Marshall Hall, Jr.

Automorphisms of Steiner Triple Systems

Abstract: This paper treats the following problem in combinatorial analysis: Find an incomplete balanced block design D with parameters b, v, r, k, and $\lambda = 1$, possessing an automorphism group G which is doubly transitive on the elements of D and such that the subgroup H of G fixing all the elements of a block is transitive on the remaining elements. Also find transitive extensions of such groups G. If the block design is a finite projective plane, the plane is necessarily Desarguesian. Thus, these properties of the automorphism group may be considered as a "Desarguesian" property of the designs.

This paper considers the case in which D is a Steiner triple system. The main result is that a "Desarguesian" Steiner triple system is either 1) a projective geometry over $GF(2)$ or 2) an affine geometry over $GF(3)$. Two intermediate results are of interest: 1) A Steiner triple system has for each element an involution fixing only this element, if and only if every triangle generates an $S(9)$, a Steiner triple system with 9 elements; 2) if a Steiner triple system has for each triple an involution fixing only the elements of this triple, then every triangle generates an $S(7)$ or an $S(9)$.

1. Introduction

It is a classical result that the validity of the Theorem of Desargues in a projective plane is equivalent to the existence of a certain family of collineations [1, p. 352]. And recently Ostrom and Wagner [2] have shown that a finite projective plane is Desarguesian if it has a group of collineations doubly transitive on its points. Thus a natural generalization of the Desarguesian property to block designs is the property of having a highly transitive group of automorphisms. And conversely a family of permutation groups originally investigated by Jordan [3] leads in a very natural way to block designs. These are doubly but not triply transitive permutation groups in which a subgroup exists fixing $k \geq 3$ letters and transitive on the remaining letters. These groups and their relationship to block designs are considered in Section 2.

The Steiner triple systems are the block designs with $k = 3$ and $\lambda = 1$, i.e., systems with blocks of three elements (the elements are called points in this paper) in which every pair of distinct elements occurs together in exactly one block. Two theorems in Section 3 relate combinatorial properties of Steiner triple systems to the existence of certain automorphisms. First, if for every point of a triple system S there is an involution fixing only that point, then every triangle (three points of S not in a block) lies in a system $S(9)$ with exactly 9 points and conversely if all triangles lie in subsystems $S(9)$, then S has the corresponding family of involutions. Second, if for every triple of S there is an involution fixing exactly the points of this triple, then every triangle lies in an $S(7)$ or $S(9)$. The converse of the second theorem is false.

The final section uses the results of the previous sections to characterize Steiner triple systems which have highly transitive automorphism groups. If S has automorphisms transitive on triangles, then there are two types:

Type 1. Every triangle of S generates an $S(7)$.

Type 2. Every triangle of S generates an $S(9)$.

The systems of Type 1 are precisely the projective geometries over $GF(2)$. In Type 2 it is necessary to take the stronger hypothesis that the automorphisms are transitive on sets of 4 independent points (4 points not in an $S(9)$) to conclude that S is the

affine geometry over $GF(3)$. This stronger hypothesis is probably not necessary, but is needed for the present proof. Indeed, it is conceivable that the entire conclusion holds if we ask only that the automorphism group be doubly transitive.

Much remains to be done. The nature of the doubly transitive groups of the Steiner triple systems needs investigation. And of course analogous questions can be studied for block designs other than Steiner triple systems.

2. On a class of groups related to block designs

The following theorem is due originally to Jordan [3] and the proof may be found in Burnside [4, p. 207] or in Hall [1, p. 66]. The properties of block designs needed here may be found in Mann [5, pp. 83–129].

• *Theorem of Jordan*

Let G be a permutation group on n letters which is primitive, and let H be a transitive subgroup of G on m letters, fixing the remaining $n-m$ letters, $2 \leq m < n$. Then (1) *if H is primitive, G is $n - m + 1$ fold transitive*; (2) *in any event G is doubly transitive.*

We are here interested in the second alternative, where with $2 \leq m \leq n - 3$, G is not $n - m + 1$ fold transitive. Suppose that G is t-ply transitive, but not $t + 1$-ply transitive where $2 \leq t \leq n - m - 1$. We note that if G is $n - m$ fold transitive, it is also $n - m + 1$ fold transitive, since H fixes $n - m$ letters and is transitive on the remaining letters. Then the subgroup G^* of G fixing $t - 2$ of the letters fixed by H will be doubly but not triply transitive, and either $G = G^*$ (if $t = 2$) or G is a transitive extension of G^*. For example, the Mathieu group M_{23} quadruply transitive on 23 letters contains a subgroup H fixing 7 letters and transitive on the remaining 16 letters. A subgroup G^* of M_{23} fixing two of the fixed letters of H is doubly but not triply transitive on 21 letters and contains H. Group M_{23} is a transitive extension of G^*.

Let us call a group G a Jordan group if

1) G is doubly but not triply transitive on n letters;
2) G has a subgroup H fixing $k \geq 3$ letters and transitive on the $m = n - k$ letters which it moves

• *Theorem 2.1*

Let G be a Jordan group on n letters and suppose the subgroup H as large as possible, namely (i) *H is not contained in a subgroup H' fixing k' letters $3 \leq k' < k$ and transitive on the remaining $n - k'$ letters, and* (ii) *H contains all permutations of G fixing the k letters which H fixes. Then the sets of k letters fixed by H and its conjugates in G form the blocks of an incomplete balanced block design D with parameters $v = n$, $b = n(n-1)/k(k-1)$, $k = k$, $r = (n-1)/(k-1)$, $\lambda = 1$. The group G may be regarded as an automorphism group of D which is doubly transitive on the letters of D. The subgroup H fixes the letters of a block of D and is transitive on the remaining letters. Conversely if D is a block design with parameters v, b, r, k, and $\lambda = 1$ which has an automorphism group G doubly transitive on the letters of D in which the subgroup H fixing the letters of a block is transitive on the remaining letters, then G is a Jordan group on the v letters of D and H is the subgroup of G fixing k letters and transitive on the remaining letters.*

Proof. The proof of this theorem is not much longer than the statement. Suppose G is a Jordan group and H as large as possible. First we show that $m = n - k > n/2$. Since G is primitive there exist conjugates H_1, H_2 of H displacing some letters in common but not all. Then $H_1 \cup H_2$ is transitive on the letters it displaces. By the maximality of H, $H_1 \cup H_2$ is transitive on $n - 1$ or n letters. But $H_1 \cup H_2$ displaces at most $2m - 1$ letters. Hence $2m - 1 \geq n - 1$ and $m \geq n/2$. If $m = n/2$ and $H_1 \cup H_2$ displaces exactly $n - 1$ letters, a third conjugate H_3 will be such that either $H_1 \cup H_2$ or $H_2 \cup H_3$ is transitive on more than $n/2$ letters and on at most $3n/4$. Here $3n/4 < n - 1$ since $n \geq 6$ for all but trivial cases. Thus we must have $m > n/2$ for H with the maximal properties of the theorem. Hence any two conjugates of H, say H_1 and H_2, displaces some letters in common and $H_1 \cup H_2$ is transitive. By the maximal property of H this means that $H_1 \cup H_2$ is transitive on n or $n - 1$ letters. This is equivalent to saying that the k letters fixed by H_1 and the k letters fixed by H_2 have no letters or exactly one letter in common.

Consider the array D of the sets of k letters fixed by conjugates of H. A pair of distinct letters a_i, a_j occurs together in one of these sets at most once, since we have shown that two such sets have at most one letter in common. But since G is doubly transitive, a pair a_i, a_j will occur together in one set. If there are b conjugates of H, D has b blocks each consisting of k letters, there being n letters in all. Each unordered pair a_i, a_j occurs together exactly once in a block. This says that D is an incomplete balanced block design whose parameters v, b, r, k, λ include $v = n$, $k = k$, and $\lambda = 1$. But it is well known that the parameters satisfy $bk = vr$, $r(k-1) = \lambda(v-1)$ whence $r = (n-1)/(k-1)$, $b = n(n-1)/k(k-1)$. Clearly G permutes the conjugates of H among themselves and so G may be considered as an automorphism group of D,

being doubly transitive on the letters of D, and having a subgroup H which fixes the letters of a block and is transitive on the remaining letters. This completes the proof of the direct part of the theorem.

The converse part of the theorem is essentially obvious. Let D be a block design with parameters b, v, r, k, λ, where $k \geq 3$ and $\lambda = 1$, and let G be a group of automorphisms of D, doubly transitive on the letters of D and having a subgroup H fixing the letters of a block and transitive on the remaining letters. The group G cannot be triply transitive, for if i, j, t are letters of a block B_1 and if s is a letter not in B_1, then G does not contain a permutation mapping i, j, t onto i, j, s. Hence G is doubly but not triply transitive and contains a subgroup H fixing $k \geq 3$ letters, and transitive on the remaining letters. Thus G is a Jordan group and the converse of the theorem is proved.

