STEINER TRIPLE SYSTEMS WITH BLOCK-TRANSITIVE AUTOMORPHISM GROUPS

Thesis by

Paul Charles Clapham

In Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

1974

(Submitted May 1, 1974)

Acknowledgements

I would like to thank my advisor, Marshall Hall Jr., for directing my attention toward the topic of this thesis. I would also like to thank the California Institute of Technology for their financial support during the past four years. Finally, thanks are due to my wife, Rosemary, for not insisting upon typing the manuscript.

Abstract

If G is an automorphism group of a Steiner triple system which is doubly transitive on the points, then it is transitive on the blocks. It is shown that the converse is false and that all counterexamples have odd order. All Steiner triple systems which have a block-transitive but not doubly point-transitive group of automorphisms are described. They include the Euclidean geometries of odd dimension over GF(3), a class of systems first described by Netto in 1893, and another class of systems. A system in this third class has a group of automorphisms acting regularly on the blocks, and the number of points is a prime power congruent to 7 modulo 12. The number of such systems (up to isomorphism) with a prime number of points p, where $p \equiv 7 \pmod{12}$, is shown to be in the interval $\left((\sqrt{p} - 1)^2/27,\ 1 + (\sqrt{p} + 1)^2/27\right)$.

The classification of block-transitive Steiner triple systems is applied to prove the following theorem: if G is a doubly transitive automorphism group of a Steiner triple system and P is a p-subgroup of G maximal subject to the condition that it fix more than three points, then the points fixed by P form a subsystem with a doubly transitive automorphism group.

Table of Contents

1. Introduction

A Steiner triple system is an ordered pair (V,B), where V is a finite set of elements (called points) and B is a collection of blocks, each of which contains exactly three points of V. B must also satisfy the property that for every pair of distinct points $x,y \in V$ there exists exactly one block $\beta \in B$ such that $x,y \in \beta$. The set of blocks which contain a given point $x \in V$ will be denoted $B(x)$. If $|V| = v$, then it is not difficult to see that $|B(x)| = (v-1)/2$ and $|B| = v(v-1)/6$. In particular, a necessary condition for the existence of such a system is $v \equiv 1$ or $3 \pmod 6$.

A subset W of V forms the points of a subsystem of (V,B) if $x,y \in W$ and $\{x,y,z\} \in B$ imply $z \in W$. This subsystem is denoted $(W,B|_W)$. A triangle in (V,B) is a set of three points not all contained in a single block, and the subsystem generated by a triangle is the smallest subsystem containing it.

If g is an automorphism of (V,B) which fixes $x,y \in V$, then it must fix z, where $\{x,y,z\} \in B$. Hence (V,B) cannot have a triply transitive automorphism group. There are two infinite families of Steiner triple systems with doubly transitive automorphism groups, namely the Euclidean (or affine) geometries $EG(n,3)$ over $GF(3)$ and the projective geometries $PG(n,2)$ over $GF(2)$, for $n \geq 2$. They can be described in terms of elementary abelian groups as follows. ($E(q)$ denotes the elementary abelian group of order q.)

$EG(n,3) = (V,B)$, where $V = E(3^n)$ and $B = \left\{\{x,y,x^2y^2\} \mid x,y \in V, x \neq y\right\}$. As $x^2(x^2y^2)^2 = y$, this is indeed a Steiner triple system. Its automorphism group is $E(3^n)*GL(n,3)$.

$PG(n,2) = (V,B)$, where $V = E(2^{n+1}) - \{1\}$ and $B = \{\{x,y,xy\} \mid x,y \in V,\ x \neq y\}$. This is a Steiner triple system since $x(xy) = y$, and its automorphism group is $GL(n+1,2)$.

In this thesis we will consider properties of the automorphism group similar to double transitivity. In particular, a slight weakening of the double transitivity hypothesis will yield a "much larger" infinite family of systems.

