(q)_\alpha$ is a maximal subgroup of $L_2(q)$ it now follows that z centralizes $L_2(q)$. But $z \in \text{Aut}\, L_2(q)$ so that $z = 1$. Hence

$x \in PGL(2, q)$ and so either $G = L_2(q)$ or $PGL(2, q)$. In either case we get a contradiction to the result in [3] unless $G = L_2(q)$ where $q = 2$ or 3. Both of these groups have a normal regular subgroup.

In considering the groups $U_3(q)$ we will adopt the notation of [2, p. 233 f]. If k lies in the field with q^2 members $SU(3, q^2)$ contains the matrix

$$\begin{pmatrix} \cdot & \cdot & k^{-\tau} \\ \cdot & k^{\tau-1} & \cdot \\ k & \cdot & \cdot \end{pmatrix}$$

which interchanges the subspaces $\langle w_1 \rangle$ and $\langle w_3 \rangle$. The square of this matrix is

$$\begin{pmatrix} k^{1-\tau} & \cdot & \cdot \\ \cdot & k^{2(\tau-1)} & \cdot \\ \cdot & \cdot & k^{1-\tau} \end{pmatrix}$$

and the conditions that this be a scalar matrix is $k^{3(\tau-1)} = 1$, or $k^{3(q-1)} = 1$. This is true when k is a primitive element of the field only when $q = 2$. Hence we cannot have $M(G) = U_3(q)$ except in the case $q = 2$. Then $U_3(q)$ is a Frobenius group and G would have a normal regular subgroup.

Suppose next that $M(G) = Sz(q)$. Then $M(G)_{\alpha\beta}$ has odd order and as $G/M(G)$ is an elementary abelian 2-group each coset of $M(G)_{\alpha\beta}$ in $G_{\alpha\beta}$ contains exactly one involution and they all lie in different classes of G. Let z be an involution of $G_{\alpha\beta} - M(G)_{\alpha\beta}$ and put $\Omega = \{\sigma \in \sum;\ z(\sigma) = \sigma\}$. If $a, b \in \Omega$ we can easily show that

$$C(z) = \{x \in G;\ x(a) \in \sum,\ x(b) \in \sum\}.$$

This is because all the involutions of $G_{\alpha\beta}$ lie in different classes of G. Hence $C(z)$ is doubly transitive on Ω. Now $z \in G_\alpha$ so that z normalizes Q_α and so normalizes $Z(Q_\alpha)$. As $Z(Q_\alpha)$ is a 2-group and $z^2 = 1$, $h^z = h$ for some $h \in Z(Q_\alpha) - \{1\}$. If $w \in M(G)_{\alpha\beta}$, $wz = zw$ so that $(h^w)^z = h^w$. From the properties of $Sz(q)$ it follows that z centralizes $Z(Q_\alpha)$. Now $Z(Q_\alpha)$ has order q and Q_α has order q^2. We may suppose that z centralizes mq members of Q_α where m divides q. z centralizes the $q - 1$ members of $M(G)_{\alpha\beta}$. Hence, because of the double transitivity property of $C(z)$, z centralizes $(q-1)mq(mq+1)$ members of $Sz(q)$. This number must thus be a divisor of the order of $Sz(q)$ which is $(q-1)q^2(q^2+1)$. Because m and q are powers of 2 we can deduce that $mq + 1$ divides $q^2 + 1$. From this we easily deduce that $m = q$ and so z centralizes $Sz(q)$. As $z \in \mathrm{Aut}\, Sz(q)$ we must have $z = 1$, a contradiction. Thus $G = M(G) = Sz(q)$ which contradicts the result in [3]. Hence we cannot have $M(G) = Sz(q)$.

Lastly under (4) we consider the possibility that $M(G) = R(q)$, a group of Ree type. The properties of these groups may be found in [5]. Let t be the unique involution of $R(q)_{\alpha\beta}$. As $M(G)_{\alpha\beta} \lhd G_{\alpha\beta}$, t has no other conjugate in $G_{\alpha\beta}$. Let Ω be the subset of $\sum$ fixed pointwise by t. As above we find that if $a, b \in \Omega$, then

$$C(t) = \{x \in G;\ \ x(a) \in \Omega,\ \ x(b) \in \Omega\}.$$

Hence $C(t)$ is doubly transitive on Ω. As $C(t) \cap R(q) = \{1, t\} \times K$ where K is isomorphic to $L_2(q)$ we find that Ω must have $q + 1$ members and we must have K permutation isomorphic to $L_2(q)$ as a permutation group on Ω. We write $K = L_2(q)$. Suppose now that z is a 2-element of $G_{\alpha\beta} - M(G)_{\alpha\beta}$. Then $z^2 \in M(G)_{\alpha\beta}$ os that either $z^2 = 1$ or $z^2 = t$. In either case z^2 centralizes K. Clearly z normalizes K. Using the same considerations as we applied above to the case $M(G) = L_2(q)$ we can prove that either z centralizes K or acts on $K = L_2(q)$ as an involution of $PGL(2, q)_{\alpha\beta}$. Now consider the representation of $C(t)$ as a permutation group on Ω. From the above it follows that the image of $C(t)$ under this representation is either $L_2(q)$ or $PGL(2, q)$. The image of $R \cap C(t)$ is then a doubly transitive subset of the group which occurs. This contradicts the result of [3] except when $q = 3$ and the group which occurs is $L_2(q)$. In this case we get the only group of Ree type for the parameter $q = 3$, namely the Ree group $R(3)$ of order $28 \cdot 27 \cdot 2$ and degree 28. But $R(3) \simeq P\Gamma L(2, 8) \simeq \mathrm{Aut}\, L_2(8)$. Hence $\mathrm{Aut}\, R(3) = R(3)$ so that $G = M(G) = R(3)$ and we have already shown that we cannot have $G = R(3)$.