In the Mathieu group M_{23} mentioned above, the group G^* is doubly but not triply transitive on 21 letters with a subgroup H transitive on 16 letters and fixing the rest. In G^* a conjugate of H fixes $k = 5$ letters and we have $n = v = 21, \lambda = 1$ for the block design D. Here for D,

$$r = (n - 1)/(k - 1) = 20/4 = 5$$

and

$$b = n(n - 1)/k(k - 1) = 21 \cdot 20/5 \cdot 4 = 21.$$

Thus D is the finite projective plane of order $k - 1 = 4$. The group G^* is the group of unimodular collineations of the plane. M_{23} is, of course, a transitive extension of G^*.

In this paper we investigate Jordan groups with $k = 3$. The corresponding design is, of course, a Steiner triple system. An automorphism α of a Steiner triple system which fixes two distinct points, say x, y, will fix the triple, say x, y, z, containing these two points and therefore will also fix the third point z of the triple. Hence the subgroup H fixing a triple is just the subgroup fixing two points. Thus if G is a group of automorphisms of a Steiner triple system S which is doubly transitive on the points of S, and if the subgroup H, fixing a triple, is transitive on the remaining points, this is equivalent to saying that G is transitive on triangles of S, meaning by a triangle an ordered set of three points not in a triple.

3. Combinatorial theorems

In this section we establish two theorems which relate the structure of a Steiner triple system to the existence of a family of involutions of certain types. We note that an involution of a Steiner system S which interchanges two points x, y necessarily fixes the third point of the triple containing them. For if α is the involution, $(x)\alpha = y$, $(y)\alpha = x$, the triple $(x, y, z)\alpha = y, x, (z)\alpha = y, x, z$ whence $z = (z)\alpha$. By a triangle of a Steiner triple system we shall mean three points not in a triple. An $S(v)$ is a Steiner triple system with exactly v points.

Theorem 3.1

Let S be a Steiner triple system in which, for every point x, there is an involution α of S which has x as its only fixed point. Then every triangle of S generates an $S(9)$. Conversely suppose that S is a Steiner triple system in which triangle generates an $S(9)$. Then for every point x of S there is an involution α of S which has x as its only fixed point.

Proof. Suppose S has a family of involutions such that for every point x of S there is an involution α which has x as its only fixed point. By the remark above, if r is a point and $(r)\alpha = s$, $(s)\alpha = r$, x, r, s is a triple of S, and conversely if x, r, s is a triple, then, since x, r, $(r)\alpha$ is a triple, $(r)\alpha = s$ and $(s)\alpha = r$. Let 1, 2, 4 be a triangle of S. Then the following triples are determined:

1, 2, 3 2, 4, 6

1, 4, 5

1, 6, 7. (3.1)

Here we have involutions a_1, a_2

$$a_1 = (1)\ (2, 3)\ (4, 5)\ (6, 7)$$

$$a_2 = (2)\ (1, 3)\ (4, 6). \quad (3.2)$$

Applying a_1 to 2, 4, 6 we have $(2, 4, 6)a_1 = 3, 5, 7$, a new triple. Thus 2, 5, 7 is not a triple, and a_2 does not interchange 5 and 7 but must interchange 5 with a further point 8, there being a triple 2, 5, 8, and let 9 be the third point of the triple 1, 8, 9. We now have triples

1, 2, 3 2, 4, 6 3, 5, 7

1, 4, 5 2, 5, 8

1, 6, 7

1, 8, 9 (3.3)

and also involutions

$$a_1 = (1)\ (2, 3)\ (4, 5)\ (6, 7)\ (8, 9)$$

$$a_2 = (2)\ (1, 3)\ (4, 6)\ (5, 8)$$

$$a_3 = (3)\ (1, 2)\ (5, 7)$$

$$a_4 = (4)\ (1, 5)\ (2, 6)$$

$a_5 = (5)\ (1, 4)\ (2, 8)\ (3, 7).$ (3.4)

We now find further triples by applying the involutions

$(2, 5, 8)a_1 = 3, 4, 9$

$(1, 2, 3)a_5 = 4, 8, 7$

$(4, 8, 7)a_1 = 5, 6, 9.$ (3.5)

This adds to our information, giving triples

1, 2, 3 2, 4, 6 3, 4, 9 4, 7, 8 5, 6, 9

1, 4, 5 2, 5, 8 3, 5, 7

1, 6, 7

1, 8, 9 (3.6)

and involutions

$a_1 = (1)\ (2, 3)\ (4, 5)\ (6, 7)\ (8, 9)$

$a_2 = (2)\ (1, 3)\ (4, 6)\ (5, 8)$

$a_3 = (3)\ (1, 2)\ (4, 9)\ (5, 7)$

$a_4 = (4)\ (1, 5)\ (2, 6)\ (3, 9)\ (7, 8)$

$a_5 = (5)\ (1, 4)\ (2, 8)\ (3, 7)\ (6, 9).$ (3.7)

We now find

$(1, 4, 5)a_3 = 2, 9, 7$

$(2, 9, 7)a_1 = 3, 8, 6.$ (3.8)

This yields the triples of a complete $S(9)$

1, 2, 3 2, 4, 6 3, 4, 9 4, 7, 8 5, 6, 9

1, 4, 5 2, 5, 8 3, 5, 7

1, 6, 7 2, 7, 9 3, 6, 8

1, 8, 9 (3.9)

and the nine involutions

$a_1 = (1)\ (2, 3)\ (4, 5)\ (6, 7)\ (8, 9)$

$a_2 = (2)\ (1, 3)\ (4, 6)\ (5, 8)\ (7, 9)$

$a_3 = (3)\ (1, 2)\ (4, 9)\ (5, 7)\ (6, 8)$

$a_4 = (4)\ (1, 5)\ (2, 6)\ (3, 9)\ (7, 8)$

$a_5 = (5)\ (1, 4)\ (2, 8)\ (3, 7)\ (6, 9)$

$a_6 = (6)\ (1, 7)\ (2, 4)\ (3, 8)\ (5, 9)$

$a_7 = (7)\ (1, 6)\ (2, 9)\ (3, 5)\ (4, 8)$

$a_8 = (8)\ (1, 9)\ (2, 5)\ (3, 6)\ (4, 7)$

$a_9 = (9)\ (1, 8)\ (2, 7)\ (3, 4)\ (5, 6).$ (3.10)

This completes the proof of the first part of the theorem, since we have shown that given the involutions the triangle 1, 2, 4 generates the $S(9)$ of (3.9).

For the converse part of the theorem suppose that S is a Steiner triple system in which every triangle generates an $S(9)$. Let 1 be a point of S and let a_1 be the permutation which fixes 1 and interchanges x and y if 1, x, y, is a triple of S. We must prove that a_1 is an automorphism of S, namely, that a_1 maps triples of S onto triples. This is trivial for every triple through 1. Hence consider a triple, say 2, 4, 6 not through 1. Let 3, 5, 7 be the third points of the triples containing 1, 2; 1, 4; 1, 6 respectively. Thus we have

1, 2, 3 2, 4, 6

1, 4, 5

1, 6, 7. (3.11)

By hypothesis the triangle 1, 2, 4 generates an $S(9)$ whose points are 1, $\cdots$, 7 as above and two further points 8, 9. Thus 1, 8, 9 is a triple. If 2, 5, 7 were a triple then we would have to have 2, 8, 9 as a triple and 8, 9 would appear in two triples, a conflict.

Hence 2, 5 is in a triple with one of 8, 9, say 8. The remaining triple with 2 must be 2, 7, 9. This gives triples

1, 2, 3 2, 4, 6

1, 4, 5 2, 5, 8

1, 6, 7 2, 7, 9

1, 8, 9. (3.12)

We easily find that the only possible way to complete (3.12) to an $S(9)$ is to add the further triples which appear in (3.9). Thus with $a_1 = (1)\ (2, 3)\ (4, 5)\ (6, 7)\ (8, 9)$ we find $(2, 4, 6)a_1 = 3, 5, 7$ and 3, 5, 7 is indeed a triple. This proves that a_1 is an automorphism of S and the proof of our theorem is complete.

There is a second theorem much like the first, though it does not contain the converse (which is indeed false). [6]

• *Theorem 3.2*

Let S be a Steiner triple system and suppose that for each triple of S there is an involution whose fixed points are precisely the three points of the triple. Then every triangle of S generates an $S(7)$ or an $S(9)$.

Proof. Let 1, 2, 4 be a triangle and 1, 2, 3 the triple containing 1, 2. Let $a = (1)\ (2)\ (3)\ (4,5)$ be an involution fixing the points 1, 2, 3 and no others. Then 4, 5, x is a triple with $x = 1$, 2, or 3 and renumbering, suppose $x = 1$. This renumbering does not alter what we need to prove since 1, 2, 4; 1,

3, 4; and 2, 3, 4 all generate the same Steiner subsystem. Thus we have the triple 1, 4, 5. The third points u, v of the triples 2, 4, u and 2, 5, v will be new points which we shall number $u = 6$, $v = 7$ giving triples 2, 4, 6 and 2, 5, 7. Here $(2, 4, 6)a = 2, 5, t$ whence $t = 7$ and $a = (1)\ (2)\ (3)\ (4, 5)\ (6, 7)$. At this stage we have

1, 2, 3 2, 4, 6

1, 4, 5 2, 5, 7

$$a = (1)\ (2)\ (3)\ (4, 5)\ (6, 7). \tag{3.13}$$

The triple 6, 7, y is fixed by a and so $y = 1$, 2, or 3. The triple 2, 6, 7 is impossible and so there are two cases: Case 1, $y = 1$, Case 2, $y = 3$. We shall show that Case 1 is possible only when the triangle 1, 2, 4 generates an $S(7)$, while Case 2 is possible only when 1, 2, 4 generates an $S(9)$. The cases are shown in Fig. 1.