The permutation group-theoretic terminology used is standard and can be found in [19], with the following exceptions: if R^Ω is a permutation group and $A \leq \Omega$, then $R_{(A)} = \left\{r \in R \mid A^r = A\right\}$ and $R_A = \left\{r \in R \mid a^r = a \text{ for all } a \in A\right\}$, and if $T \leq R$ then $F(T) = \left\{x \in \Omega \mid x^T = x\right\}$. Also, what Wielandt calls a block in [19; ch. 6 ff] will be called a <u>set of imprimitivity</u>. Other group-theoretic notions are in [6], except: D_n is the dihedral group of order n, SD_n is the semidihedral group of order n (a power of 2), $\Sigma(q) = \left\{t \rightarrow at^\theta + b \mid a,b,t \in GF(q),\ a \neq 0, \theta \in \mathrm{Aut}GF(q)\right\}$ is the group of semilinear transformations on GF(q), and $\mathrm{Syl}_p(R)$ is the set of Sylow p-groups of a group R.

2. Useful Lemmas

This chapter consists of a number of lemmas, mostly from the literature, which will be applied in later chapters. Only Lemma 2.13 is new.

Lemma 2.1 [1] Let c and n be integers greater than 1. Assume that for every prime p dividing c^n-1 there exists a positive integer $m<n$ such that $p \mid c^m-1$. Then either c is a Mersenne prime and $n = 2$, or $c = 2$ and $n = 6$.

Lemma 2.2 [4] If (W,A) is a Steiner triple system, $|W| = w$, and $(U, A|_U)$ is a proper subsystem, then $|U| \leq (w-1)/2$.

Lemma 2.3 [7] Let (W,A) be a Steiner triple system such that for every block $\alpha \in A$ there exists an automorphism g of order 2 with $F(g) = \alpha$. Then either every triangle generates a subsystem isomorphic to PG(2,2) or every triangle generates a subsystem isomorphic to EG(2,3).

Lemma 2.4 [8] If (W,A) is a Steiner triple system such that $|W| = 27$ and every triangle generates a subsystem isomorphic to EG(2,3), then $(W,A) \cong EG(3,3)$.

Lemma 2.5 Let (W,A) be a Steiner triple system in which every triangle generates a subsystem isomorphic to PG(2,2). Then $(W,A) \cong PG(n,2)$ for some integer $n \geq 2$.

Proof Let $V = W \cup \{1\}$, where $1 \notin W$, and define multiplication on V as follows: first, $x^2 = 1$ and $1x = x1 = x$ for all $x \in V$, and second, if $x, y \in W$ and $x \neq y$ then $\{x, y, xy\} \in A$. Since $(xy)z = x(yz)$ in $PG(2,2)$, it follows easily that multiplication on V is associative, whence V is an elementary abelian 2-group. Therefore $(W, A) \cong PG(n,2)$ for some n, since A is the correct set of blocks.

Lemma 2.6 [18] Let T be a 2-group containing an involution t such that $C_T(t) \cong Z_2 \times Z_2$. Then $T \cong D_n$ or SD_n.

Lemma 2.7 [15] Let R^Ω be a solvable 3/2-transitive permutation group. Then one of the following situations occurs:

1. R^Ω is a Frobenius group;
2. $\Omega = GF(q)$, $R \leq \Sigma(q)$;
3. R^Ω is a certain group of transformations on $GF(q) \times GF(q)$;
4. $|\Omega| \in \{3^2, 5^2, 7^2, 11^2, 17^2, 3^4\}$.

Lemma 2.8 [20] Let R^Ω be doubly transitive and let $T \in Syl_p(R_{xy})$ for some prime p. Then $N_R(T)^{F(T)}$ is doubly transitive.

Lemma 2.9 Let R^Ω be a permutation group and let p be a fixed prime. Assume that for every $x \in \Omega$ there is a p-group $P \leq R$ with $F(P) = \{x\}$. Then R^Ω is transitive.

Proof Let $\Gamma \subseteq \Omega$ be an orbit of R and let $x \in \Gamma$. Then there is a p-group $P \leq R$ with $F(P) = \{x\}$, so $|\Gamma| \equiv 1 \pmod p$. If $y \in \Omega - \Gamma$ then there is a p-group $Q \leq R$ such that $F(Q) = \{y\}$. But then $|\Gamma| \equiv 0 \pmod p$, a contradiction. Hence $\Gamma = \Omega$ and R^{Ω} is transitive.