We have now shown that conclusions (2), (3) and (4) of Aschbacher's result cannot hold unless (1) holds also. We now investigate conclusion (1) in more detail.

Assume from now on that G has a regular normal subgroup V and let σ be a fixed member of $\sum$. If H is the stabilizer of σ in G we have $G = VH$ and $V \cap H = 1$. As G is doubly transitive V is an elementary abelian group and we may take V as a vector space over a prime field F of order say p and H as a group of linear transformations over V. If $v \in V$, $h \in H$ we will denote the element vh of G from now on also by (v, h). We may identify the elements of $\sum$ with those of V in such a way that we may assume that G is doubly transitive on V and (v, h) is the mapping $V \to V$ given by $w \to v + h(w)$. We shall write $(v, h)w = v + h(w)$. Under this identification σ corresponds to 0.

Suppose $v \in V - \{0\}$. The members of G which interchange 0 and v are the elements (v, h) with $h(v) + v = 0$. Such an element of G must be an involution and the condition for this is $h^2 = 1$.

We now split our considerations into two parts depending on whether p is odd or even.

First suppose that p is odd. Let S be any sharply doubly transitive subset of G. Then S contains a member (v, h), $h^2 = 1$ which interchanges 0 and $v \neq 0$. If $h(w) = w$ for some $w \in V - \{0\}$ we have

$$(v, h)(\tfrac{1}{2}v + \alpha w) = \tfrac{1}{2}v + \alpha w$$

for each $\alpha \in F$. But 1 is the only member of S which fixes two members of V so that no such w can exist. But H is a group of linear transformations on V, $h^2 = 1$ and char $F \neq 2$. The only possibility is $h = -1$. Hence S contains all the vectors $(v, -1), v \neq 0$. Suppose $v \neq 0$. Then the set $(v, -1)^{-1}S$ is also a sharply doubly transitive subset of G and so contains every vector of the form $(w, -1)$, $w \neq 0$. Hence S contains every vector of the form $(v, -1)(w, -1) = (v - w, 1)$, $v, w \neq 0$. As v has more than two elements this is enough to ensure that $V \subseteq S$. If $g \in S$ $g^{-1}S$ is also a sharply doubly transitive subset of G so that $V \subseteq g^{-1}S$ or $gV \subseteq S$. Now consider R and put $R_\sigma = R \cap H$. We then get $R = VR_\sigma$. Finally suppose $(0, h)$ fixes 0 and v. $(v, -1)$ interchanges 0 and v so that $(v, -1)(0, h)$ does also. Hence this is an involution so that $h^2 = 1$. This proves Theorem 1 in the case that p is odd.

Now suppose that $p = 2$. If $v \neq 0$, $(v, 1)$ interchanges 0 and v. If $h(v) = v$, (v, h) also interchanges 0 and v and so is an involution. Hence $h^2 = 1$ and we deduce that the stabilizer of any two points is an elementary abelian 2-group. Now refer to the remark of [1, p. 114]. Either G is a group of semilinear transformations over a field or V has order q^2 and H is isomorphic to $L_2(q)$. Suppose that the first is true. We may take V as the additive group of the field and H is then the set of transformations of the form $x \to ax^\sigma$ where σ is a field automorphism. The transformations which fix 0 and 1 are those of the form $x \to x^\sigma$ and the condition that this be an involution is $\sigma^2 = 1$. A finite field contains at most one automorphism which is an involution, so that the stabilizer of any two points has order at most two. Suppose that the stabilizer of 0 and 1 has two members 1 and $x \to x^\tau$. Then G contains two members interchanging 0 and 1, namely $x \to x + 1$ and $x \to x^\tau + 1$. The latter is conjugate to $x \to x^\tau$ and so the only involutions of G fixing less than 2 symbols are those of V. The same is clearly true if the stabilizer of any two points has order 1. Now consider the other case when V has q^2 members and H is isomorphic to $L_2(q)$. If a is an involution of H then a fixes exactly q symbols of V and as $C(a) \cap H$ has order q, $C(a)$ has order q^2. Thus a has $q(q^2 - 1)$ conjugates. The number of conjugates in H is $q^2 - 1$ so that the number in $G - H$ is $(q - 1)(q^2 - 1)$. As G is doubly transitive each of the $q^2 - 1$ cosets of H in $G - H$ contains the same number of these involutions. This number is $q - 1$. As each such coset contains q involutions each contains exactly one member fixing less than 2 symbols of V and this is a member of V. In any case we have shown that if $p = 2$ then the only involutions of G which fix less than 2 symbols are those of V. Let S be any sharply doubly transitive subset of G. Then S contains one such involution from each coset of H in G. Hence $V \subseteq S$. As in the case that p is odd this is sufficient to establish Theorem 1.

The proof of Theorem 1 is now complete.

References

1. ASCHBACHER, M., Doubly transitive groups in which the stabilizer of two points is abelian. *J. Algebra* 18 (1971), 114–136.
2. HUPPERT, B., *Endliche Gruppen I*, Springer-Verlag, 1968.
3. LORIMER, P., A note on doubly transitive groups. *J. Austral. Math. Soc.* 6 (1966), 449–451.
4. TITS, J., Généralisations des groupes projectifs I, II, III, IV. *Acad. Roy. Belg. Bull. Cl. Sci.* (5) 35 (1949), 197–208, 224–233, 568–589, 756–773.
5. WALTER, J. H., Finite groups with abelian Sylow 2-groups of order 8. *Invent. Math.* 2 (1967), 332–376.

Received November 17, 1971

Peter Lorimer
Department of Mathematics
University of Auckland
Private Bag
Auckland
New Zealand