Case 1.

1, 2, 3 2, 4, 6

1, 4, 5 2, 5, 7

1, 6, 7.

$$a = (1)\ (2)\ (3)\ (4, 5)\ (6, 7) \tag{3,14}$$

Here in a triple 3, 4, z we find that $z \neq 1, 2, 3, 4, 5, 6$. Hence we have two possibilities: Case 1.1 $z = 7$, Case 1.2 $z = 8$ a new point. In Case 1.1 we have $(3, 4, 7)a = 3, 5, 6$ giving the $S(7)$

1, 2, 3 2, 4, 6 3, 4, 7

1, 4, 5 2, 5, 7 3, 5, 6

1, 6, 7. (3.15)

We shall show that Case 1.2 is in fact impossible. In Case 1.2 we have 3, 4, 8 as a triple and if $a = (8, 9)$ then $(3, 4, 8)a = 3, 5, 9$. Hence in Case 1.2 we have:

Case 1.2

1, 2, 3 2, 4, 6 3, 4, 8

1, 4, 5 2, 5, 7 3, 5, 9

1, 6, 7

$$a = (1)\ (2, 3)\ (4, 5)\ (6, 7)\ (8, 9). \tag{3.16}$$

Let b be an involution fixing exactly (1) (4) (5). Then if $b = (1)\ (4)\ (5)\ (2, x)$, either 1, 2, x; 4, 2, x; or 5, 2, x is a triple, whence $x = 3$, 6, or 7. We subdivide into cases:

Case 1.2.1 $b = (1)\ (4)\ (5)\ (2, 3)$,

Case 1.2.2 $b = (1)\ (4)\ (5)\ (2, 6)$,

Case 1.2.3 $b = (1)\ (4)\ (5)\ (2, 7)$.

In Case 1.2.1, $(2, 4, 6)b = (3, 4, t) = (3, 4, 8)$ and $b = (6, 8)$. Also $(2, 5, 7)b = (3, 5, t) = (3, 5, 9)$ and $b = (7, 9)$. Thus $b = (1)\ (4)\ (5)\ (2, 3)\ (6, 8)\ (7, 9)$ and $(1, 6, 7)b = 1, 8, 9$ is a triple.

From the transpositions (6, 8) and (7, 9) of b we must have one of the triples 1, 6, 8; 4, 6, 8; or 5, 6, 8; and also one of 1, 7, 9; 4, 7, 9; 5, 7, 9. Of these only 5, 6, 8 and 4, 7, 9 are consistent with (3.16), and so we have

Case 1.2.1

1, 2, 3 2, 4, 6 3, 4, 8 4, 7, 9

1, 4, 5 2, 5, 7 3, 5, 9 5, 6, 8

1, 6, 7

1, 8, 9

$$a = (1)\ (2)\ (3)\ (4, 5)\ (6, 7)\ (8, 9),$$

$$b = (1)\ (4)\ (5)\ (2, 3)\ (6, 8)\ (7, 9). \tag{3.17}$$

Here for the involution $c = (2)\ (4)\ (6)\ (1, x)$ we have three possibilities

Case 1.2.1.1 $c = (2)\ (4)\ (6)\ (1, 3)$,

Case 1.2.1.2 $c = (2)\ (4)\ (6)\ (1, 5)$,

Case 1.2.1.3 $c = (2)\ (4)\ (6)\ (1, 7)$.

All three lead to conflicts.

In Case 1.2.1.1, $(1, 4, 5)c = 3, 4, y = 3, 4, 8$ and $c = (5, 8)$. Then $(1, 8, 9)c = 3, 5, t = 3, 5, 9$ whence c fixes a fourth letter (9), a conflict. In Case 1.2.1.2, $(1, 2, 3)c = 5, 2, y = 5, 2, 7$ and $c = (3, 7)$. But then $(1, 6, 7)c = 5, 6, 3$ conflicting with 3, 5, 9 in 3.17). In Case 1.2.1.3, $(1, 2, 3)c = 7, 2, x = 7, 2, 5$ and $c = (3, 5)$, whence $(1, 4, 5)c = 7, 4, 3$ conflicting with 3, 4, 8. Thus Case 1.2.1 leads to conflicts in every case.

In Case 1.2.2, $b = (1)\ (4)\ (5)\ (2, 6)$ and, referring to (3.16), $(1, 2, 3)b = 1, 6, x = 1, 6, 7$ whence $b = (3, 7)$. But then in the triple 3, 7, y; y is a fixed point of b, $y = 1$, 4, or 5. But no one of the triples 1, 3, 7; 3, 7, 4; or 3, 7, 5 is consistent with (3.16). Hence Case 1.2.2 leads to conflicts.

In Case 1.2.3, $b = (1)\ (4)\ (5)\ (2, 7)$ and $(1, 2, 3)b = 1, 7, x = 1, 7, 6$, whence $b = (3, 6)$. Then in the triple 3, 6, y; y is one of 1, 4, or 5. Again the triples 3, 6, 1; 3, 6, 4; and 3, 6, 5 all conflict with (3.16). Thus Case 1.2.3 also leads to conflicts and so all alternatives under Case 1.2 lead to conflicts. Thus in Case 1, the only possible consistent alternative is the Steiner system $S(7)$ arising in Case 1.1.

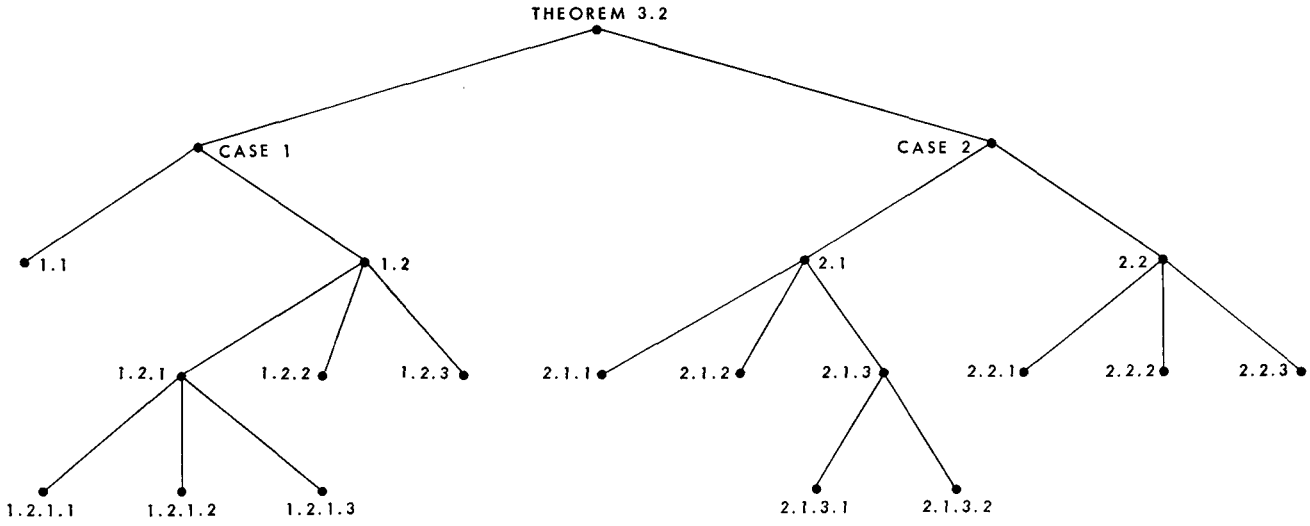

Figure 1 **Case diagram for Theorem 3.2.**

Case 2. Triple 3, 6, 7

1, 2, 3 2, 4, 6 3, 6, 7

1, 4, 5 2, 5, 7

$a = (1)\ (2)\ (3)\ (4, 5)\ (6, 7).$ (3.18)

Here we must have further triples 1, 6, 8 and if $a = (8, 9)$ then also $(1, 6, 8)a = 1, 7, 9$. Thus our basis for Case 2 is the array

Case 2

1, 2, 3 2, 4, 6 3, 6, 7

1, 4, 5 2, 5, 7

1, 6, 8

1, 7, 9

$a = (1)\ (2)\ (3)\ (4, 5)\ (6, 7)\ (8, 9).$ (3.19)

Here in the triple x, 8, 9 we must have $x = 1$, 2, or 3. 1, 8, 9 is inconsistent. We have two cases. Case 2.1 Triple 2, 8, 9. Case 2.2 Triple 3, 8, 9. We shall show that Case 2.1 leads to an $S(9)$ and that Case 2.2 leads to conflicts.