Lemma 2.10 [12] If R^{Ω} is faithful and doubly transitive, and $PSL(2,q) \leq R \leq P\Gamma L(2,q)$, then either R^{Ω} is contained in the usual representation of $P\Gamma L(2,q)$ on $q+1$ points or one of the following holds:

1. $|\Omega| = 6$, $R \cong PSL(2,4)$ or $P\Gamma L(2,4)$;
2. $|\Omega| = 5$, $R \cong PSL(2,5)$ or $PGL(2,5)$;
3. $|\Omega| = 7$, $R \cong PSL(2,7)$;
4. $|\Omega| = 28$, $R \cong P\Gamma L(2,8)$;
5. $|\Omega| = 6$, $R \cong PSL(2,9)$ or $PSL(2,9)\langle\sigma\rangle$, $\langle\sigma\rangle = \mathrm{Aut}GF(9)$
6. $|\Omega| = 11$, $R \cong PSL(2,11)$.

Lemma 2.11 [2] Let R^{Ω} be a primitive permutation group such that the maximum number of fixed points of an involution is 3. Let T be a minimal normal subgroup of R. Then one of the following cases occurs:

1. $R^{\Omega} = E(9)*GL(2,3)$;
2. $R^{\Omega} = E(9)*SD_{16}$;
3. $R^{\Omega} = E(9)*D_8$ (rank 3);
4. $R^{\Omega} = E(27)*SL(3,3)$;
5. $R^{\Omega} = E(27)*S_4$ (rank 4);

6. $R^\Omega = E(27)*A_4$ (rank 5);

7. $R^\Omega = S_5$;

8. $R^\Omega = A_7$;

9. $R^\Omega = M_{11}$;

10. $R \cong A_7$, $|\Omega| = 15$;

11. $R^\Omega = GL(3,2)$;

12. $R \cong PSL(2,11)$, $|\Omega| = 11$;

13. $R \cong PSL(2,9)$, $|\Omega| = 15$ (rank 3);

14. $T \cong PSL(2,9)$, $|R:T| = 2$, $|\Omega| = 15$, $R-T$ has no involutions (rank 3);

15. $R \cong PSL(2,13)$, $|\Omega| = 91$ (rank 10).

Let R^Ω be a transitive permutation group of rank r, and let the orbits of R_x be $\Gamma_0(x) = \{x\}, \Gamma_1(x), \cdots, \Gamma_{r-1}(x)$. We can choose the notation so that $\Gamma_i(x)^g = \Gamma_i(x^g)$ for all $x \epsilon \Omega$ and $g \epsilon R$ and for $0 \le i \le r-1$. Let $h_i = |\Gamma_i(x)|$, and define i' by $\Gamma_{i'}(x) = \Gamma_i'(x)$. The intersection numbers for R^Ω are defined by

$$\mu_{ij}^{(k)} = |\Gamma_k(y) \cap \Gamma_i(x)| \quad \text{if } y \epsilon \Gamma_j(x)$$

Clearly $\mu_{ij}^{(k)}$ is independent of the choice of x and y. The intersection matrices for R^Ω are

$$M_k = \left[\mu_{ij}^{(k)}\right]$$

for $0 \leq k \leq r - 1$. (Note that the rows and columns are numbered from 0 to $r - 1$.) By [10; 4.1 - 4.3], the following relations hold:

$$h_j \mu_{ij}^{(k)} = h_i \mu_{ji}^{(k')} \tag{1}$$

$$h_i \mu_{k'i}^{(j)} = h_j \mu_{i'j}^{(k)} \tag{2}$$

$$M_k \text{ has column sum } h_k \tag{3}$$

<u>Lemma 2.12</u> If $r \leq 4$ then M_i and M_j commute for all $i, j \in \{0, 1, \cdots, r - 1\}$.

<u>Proof</u> By [10; 4.10], M_i and M_j commute if and only if the irreducible constituents of the permutation representation of R^Ω are all inequivalent, which is true if and only if the irreducible constituents of the permutation character have multiplicity 1. As r is the sum of the squares of these multiplicities [19; 29.2] and the identity character has multiplicity 1, all of the multiplicities must be 1 and all M_i and M_j commute.

<u>Lemma 2.13</u> Let R^Ω be a 3/2-transitive rank-4 permutation group with a suborbit which is not self-paired. Then $|\Omega| \equiv 4 \pmod 6$.

<u>Proof</u> Let $\Gamma_0(x) = \{x\}, \Gamma_1(x), \Gamma_2(x)$, and $\Gamma_3(x)$ be the orbits of R_x, where $\Gamma_1' = \Gamma_2$, and let $h = h_1 = h_2 = h_3$. When $i,j,k > 0$, equations (1) and (2) above become

$$\mu_{ij}^{(k)} = \mu_{ji}^{(k')} \tag{4}$$

$$\mu_{k'i}^{(j)} = \mu_{i'j}^{(k)} \tag{5}$$

The first of these gives

$$M_1 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ h & a & d & m \\ 0 & b & f & n \\ 0 & c & g & p \end{pmatrix}, \quad M_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & a & b & c \\ h & d & f & g \\ 0 & m & n & p \end{pmatrix}$$

and the second gives

$$d = \mu_{12}^{(1)} = \mu_{2'2}^{(1)} = \mu_{2'1}^{(2)} = \mu_{11}^{(2)} = a,$$

$$f = \mu_{22}^{(1)} = \mu_{1'2}^{(1)} = \mu_{2'1}^{(1)} = \mu_{11}^{(1)} = a$$

As all column sums of M_1 and M_2 are h, we have

$$M_1 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ h & a & a & h-2a-1 \\ 0 & b & a & h-a-b \\ 0 & h-a-b & h-2a-1 & 3a+b+1-h \end{pmatrix}$$

$$M_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & a & b & h-a-b \\ h & a & a & h-2a-1 \\ 0 & h-2a-1 & h-a-b & 3a+b+1-h \end{pmatrix}$$

By Lemma 2.12, M_1 and M_2 commute. Equating the (1,1)-entries of M_1M_2 and M_2M_1 yields

$$h + 2a^2 + (h - 2a - 1)^2 = a^2 + b^2 + (h - a - b)^2,$$

whence

$$2b^2 + 2ab - 2bh + 2ah - 4a^2 - 4a + h - 1 = 0.$$

Therefore h is odd and $|\Omega| = 3h + 1 \equiv 4 \pmod 6$.

3. The Main Theorem

Suppose that (V,B) is a Steiner triple system with a doubly transitive automorphism group G. If $\beta_1, \beta_2 \in B$ and $\beta_i = \{x_i, y_i, z_i\}$, then there exists $g \in G$ such that $x_1^g = x_2$ and $y_1^g = y_2$. But then $\beta_1^g = \beta_2$, so G is block-transitive. In this chapter, we investigate the converse of this observation. Throughout the chapter, (V,B) denotes a Steiner triple system with an automorphism group G acting transitively on B. Also, we define $v = |V|$.

Lemma 3.1 G^V is primitive, 3/2-transitive, and has rank 2,3,4, or 7.

Proof First, G^V is transitive [3; 2.3.2]. Let $\beta \in B$; then $e = |G_{(\beta)} : G_\beta|$ does not depend on the choice of β, since G^B is transitive. Let $x, y \in V$ be distinct points. Then if $\{x, y, z\} = \beta \in B$,

$$|G_x : G_{xy}| = |G_x : G_\beta|$$

$$= \frac{|G : G_{(\beta)}|\,|G_{(\beta)} : G_\beta|}{|G : G_x|} = \frac{v(v-1)}{6}\,\frac{e}{v} = \frac{e(v-1)}{6}$$

Thus G^V is 3/2-transitive. Now $G_{(\beta)}/G_\beta$ is isomorphic to a subgroup of S_3, so $e \in \{1,2,3,6\}$ and the nontrivial orbits of G_x have length $v - 1$, $(v-1)/2$, $(v-1)/3$, or $(v-1)/6$. In particular, the rank of G^V is 2,3,4, or 7.