Case 2.1

1, 2, 3 2, 4, 6 3, 6, 7

1, 4, 5 2, 5, 7

1, 6, 8 2, 8, 9

1, 7, 9

$a = (1)\ (2)\ (3)\ (4, 5)\ (6, 7)\ (8, 9).$ (3.20)

This we must subdivide into cases according to the value of x in $b = (1)\ (6)\ (8)\ (2, x)$, since the pair 2, x is in a triple with one of 1, 6, or 8.

Case 2.1.1 $b = (1)\ (6)\ (8)\ (2, 3)$,

Case 2.1.2 $b = (1)\ (6)\ (8)\ (2, 4)$,

Case 2.1.3 $b = (1)\ (6)\ (8)\ (2, 9)$.

In Case 2.1.1, $b = (1)\ (6)\ (8)\ (2, 3)$

$(2, 6, 4)b = (3, 6, y) = 3, 6, 7$
and $b = (4, 7)$.

In the triple 4, 7, z; $z = 1$, 6, or 8, of which only $z = 8$ is consistent with (3.20). Hence 4, 7, 8 is a triple and also $(4, 7, 8)a = 5, 6, 9$. Here $b = (1)\ (6)\ (8)\ (2, 3)\ (4, 7)\ (9, t)$ with 9, t in a triple with 1, 6, or 8. Thus $t = 7$, 5, or 2 of which only $t = 5$ is possible. Then $(2, 5, 7)b = 3, 4, 9$ and $(2, 8, 9)b = 3, 8, 5$ yielding the complete $S(9)$.

1, 2, 3 2, 4, 6 3, 6, 7 4, 7, 8 5, 6, 9

1, 4, 5 2, 5, 7 3, 4, 9

1, 6, 8 2, 8, 9 3, 5, 8

1, 7, 9

$a = (1)\ (2)\ (3)\ (4, 5)\ (6, 7)\ (8, 9),$

$b = (1)\ (6)\ (8)\ (2, 3)\ (4, 7)\ (5, 9).$ (3.21)

Case 2.1.2. $b = (1)\ (6)\ (8)\ (2, 4)$.

Here $(1, 2, 3)b = 1, 4$, $x = 1, 4, 5$ and $b = (3, 5)$ and in the triple 3, 5, y of the values $y = 1$, 6, 8 only $y = 8$ is consistent with (3.20). Hence we have the triple 3, 5, 8 and also $(3, 5, 8)a = 3, 4, 9$. At this stage we have

Case 2.1.2

1, 2, 3 2, 4, 6 3, 6, 7

1, 4, 5 2, 5, 7 3, 5, 8

1, 6, 8 2, 8, 9 3, 4, 9

1, 7, 9

$a = (1)\,(2)\,(3)\,(4, 5)\,(6, 7)\,(8, 9),$

$b = (1)\,(6)\,(8)\,(2, 4)\,(3, 5).$ (3.22)

Here $(2, 5, 7)b = (4, 3, y) = 4, 3, 9$ whence $b = (7, 9)$. Then $(2, 8, 9)b = 4, 8, 7$ and $(4, 8, 7)a = 5, 6, 9$. This completes (3.22) to an $S(9)$ and indeed the $S(9)$ identical with that of (3.21).

Case 2.1.3 $b = (1)\,(6)\,(8)\,(2, 9)$

Here $(1, 2, 3)b = (1, 9, x) = (1, 9, 7)$ and $b = (3, 7)$, $b = (1)\,(6)\,(8)\,(2, 9)\,(3, 7)$. In this case consider an involution $c = (2)\,(8)\,(9)\,(1, y)$. Here $y = 3$, 6, or 7. If $c_1 = (2)\,(8)\,(9)\,(1, 3)$ then $bc_1b = c_2 = (2)\,(8)\,(9)\,(1, 7)$ and the two cases $y = 3$ and $y = 7$ go together. Thus we need subdivide into only two cases. Case 2.1.3.1, $c = (2)\,(8)\,(9)\,(1, 6)$ and Case 2.1.3.2, $c_1 = (2)\,(8)\,(9)\,(1, 3)$ and $c_2 = (2)\,(8)\,(9)\,(1, 7)$.

Case 2.1.3.1

1, 2, 3 2, 4, 6 3, 6, 7

1, 4, 5 2, 5, 7

1, 6, 8 2, 8, 9

1, 7, 9

$a = (1)\,(2)\,(3)\,(4, 5)\,(6, 7)\,(8, 9),$

$b = (1)\,(6)\,(8)\,(2, 9)\,(3, 7),$

$c = (2)\,(8)\,(9)\,(1, 6).$ (3.23)

Here $(1, 2, 3)c = (6, 2, x) = (6, 2, 4)$ and $c = (3, 4)$. Also $(3, 6, 7)c = 4, 1, y = 4, 1, 5$ and $c = (5, 7)$. Thus $c = (2)\,(8)\,(9)\,(1, 6)\,(3, 4)\,(5, 7)$, $(1, 7, 9)c = 6, 5, 9$ and $(5, 6, 9)a = 4, 7, 8$. $(4, 7, 8)c = 3, 5, 8$, and $(3, 5, 8)a = 3, 4, 9$. These triples complete (3.23) to the same $S(9)$ as (3.21).

As our final case under 2.1 consider Case 2.1.3.2 with $c_1 = (2)\,(8)\,(9)\,(1, 3)$ and also $c_2 = (2)\,(8)\,(9)\,(1, 7)$.

Case 2.1.3.2

1, 2, 3 2, 4, 6 3, 6, 7

1, 4, 5 2, 5, 7

1, 6, 8 2, 8, 9

1, 7, 9 (3.24)

$a = (1)\,(2)\,(3)\,(4, 5)\,(6, 7)\,(8, 9),$

$b = (1)\,(6)\,(8)\,(2, 9)\,(3, 7),$

$c_1 = (2)\,(8)\,(9)\,(1, 3),$

$bc_1b = c_2 = (2)\,(8)\,(9)\,(1, 7).$

Here

$(1, 2, 3)c_2 = 7, 2, x = 7, 2, 5$ and $c_2 = (3, 5)$,

$(3, 6, 7)c_2 = 5, y, 1 = 5, 4, 1$ and $c_2 = (4, 6)$.

Thus

$c_2 = (2)\,(8)\,(9)\,(1, 7)\,(3, 5)\,(4, 6),$

$(1, 6, 8)c_2 = 7, 4, 8$ and $(7, 4, 8)a = 6, 5, 9,$

$(5, 6, 9)c_2 = 3, 4, 9$ and $(3, 4, 9)a = 3, 5, 8.$

This completes (3.24) to the same $S(9)$ as (3.21). We note that all subcases of Case 2.1 lead to the same $S(9)$.

We now consider Case 2.2.

Case 2.2

1, 2, 3 2, 4, 6 3, 6, 7

1, 4, 5 2, 5, 7 3, 8, 9

1, 6, 8

1, 7, 9

$a = (1)\,(2)\,(3)\,(4, 5)\,(6, 7)\,(8, 9).$ (3.25)

We shall show that this always leads to a conflict. We consider the involution $b = (3)\,(6)\,(7)\,(1, x)$, and this divides into subcases

Case 2.2.1 $b = (3)\,(6)\,(7)\,(1, 2)$

Case 2.2.2 $b = (3)\,(6)\,(7)\,(1, 8)$

Case 2.2.3 $b = (3)\,(6)\,(7)\,(1, 9).$

First we treat Case 2.2.1. Here

$(1, 6, 8)b = 2, 6, y = 2, 6, 4$ and $b = (4, 8)$.

Here in the triple 4, 8, z; $z = 3$, 6, or 7 of which only $z = 7$ is consistent with (3.25), and 4, 7, 8 is a triple. Then $(4, 7, 8)a = 5, 6, 9$. Also $(1, 7, 9)b = 2, 7, t = 2, 7, 5$ and $b = (5, 9)$. But then $(3, 8, 9)b = 3, 4, 5$, a conflict. This eliminates Case 2.2.1.

Case 2.2.2 $b = (3)\,(6)\,(7)\,(1, 8).$

Here $(1, 2, 3)b = 8, x, 3 = 8, 9, 3$ and $b = (2, 9)$. But then in the triple 2, 9, y we have $y = 3$, 6, or 7. All three of these conflict with (2.25). Thus Case 2.2.2 leads to a conflict.

Case 2.2.3 $b = (3)\,(6)\,(7)\,(1, 9).$

Here $(1, 2, 3)b = 9$, $x, 3 = 9, 8, 3$ and $b = (2, 8)$. But then in the triple 2, 8, y we have $y = 3, 6$, or 7. All three of these conflict with (3.25). Thus all subcases of Case 2.2 lead to conflicts.

This completes the proof of Theorem 3.2 The only consistent subcase of Case 1 leads to an $S(7)$. All consistent subcases of Case 2 lead to the same $S(9)$.