If $|G|$ is even then there exists $g = (x\ y)\cdots \in G$ for some $x, y \in V$. Then $\{x, y, z\} \in B$ for some $z \in V$, so $g = (x\ y)(z)\cdots$ and e is even. Hence, if $|G|$ is even then G^V has rank 2 or 4.

Suppose G^V were imprimitive. Then a set of imprimitivity T would consist of a point $x \in V$ together with some orbits of G_x. There are three cases to consider.

If G^V has rank 3 then e = 3. As $|T|$ divides $|V|$, we have $1 + (v - 1)/2 | v$. But this implies $v + 1 | 2v$ and $v = 1$, an absurdity.

If G^V has rank 4 then e = 2. So $1 + (v - 1)/3 | v$, $v + 2 | 3v$, and $v = 1$ or 4. This is also impossible.

If G^V has rank 7 then e = 1. The previous two cases show that $|T| = 1 + (v - 1)/2$ and $|T| = 1 + (v - 1)/3$ are impossible, so $|T| = 1 + (v - 1)/6 | v$. Then $v + 5 | 6v$ and $v \in \{1, 5, 10, 25\}$. As $v \equiv 1$ or 3 (mod 6), the only possibility is $v = 25$. But then $|B| = 100$, so $|G|$ is even, which implies that G^V has rank 2 or 4. This contradicts the assumption that G^V had rank 7, so G^V is primitive.

<u>Lemma 3.2</u> If $v \equiv 1 \pmod 6$ then one of the following holds:

1. G^V is doubly transitive;
2. $|G|$ is odd and $v = p^d \equiv 7 \pmod{12}$ for some prime p.

<u>Proof</u> First assume that $|G|$ is even. Then e is even and there exists an element $g = (x)(y\ z)\cdots \in G$ for some block

$\{x,y,z\} = \beta \in B$. If $e = 6$ then G^V is doubly transitive, so assume $e = 2$. Then $G^{\beta}_{(\beta)} = \langle (x)(y\ z) \rangle$ and by Lemma 3.1, G^V is a primitive 3/2-transitive rank-4 group. Also, there is no element of the form $(x\ y)\cdots \in G$, since such an element would stabilize β. Thus the orbit of G_x which contains y is not self-paired [19; 16.4]. But now Lemma 2.13 implies that $v \equiv 4 \pmod 6$. This is a contradiction, so G_V is doubly transitive if $|G|$ is even.

Now assume that $|G|$ is odd. Then G is solvable [5]. By Lemma 3.1, G^V is primitive, so it has an elementary abelian regular normal subgroup [19; 11.5]. Therefore $v = p^d$ for some prime p. If $v \equiv 1 \pmod{12}$ then $|B| = v(v - 1)/6$ is even, whence $|G|$ is even. Therefore $v \equiv 7 \pmod{12}$.

Lemma 3.3 If $v \equiv 3 \pmod 6$ then one of the following holds:

1. G^V is doubly transitive;
2. G^V is a rank-3 group of odd order and $(V,B) \cong EG(s,3)$ where s is odd.

Proof Let $\{x,y,z\} = \beta \in B$. If $G_{(\beta)}$ fixes x then $G_{(\beta)} \le G_x$, whence $v | v(v - 1)/6$. But then $6 | v - 1$, contrary to $v \equiv 3 \pmod 6$. Therefore $G^{\beta}_{(\beta)}$ is transitive and $e = 3$ or 6. If $e = 6$ then G^V is doubly transitive, so we may assume that $e = 3$. In this case, $|G|$ is odd and G^V has rank 3. Thus G is solvable [5]. By Lemma 3.1, G^V is primitive, so it contains a regular normal subgroup N, which is elementary abelian of order v [19; 11.5]. Since $3 \mid v$, $v = 3^s$. If $v \equiv 9 \pmod{12}$ then $|B| = v(v-1)/6$ is even and $|G|$ is even, a contradiction. So $v \equiv 3 \pmod{12}$ and $3^{s-1} \equiv 1 \pmod{4}$. This implies that s is odd.