4. Steiner triple systems with a Jordan group of automorphisms

We investigate here the structure of Steiner triple systems with a Jordan group of automorphisms. Our first theorem will require less, namely that the Steiner triple system S possess a group of automorphisms doubly transitive on the points of S.

• *Theorem 4.1*

Suppose a Steiner triple system S with more than 3 points has a group of automorphisms G which is doubly transitive on the points of S. Then S possesses a subsystem which is an $S(7)$ or an $S(9)$.

Proof. Since G is doubly transitive it is of even order. Since N, the number of points of S is odd, G is of order $N(N-1)m$, m being the order of a subgroup of G fixing two points. Then $N-1$ is even and $P(2)$, a Sylow 2-subgroup of G, will not be of an order dividing m. Thus $P(2)$ fixes exactly one point and displaces the rest. If m is odd, then every element of $P(2)$ except the identity, fixes exactly one point, and in particular there is an involution with exactly one fixed point. By transitibity of G there is for each point of S an involution fixing exactly this point. We may now apply Theorem 3.1 and conclude that every triangle of S generates and $S(9)$, and our theorem is proved.

Let us now suppose that m is even. Then a subgroup H fixing two points a_i, a_j (and hence the three points a_i, a_j, a_k of a triple) is of even order and has a Sylow 2-subgroup $Q(2)$. It is known [1, p. 68] that $N_G(Q(2))$ is doubly transitive on the points fixed by $Q(2)$. If x, y are two points fixed by $Q(2)$ then $Q(2)$ must also fix the third point z of the triple x, y, z containing x and y. Hence if $Q(2)$ fixes more than the three points a_i, a_j, a_k, then $Q(2)$ fixes a proper Steiner system S^* containing fewer points than S, and $N_G[Q(2)]$ restricted to S^* is a doubly transitive automorphism group of S^*. By induction on the number of points we may assume the theorem true for S^*, which therefore contains an $S(7)$ or an $S(9)$.

There remains to be considered the case in which $Q(2)$ fixes exactly the three points a_i, a_j, a_k fixed by H. Then, since G is doubly transitive, there is a conjugate of $Q(2)$ which has as its fixed points the three points of any specified triple of S. Now consider the family F of all 2-subgroups of G, including the identity as a 2-subgroup. Let U be a 2-subgroup of G fixing more than three points such that any larger 2-subgroup fixes at most 3 points. Here the identity fixes more than three points and so such a 2-subgroup must exist. The third point of a triple containing two points fixed by U must also be a fixed point of U and so the fixed points of U form a proper Steiner system S^* (we may have $S^* = S$ if $U = 1$). Let x, y, z be any triple of S^*. Then U is contained in a Sylow 2-subgroup $Q^*(2)$ of the subgroup H^* fixing x, y, z and $Q^*(2)$ is conjugate to $Q(2)$. $Q^*(2)$ fixes precisely the three points x, y, z. Let $U \subset V \subseteq Q^*(2)$ where $[V : U] = 2$. By the choice of U, V fixes at most three points, whence V fixes exactly the three points x, y, z. If $V = U + Ut$, then $U \lhd V$ and $t^2 \in U$ whence t^2 fixes the points of S^*. A point of S^* fixed by t is fixed by all of V, whence t fixes exactly the three points x, y, z. Thus t restricted to S^* is an involution fixing exactly the three points x, y, z. But we chose x, y, z as an arbitrary triple of S^*. Hence for every triple of S^* there is an involution of S^* fixing exactly the three points of the triple. Hence Theorem 3.2 applies to S^* and so S^*, and therefore S, contains an $S(7)$ or an $S(9)$. This completes the proof of Theorem 4.1.

We can now proceed to our main theorem.

• *Theorem 4.2*

The following two properties of a permutation group G are equivalent: 1) *G is a Jordan group with a subgroup H fixing three letters and transitive on the remaining letters;* 2) *G is an automorphism group of a Steiner triple system S, and G permutes the triangles of S transitively. There are two main types for S: Type 1: Every triangle of S generates an $S(7)$; Type 2: Every triangle of S generates an $S(9)$. A Steiner triple system of Type 1 is a projective geometry over $GF(2)$. If in Type 2 we further assume that G is transitive on independent sets of four points (i.e., four points not in an $S(9)$), then S is an affine geometry over $GF(3)$.*

Proof. By Theorem 2.1 a Jordan group G with a subgroup H fixing three letters and transitive on the rest may be regarded as an automorphism group of an incomplete balanced block design with $k = 3$, $\lambda = 1$. These designs are the Steiner triple systems S. Then G is doubly transitive and so a permutation fixing two points of S will fix the third point of the triple containing them, and the group of such permutations will be transitive on all others.

Hence G will be transitive on the triangles of S. Conversely a group G of automorphisms of S transitive on the triangles of S is a Jordan group with $k = 3$. This proves the equivalence of the two properties of the group G as stated in the theorem.

By Theorem 4.1, S contains an $S(7)$ or an $S(9)$. Since G is transitive on triangles there will be two types for S:

Type 1. Every triangle of S generates an $S(7)$.

Type 2. Every triangle of S generates an $S(9)$.

This information is sufficient to determine the Type 1 Steiner triple systems completely, but not those of Type 2.

The well known axioms for projective geometry are the following:

PG.1 There is one and only one line joining two distinct points.

PG.2 If A, B, C are three points not on a line, and if $D \neq C$ is a point on AC, and if $E \neq C$ is a point on BC, then there exists a point F on DE and also on AB.

PG.3 Every line contains at least three points.

Taking the blocks of a Steiner triple system as lines, the axioms PG.1 and PG.3 are always satisfied. If every triangle of a Steiner system generates an $S(7)$ then we readily verify that PG.2 is also satisfied. Thus a Steiner system of Type 1 is a projective geometry over $GF(2)$, since an $S(7)$ is a projective plane over $GF(2)$ and by classical procedures the plane coordinates may be extended to the entire projective space. This settles the statements of the theorem about Steiner systems of Type 1.

The treatment of systems of Type 2 is far more difficult. An $S(9)$ is an affine plane over $GF(3)$, but it is not true that a Steiner triple system in which every triangle generates an $S(9)$ is necessarily an affine geometry over $GF(3)$.

We may use the converse part of Theorem 3.1 to describe Steiner triple systems in which every triangle generates an $S(9)$:

• *Lemma 4.1*

Let S be a Steiner triple system in which every triangle generates an $S(9)$. For each point i of S let a_i be the involutory automorphism of S which fixes i and interchanges j and k if i, j, k is a triple. For each triple r, s, t we have $a_r a_s a_r = a_t$, $(a_r a_s)^3 = 1$ and corresponding relations obtained by permuting r, s, t. The group K generated by the a_i's is transitive. The element a_i permutes with every automorphism fixing i. Conversely let K be a group containing an element x of order 2, and suppose that for every $u \in K$, $(xu^{-1}xu)^3 = 1$. The representation of K as a permutation group on the cosets of $C = C(x)$, the centralizer of x represents a conjugate of x, say $u^{-1}xu$ by a permutation a_i fixing exactly one letter i. For every i and every transposition (j, k) of a_i let i, j, k be a triple of a system S. Then S is a Steiner triple system in which every triangle generates an $S(9)$.

Proof of Lemma. Let us first suppose that S is a Steiner triple system in which every triangle generates an $S(9)$. Then by Theorem 3.1 for each point i of S there is an involutory automorphism a_i of S, $a_i = (i) \cdots (j, k) \cdots$ which fixes only the point i and interchanges j and k if and only if i, j, k is a triple of S. We note that a_i is the unique involution of S fixing only the point i, since an involution interchanging x and y must fix the third point z of the triple x, y, z containing x and y. Hence if r, s, t is a triple of S then $a_r = (r)\ (s, t) \cdots$, $a_s = (s)\ (r, t) \cdots$, and $a_t = (t)\ (r, s) \cdots$, are the corresponding involutions fixing only one letter. But then $a_s a_r a_s = a_t$, and similarly $a_r a_s a_r = a_t$ But then $(a_r a_s)^3 = (a_r a_s a_r)(a_s a_r a_s) = a_t^2 = 1$. And of course similar relations hold if r, s, t are permuted. Since for any pair s, t there is a triple r, s, t and $a_r = (r)(s, t) \cdots$ it follows that $k = \{a_i\}$ is transitive. And since we have observed that a_i is the unique involution fixing the point i and no other, it follows that a_i is in the center of the subgroup fixing i. This completes the direct part of the lemma.

Conversely let K be a group containing an element x, with $x^2 = 1$ and suppose that for $u \in K$ we have $(xu^{-1}xu)^3 = 1$. Let $C = C(x)$ be the centralizer of x and let us represent K as a permutation group on the left cosets of C.

$$K = C + Cy_2 + \cdots + Cy_n. \tag{4.1}$$

Here the representation of x is the permutation $a_1 = (C) \cdots (Cy_i, Cy_j) \cdots$ where $Cy_i x = Cy_j$. The permutation a_1 fixes C, but no other coset. For if $Cyx = Cy$, then $yxy^{-1} = h \in C$, whence $xyxy^{-1} = yxy^{-1}x$. But we have $1 = (xyxy^{-1})^3 = x^3(yxy^{-1})^3 = x^3yx^3y^{-1} = xyxy^{-1}$, whence $yxy^{-1} = x$ and so $y \in C$ and hence $Cy = C$. It follows that a_1 and its n conjugates $a_1, \cdots, a_n$ are involutions where a_i fixes the letter i and no other, and a_i is in the center of the subgroup fixing i. With a_1 the permutation representing x and any conjugate a_i representing $u^{-1}xu$, from $(xu^{-1}xu)^3 = 1$ we conclude that $(a_1 a_i)^3 = 1$. By taking conjugates of this relation we conclude more generally that for any a_j, a_k we have $(a_j a_k)^3 = 1$. If $a_i = (i) \cdots (j, k) \cdots$, then $a_i a_j a_i$ is the conjugate of a_1 fixing k and so $a_i a_j a_i = a_k$, and conversely this relation implies

that $a_i = (i) \cdots (j, k) \cdots$. But as $(a_i a_j)^3 = 1$ we have $a_k = a_i a_j a_i = a_j a_i a_j$ whence $a_j = (j) \cdots (i, k)$, and since also $a_j = a_r a_k a_r$ and $a_i a_k a_i = a_k a_i a_i$ we have $a_k = (k) \cdots (i, j) \cdots$. This shows that if we take the letters $1, \cdots, n$ as points of a system S and select triples of points taking i, j, k as a triple if $a_i = (i) \cdots (j, k) \cdots$ then we obtain the same triple from $a_j = (j) \cdots (i, k) \cdots$ and from $a_k = (k) \cdots (i, j) \cdots$. Thus a selected triple is determined uniquely by any two of its points. Furthermore, any pair i, j does occur in one triple, namely, i, j, k if $a_i = (i) \cdots (j, k) \cdots$, since a_i displaces every letter except i. Thus the system S of triples is a Steiner triple system, since every pair of points occurs in a unique triple. And since $a_i a_1 a_i, a_i a_2 a_i, \cdots, a_i a_n a_i$ are the same as $a_1, \cdots, a_n$ in some order, it follows that a_i is an automorphism of S. Hence Theorem 3.1 is applicable to S and so every triangle of S generates an $S(9)$. This completes the proof of Lemma 4.1.

Lemma 4.1 shows that the construction of Steiner triple systems in which every triangle generates an $S(9)$ is precisely equivalent to the construction of groups K generated by a set of elements a_i of order 2 in which $(a_i a_j)^3 = 1$.

In general K is generated by r involutions $\{a_i\}$. The subgroup K_1 of K generated by products $a_i a_j$ will be of index 2, and since $a_i a_j = a_i a_1 a_1 a_j = (a_1 a_i)^{-1}(a_1 a_j)$ it follows that K_1 is generated by the elements $a_1 a_i$, $i \neq 1$. Thus $K = K_1 + K_1 a_1$, with $[K : K_1] = 2$. Indeed the homomorphism $a_i \to a_1$, $i = 1 \cdots r$ of K has K_1 as its kernel. We shall consider the cases $r = 2, 3, 4$.

If $r = 2$ and K is generated by a_1, a_2 then K_1 is cyclic of order 3 generated by $a = a_1 a_2$ and K is of the order 6. Here put $a_3 = a_1 a_2 a_1 = a_2 a_1 a_2$. Here K corresponds somewhat trivially to the Steiner system consisting of a single triple 1, 2, 3.

If $r = 3$, let K be generated by a_1, a_2, a_4 where $a_3 = a_1 a_2 a_1 = a_2 a_1 a_2$. If we write $a = a_1 a_2$, $b = a_1 a_4$, and $x = a_1$ then $a^3 = 1$, $b^3 = 1$, $xax = a_1(a_1 a_2)\, a_1 = a_2 a_1 = a^{-1}$, and similarly $xbx = b^{-1}$. In the relation $(xu^{-1}xu)^3 = 1$ let us take $u = a^{-1}b^{-1}$, and so $(xbaxa^{-1}b^{-1})^3 = 1$ or $(b^{-1}a^{-1}a^{-1}b^{-1})^3 = 1$ or $(b^{-1}ab^{-1})^3 = 1$ or $(ab^{-2})^3 = 1$ or $(ab)^3 = 1$. Similarly using $u = a^{-1}b$ we find $(ba^{-1}a^{-1}b)^3 = 1$ whence $(ab^{-1})^3 = 1$. These relations show that $K_1 = \{a, b\}$ is the group of exponent 3 with two generators and K_1 is of order 27. The corresponding Steiner triple system is $S(9)$ since $x(a, b)x = (a^{-1}, b^{-1}) = (a, b)$ and the commutator (a, b) is in C, the centralizer of x, and so $[K : C] = 9$, the number of conjugates of $a_1 = x$. The following well known relations hold in K_1 as may easily be verified.

$$(a, b)^3 = 1, \qquad (a^{-1}, b) = (a, b^{-1}) = (a, b)^{-1}$$
$$(a^{-1}, b^{-1}) = (a, b),$$
$$(a, b, a) = 1, \qquad (a, b, b) = 1. \tag{4.1}$$

The argument above proves a little more, namely that in a group K if $u^3 = v^3 = 1$ and $xux = u^{-1}$, $xvx = v^{-1}$, then $\{u, v\}$ is a group of exponent 3 and order at most 27.

When K is generated by four independent involutions, a_1, a_2, a_4, a_{10}, let us put $x = a_1$, $a = a_1 a_2$, $b = a_1 a_4$, $c = a_1 a_{10}$. Then each of the groups $\{a, b\}$, $\{a, c\}$, $\{b, c\}$ is of exponent 3 and order at most 27. Let us write $u_1 = (a, b)$, $u_2 = (b, c)$, $u_3 = (c, a)$, $v_1 = (a, b, c)$, $v_2 = (a, b, c^{-1})$, $v_3 = (b, c, a)$, $v_4 = (b, c, a^{-1})$, $v_5 = (c, a, b)$, $v_6 = (c, a, b^{-1})$. Then we find

$$a^{-1}u_2 a = a^{-1}(b, c)a = a^{-1}a(b, c)(b, c, a) = u_2 v_3.$$
$$\begin{aligned} a^{-1}v_1 a &= a^{-1}(a, b, c)a = a^{-1}(a, b)^{-1}c^{-1}(a, b)ca \\ &= (a, b)^{-1}a^{-1}c^{-1}acc^{-1}a^{-1}(a, b)acc^{-1}a^{-1}ca \\ &= (a, b)^{-1}(a, c)c^{-1}(a, b)c(c, a) \\ &= (a, b)^{-1}(a, c)(a, b)(a, b, c)(c, a) \\ &= u_1^{-1}u_3^{-1}u_1 v_1 u_3. \end{aligned} \tag{4.2}$$
$$\begin{aligned} a^{-1}v_3 a &= a^{-1}(b, c, a)a = a^{-1}(b, c)^{-1}a^{-1}(b, c)aa \\ &= [a^{-1}(b, c)a]^{-1}a(b, c)a^{-1} \\ &= [(b, c)(b, c, a)]^{-1}(b, c)(b, c, a^{-1}) \\ &= (b, c, a)^{-1}(b, c, a^{-1}) \\ &= v_3^{-1}v_4. \end{aligned}$$

In this way we construct the transformation table:

z	$a^{-1}za$	$b^{-1}zb$	$c^{-1}zc$
u_1	u_1	u_1	$u_1 v_1$
u_2	$u_2 v_3$	u_2	u_2
u_3	u_3	$u_3 v_5$	u_3
v_1	$u_1^{-1}u_3^{-1}u_1 v_1 u_3$	$u_1^{-1}u_2 u_1 v_1 u_2^{-1}$	$v_1^{-1}v_2$
v_2	$u_1^{-1}u_3 u_1 v_2 u_3^{-1}$	$u_1^{-1}u_2^{-1}u_1 v_2 u_2$	v_1^{-1}
v_3	$v_3^{-1}v_4$	$u_2^{-1}u_1^{-1}u_2 v_3 u_1$	$u_2^{-1}u_3 u_2 v_3 u_3^{-1}$
v_4	v_3^{-1}	$u_2^{-1}u_1^{-1}u_2 v_4 u_1^{-1}$	$u_2^{-1}u_3^{-1}u_2 v_4 u_3$
v_5	$u_3^{-1}u_1 u_3 v_5 u_1^{-1}$	$v_5^{-1}v_6$	$u_3^{-1}u_2^{-1}u_3 v_5 u_2$
v_6	$u_3^{-1}u_1^{-1}u_3 v_6 u_1$	v_5^{-1}	$u_3^{-1}u_2 u_3 v_6 u_2^{-1}$.

(4.3)

In the same way we find the effect of the replacements $a \to a^{-1}$, $b \to b^{-1}$ and $c \to c^{-1}$.

	$a \to a^{-1}$	$b \to b^{-1}$	$c \to c^{-1}$
u_1	u_1^{-1}	u_1^{-1}	u_1
u_2	u_2	u_2^{-1}	u_2^{-1}
u_3	u_3^{-1}	u_3	u_3^{-1}
v_1	$u_1v_1^{-1}u_1^{-1}$	$u_1v_1^{-1}u_1^{-1}$	v_2
v_2	$u_1v_2^{-1}u_1^{-1}$	$u_1v_2^{-1}u_1^{-1}$	v_1
v_3	v_4	$u_2v_3^{-1}u_2^{-1}$	$u_2v_3^{-1}u_2^{-1}$
v_4	v_3	$u_2v_4^{-1}u_2^{-1}$	$u_2v_4^{-1}u_2^{-1}$
v_5	$u_3v_5^{-1}u_3^{-1}$	v_6	$u_3v_5^{-1}u_3^{-1}$
v_6	$u_3v_6^{-1}u_3^{-1}$	v_5	$u_3v_6^{-1}u_3^{-1}$. (4.4)

The relations (4.3) show that the u's and the v's generate a normal subgroup of K_1 containing (a, b), (b, c), and (c, a). This must therefore be the derived group K_1'. Note that the group K subject only to the relations of the lemma has as automorphisms permutations of the generators and replacement of a generator by its inverse.

Since $x(aba)x = a^{-1}b^{-1}a^{-1} = (aba)^{-1}$ and $xcx = c^{-1}$ then $\{aba, c\}$ is of exponent 3 and in particular $(c\ aba)^3 = 1$. We shall apply the collecting process to this using the rule $RS = SR(R, S)$ repeatedly. We shall put a bar over the letter to be collected in the next stage:

$$c\ aba\ c\ \bar{a}\ ba\ caba = 1$$

$$c\ a\ b\ a^{-1}\ c(c, a)\ b\ \bar{a}\ c\ aba = 1$$

$$c\ ab\ c\ (c, a)^2\ b(b, a)\ c\ \bar{a}\ ba = 1$$

$$c\ a^{-1}\ b(b, a)\ c\ b\ (b, a)^2\ c(c, a)\ b\ \bar{a} = 1$$

$$c\ b\ (b, a)^2\ c(c, a)\ b\ c(c, a)^2\ b(b, a) = 1$$

$$c(a, b)\ bc(c, a)\ bc(a, c)\ b(b, a) = 1$$

$$c\ u_1\ b\ c\ u_3\ \bar{b}\ c\ u_3^{-1}\ b\ u_1^{-1} = 1$$

$$c\ u_1\ b\ c\ b\ u_3\ v_5\ \bar{c}\ u_3^{-1}\ b\ u_1^{-1} = 1$$

$$c\ u_1\ bc\ bc\ u_3\ u_3^{-1}\ u_2^{-1}\ u_3\ v_5\ u_2\ u_3^{-1}\ b\ u_1^{-1} = 1$$

$$c\ u_1\ bcbc\ u_2^{-1}\ u_3\ v_5\ u_2\ u_3^{-1}\ \bar{b}\ u_1^{-1} = 1$$

$$c\ u_1\ bc\ bc\ b\ u_2^{-1}\ u_3\ v_5\ v_5^{-1}\ v_6\ u_2\ v_5^{-1}\ u_3^{-1}\ u_1^{-1} = 1$$

$$c\ u_1\ c^{-1}\ u_2^{-1}\ u_3\ v_6\ u_2\ v_5^{-1}\ u_3^{-1}\ u_1^{-1} = 1. \quad (4.5)$$

If we now use the rule

$$cu_1c^{-1} = c^{-1}(c^{-1}u_1c)c = c^{-1}(u_1v_1)c = u_1v_1v_1^{-1}v_2 = u_1v_2,$$

then (4.5) transformed by u_1 gives

$$v_2u_2^{-1}\ u_3\ v_6\ u_2\ v_5^{-1}\ u_3^{-1} = 1. \quad (4.6)$$

Since $(a, b)^{-1}c(a, b)$ and c are of order 3 and transformed into their inverses by x, they generate a group of exponent 3. In particular

$$v_1^3 = [(a, b)^{-1}\ c^{-1}(a, b)\ c]^3 = 1$$

and also

$$(cv_1)^3 = 1$$

$$cv_1\ cv_1\ c\ v_1 = 1$$

$$cv_1\ c^{-1}\ c^{-1}\ v_1\ c\ v_1 = 1$$

$$v_2^{-1}\ v_1^{-1}\ v_2\ v_1 = 1. \quad (4.7)$$

Hence by automorphisms of K

$$v_i^3 = 1 \qquad i = 1, \cdots, 6$$

$$(v_1, v_2) = 1, \qquad (v_3, v_4) = 1, \qquad (v_5, v_6) = 1. \quad (4.8)$$

Transform (4.6) by c^{-1}, obtaining

$$v_2^{-1}\ v_1\ u_2^{-1}\ u_3\ u_3^{-1}\ u_2^{-1}\ u_3\ v_6\ u_2 \cdot u_2\ u_2\ v_5^{-1}\ u_3^{-1}\ u_2^{-1}\ u_3\ u_3^{-1} = 1, \quad (4.9)$$

whence

$$v_2^{-1}\ v_1 = u_2\ u_3\ v_5\ v_6^{-1}\ u_3^{-1}\ u_2^{-1}. \quad (4.10)$$

In (4.10) replace c by c^{-1}, giving

$$v_1^{-1}\ v_2 = u_2^{-1}\ u_3^{-1}\ (u_3\ v_5^{-1}\ u_3^{-1})(u_3\ v_6\ u_3^{-1})u_3\ u_2 = u_2^{-1}\ v_5^{-1}\ v_6\ u_2. \quad (4.11)$$

Take the inverse of (4.11) and use (4.8)

$$v_2^{-1}\ v_1 = u_2^{-1}\ v_6^{-1}\ v_5\ u_2 = u_2^{-1}\ v_5\ v_6^{-1}\ u_2 \quad (4.12)$$

Comparing (4.10) and (4.12) we find that $v_5v_6^{-1}$ and $u_3^{-1}u_2$ permute, or

$$(v_5\ v_6^{-1},\ u_3^{-1}\ u_2) = 1. \quad (4.13)$$

Transform (4.13) by b and we find

$$(v_6,\ v_5^{-1}\ u_3^{-1}\ u_2) = 1, \quad (4.14)$$

whence using (4.8) and (4.13)

$$(v_6,\ u_3^{-1}\ u_2) = 1, \qquad (v_5,\ u_3^{-1}\ u_2) = 1. \quad (4.15)$$

In (4.15) replace b by b^{-1}, giving

$$(v_5,\ u_3^{-1}\ u_2^{-1}) = 1 \qquad (v_6,\ u_3^{-1}\ u_2^{-1}) = 1. \quad (4.16)$$

But since $u_2^{-1} = (u_3^{-1}u_2^{-1})^{-1}u_3^{-1}u_2$, (4.15) and (4.16) together give

$$(v_5, u_2) = 1 \qquad (v_5, u_3) = 1$$

$$(v_6, u_2) = 1 \qquad (v_6, u_3) = 1. \quad (4.17)$$

In $(v_5,\ u_2) = 1$ interchange c and a, giving $(u_3v_5^{-1}u_3^{-1},\ u_1^{-1}) = 1$, or $(v_5^{-1},\ u_1^{-1}) = 1$, whence

$$(v_5, u_1) = 1. \quad (4.18)$$

Making appropriate substitutions in (4.17) and

(4.18) we find

$$(v_i, u_j) = 1 \qquad i = 1, \cdots 6, j = 1, 2, 3. \tag{4.19}$$

The equation (4.11) now takes the form

$$v_1^{-1} v_2 = v_5^{-1} v_6, \tag{4.20}$$

and permuting the generators, gives

$$v_1^{-1} v_2 = v_3^{-1} v_4 = v_5^{-1} v_6. \tag{4.21}$$

Using (4.19), (4.6) now becomes

$$u_2^{-1} u_3 u_2 u_3^{-1} = v_5 v_6^{-1} v_2^{-1} \tag{4.22}$$

and substituting in this from (4.21) we have

$$u_2^{-1} u_3 u_2 u_3^{-1} = v_1 v_2^{-1} v_2^{-1} = v_1 v_2. \tag{4.23}$$

From the transformation table (4.3) and (4.19) we see that the left-hand side of (4.23) is unchanged by transformation by a, b, c and therefore v_1v_2 is in the center of K_1. Let us write $w_1 = v_1v_2$ and similarly $w_2 = v_3v_4$, $w_3 = v_5v_6$, where w_1, w_2, w_3 are in the center of K_1. Since $(a^{-1}, b^{-1}) = (a, b)xv_1x = v_2$, $xv_2x = v_1$ and as v_1 and v_2 permute by (4.8) it follows that $xw_1x = w_1$. Thus w_1 is in the center of K and similarly w_2 and w_3. We may now use (4.21) to express the v's in terms of v_1 and the w's.

$$\begin{aligned} v_2 &= v_1^{-1} w_1 \\ v_3 &= v_1 w_1 w_2^{-1} \\ v_4 &= v_1^{-1} w_1^{-1} w_2^{-1} \\ v_5 &= v_1 w_1 w_3^{-1} \\ v_6 &= v_1^{-1} w_1^{-1} w_3^{-1}. \end{aligned} \tag{4.24}$$

We can now write relations for K in the following form, applying automorphisms of K to (4.23):

$$x^2 = 1, \quad a^3 = b^3 = c^3 = 1, \quad u_1^3 = u_2^3 = u_3^3 = 1$$

$$v_1^3 = w_1^3 = w_2^3 = w_3^3 = 1$$

$$u_1 = (a, b), \quad u_2 = (b, c), \quad u_3 = (c, a)$$

$$v_1 = (a, b, c), \quad u_i^{-1} v_1 u_i = v_1$$

$$(u_2 , u_3^{-1}) = (u_2^{-1}, u_3) = (u_2 , u_3)^{-1} = (u_2^{-1}, u_3^{-1})^{-1} = w_1$$

$$(u_3 , u_1^{-1}) = (u_3^{-1}, u_1) = (u_3 , u_1)^{-1} = (u_3^{-1}, u_1^{-1})^{-1} = w_2$$

$$(u_1 , u_2^{-1}) = (u_1^{-1}, u_2) = (u_1 , u_2)^{-1} = (u_1^{-1}, u_2^{-1})^{-1} = w_3$$

$$a^{-1}u_1a = u_1, \quad b^{-1}u_1b = u_1, \quad c^{-1}u_1c = u_1v_1$$

$$a^{-1}u_2a = u_2v_1w_1w_2^{-1}, \quad b^{-1}u_2b = u_2, \quad c^{-1}u_2c = u_2$$

$$a^{-1}u_3a = u_3, \quad b^{-1}u_3b = u_3v_1w_1w_3^{-1}, \quad c^{-1}u_3c = u_3$$

$$a^{-1}v_1a = v_1w_2, \quad b^{-1}v_1b = v_1w_3 \quad c^{-1}v_1c = v_1w_1$$

$$a^{-1}w_ia = w_i \quad b^{-1}w_ib = w_i \quad c^{-1}w_ic = w_i$$

$$x\,ax = a^{-1}, \quad x\,bx = b^{-1}, \quad x\,cx = c^{-1},$$

$$x\,u_i\,x = u_i, \quad x\,v_1\,x = v_1^{-1}\,w_1, \quad x\,w_i\,x = w_i. \tag{4.25}$$

Further calculations, which will not be given here, show that the relations of (4.25) define a group K of order $2 \cdot 3^{10}$ and that for every $z \in K$, $(xz^{-1}xz)^3 = 1$. This may be done by taking an elementary Abelian 3-group generated by v_1, w_1, w_1, w_3 and extending this group by adjoining u_3, u_2, u_1, c, b, and a in succession, using the appropriate relations from (4.25) to define the extensions, and then checking $(xz^{-1}xz)^3 = 1$ for representative values of z, observing that if $h \in C(x)$ then $x(hz)^{-1}z(hz) = xz^{-1}xz$.

What sort of Steiner triple system S corresponds to the group K defined by the relations (4.25)? Here u_1, u_2, u_3, w_1, w_2, $w_3 \in C(x)$. For $g \in G$ we have

$$g = a^{e_1} b^{e_2} c^{e_3} v_1^f h, \quad h \in C(x). \tag{4.26}$$

We find

$$\begin{aligned} g\,x\,g^{-1} &= x(xgx)g^{-1} \\ &= xa^{-e_1} b^{-e_2} c^{-e_3} v^{-f} w_1^f v_1^{-f} c^{-e_3} b^{-e_2} a^{-e_1} \\ &= x \cdot k(g). \end{aligned} \tag{4.27}$$

The number of conjugates of x is the number of values of $k(g)$ and this is in turn the number of points of S. Thus the group K defines a Steiner triple system with 81 points, and $S(81)$.

We must also consider Steiner triple systems defined by homomorphic images of K, if we are to find all systems generated by four independent points, where every triangle generates on $S(9)$. We see that

$$k(g) \equiv a^{e_1} b^{e_2} c^{e_3} \pmod{K_1'}. \tag{4.28}$$

Here if S has fewer than 81 points then S corresponds to a factor group K/T where the kernel T is determined by the identification of different values of $k(g)$ in (4.27). If $k(g_1)k(g_2)^{-1} \in T$ and $k(g_1) \equiv k(g_2) \mod K_1'$, then K_1/T is generated by at most two elements, and we have an $S(3)$ or $S(9)$. Hence suppose $k(g_1) \equiv k(g_2) \mod K_1'$, but $k(g_1) \not\equiv k(g_2)$. From (4.27) we see that this shows that $v_1w_1 \in T$ and by transformation that v_1, w_1, w_2, $w_3 \in T$. Then in K_1/T we have relations $v_i = 1$, $i = 1, \cdots, 6$.

We state these results in a lemma which now leads to the proof of our theorem.

• *Lemma 4.2*

If S is a Steiner triple system in which every triangle

generates an $S(9)$, then four independent points generate either an $S(81)$ or an $S(27)$. If they generate an $S(81)$ the group K associated with S satisfies the relations (4.25). If they generate an $S(27)$ the associated group K satisfies the further relations $v_i = 1, i = 1, \cdots, 6$.

We now observe that if four independent points, 1, 2, 4, 10 generate an $S(81)$, then this $S(81)$ contains an $S(27)$, corresponding to the subgroup K^* of K generated by $a_1 = x$, $a = a_1a_2$, $b = a_1a_4$ and v_1. For we easily verify that in K^* all elements are products of x, a, b, u_1, v_1, w_1, w_2, w_3 in this order with appropriate exponents and that in K^* there are exactly 27 conjugates of x, this corresponding to an $S(27)$ generated by points 1, 2, 4, t, $a_t = v_1^{-1}xv_1$.

We now have everything needed to complete the proof of Theorem 4.2. Lemma 4.2 shows that if S has the property that every triangle generates an $S(9)$, then if S has more than 9 points there exist four independent points generating an $S(27)$. As we are assuming that our group G of automorphisms of S is transitive on sets of four independent points, it follows that every set of four independent points generates an $S(27)$. Now consider the group K associated with S, and suppose K generated by involutions $a_1 = x, a_2, \cdots, a_r$. If we write $a_1a_2 = b_1$, $a_1a_3 = b_2 \cdots a_1a_r = b_{r-1}$ then reference to Lemma 4.2 tells us that $(b_i, b_j, b_k) = 1$ in every instance. Hence every commutator (b_i, b_j) permutes with every b as well as with x and so is in the center of K. But K as a permutation group is represented on the cosets of $C(x)$. In this representation every commutator (b_i, b_j) is represented by the identity. Hence we obtain the same Steiner system if we take every commutator (b_i, b_j) to be the identity, i.e., if K_1 is simply an elementary Abelian 3-group A and x as an involution which transforms every element of A into its inverse. By Lemma 4.1 we can now construct S explicitly. Let $b_1 = 1, b_2, \cdots, b_n$ be the distinct elements of A, where of course $n = 3^r$ for some r. Then $x = a_1$, $a_2 = b_2^{-1}xb_2, \cdots, a_n = b_n^{-1}xb_n$ are the involutions of K. The triples of S are i, j, k, if $a_i = (i) \cdots (j, k) \cdots$. Here $C(x)$ contains the two elements 1, $x = a_1$ and the point i is associated with the coset $C(x)b_i$ whose two elements are b_i and xb_i. Here $a_i = b_i^{-1}xb_i = xb_i^{-1}$. Then i, j, k is a triple of S if and only if $C(x)b_ja_i = C(x)b_k$. But this gives $b_k = b_i^{-1}b_j^{-1}$. Hence i, j, k is a triple if and only if $b_ib_jb_k = 1$ in A. If we write A as the additive group of r dimensional vectors over $GF(3)$ a relation $P_i + P_j + P_k = 0$ holds if and only if the points P_i, P_j, P_k lie on a line. Thus S may be regarded as the affine geometry of dimension r over $GF(3)$. This completes the proof of Theorem 4.2.

References and footnotes

[1] Marshall Hall, Jr., *Theory of Groups*, Macmillan, New York, 1959.

[2] T. G. Ostrom and A. Wagner, *Math. Zeitschr.*, **71**, 186–199 (1959).

[3] C. Jordan, *Jour. de Math. Pures et Appl.*, **16**, 383-408 (1871).

[4] W. Burnside, *Theory of Groups of Finite Order*, Cambridge University Press, 2nd ed., 1911.

[5] H. B. Mann, *Analysis and Design of Experiments*, Dover Publications, New York, (1949).

[6] In a projective geometry of dimension n over $GF(2)$, every triangle generates an $S(7)$ and the points may be regarded as the elements of an elementary Abelian 2-group A of order 2^{n+1} with the identity excluded. If F is the subgroup of A fixed pointwise by an involution, it can be shown that $[F : 1] \geq [A : F]$. Thus, if $n \geq 4$, any involution of A fixes a subgroup F of order at least 8 and hence fixes at least 7 points in the corresponding Steiner triple system.

Received June 27, 1960.