As $|N| = 3^s$ and $|B| = 3^{s-1}(3^s - 1)/2$, N^B is not semi-regular, i.e., there exists $\beta \in B$ such that $\beta^n = \beta$ for some $n \in N^\#$. Therefore $\beta = \{x, x^n, x^{n^2}\}$. Now G_x acts as a group of automorphisms on N [19; 11.2], and n and n^2 are in different orbits as $|G|$ is odd. As G_x has only two orbits on $N^\#$, it permutes the cyclic subgroups of N transitively. Thus $\{x, x^n, x^{n^2}\} \in B$ for every $n \in N^\#$. If $m, n \in N$ and $m \neq n$ then $\{x, x^{m^{-1}n}, x^{mn^2}\} \in B$, so $\{x^m, x^n, x^{m^2n^2}\} = \{x, x^{m^{-1}n}, x^{mn^2}\}^m \in B$. Therefore $(V,B) \cong EG(s,3)$.

<u>Theorem 3.4</u> One of the following conclusions holds:

1. G^V is doubly transitive;
2. $|G|$ is odd, $V = GF(p^d)$, $G^V \leq \Sigma(p^d)$, and one of the following holds:
   a. $p = 3$, d is odd, G^V has rank 3, $(V,B) \cong EG(d,3)$
   b. $p^d \equiv 7 \pmod{12}$, G^V has rank 3, $\{0,1,x\} \in B$, where x is a primitive sixth root of unity in $GF(p^d)$;
   c. $p^d \equiv 7 \pmod{12}$, G^V has rank 7.

Proof First, consider the case $v \equiv 1 \pmod 6$. By Lemma 3.2, either G^V is doubly transitive or $|G|$ is odd and $v = p^d \equiv 7 \pmod{12}$. We may assume the latter. By Lemma 3.1 and [5], G^V is solvable and 3/2-transitive. Since $p^d \equiv 7 \pmod{12}$, we have $p \equiv 7 \pmod{12}$ and d odd. So Lemma 2.7 implies that either G^V is a Frobenius group or $G^V \leq \Sigma(p^d)$ and $V = GF(p^d)$.

We will now show that conclusion 2 holds even if G^V is Frobenius. We have $G = NG_x$, where N is elementary abelian of order p^d and $N \lhd G$. It follows from the proof of [14; 18.2] that $G_x = \langle a,b \mid a^n = b^m = 1, a^{-1}ba = b^r \rangle$, where $(r-1,m) = (n,m) = 1, r^{n/n'} \equiv 1 \pmod m$, and n' is the product of the distinct prime factors of n. Clearly $Y = \langle a^{n/n'}, b \rangle$ is a normal cyclic subgroup of G_x; if Y acts irreducibly on N then $V = GF(p^d)$ and $G^V \leq \Sigma(p^d)$ by [14; 19.8]. So assume that Y normalizes a proper subgroup $M \leq N$, where $M \neq 1$. Then $|Y| = n'm \mid p^f - 1$, where $p^f = |M| < p^d$. G^V has rank 3 or 7 by Lemmas 3.1 and 3.2. For the moment assume that the rank of G^V is 7. Then $|G_x| = (p^d - 1)/6$ and $p^d - 1 = 6mn$. Let q be a prime dividing $p^d - 1$. Then $q|6$, $q|m$, or $q|n$. But $q|n$ implies $q|n'$, and $p^f \equiv 1 \pmod 6$, so $q|p^f - 1$. This contradicts Lemma 2.1, which says that d must be even. If the rank of G^V is 3 then $p^d - 1 = 2mn$ and the same contradiction occurs, so conclusion 2 holds.

As $V = GF(p^d)$ and $G^V \leq \Sigma(p^d)$, $G_0 = QR$ where $R = \langle\sigma\rangle$ is a group of field automorphisms normalizing Q. Let $\beta = \{0,1,x\} \in B$. As σ fixes 0 and 1, it must fix x also. Now R normalizes NQ, so it permutes the NQ-orbits in B. In particular, since $\beta^R = \beta$, R stabilizes the orbit containing β, whence $\beta^{NQ} = \beta^{NQR} = \beta^G = B$ and NQ is block-transitive. By Lemma 3.1, NQ^V is 3/2-transitive; as R permutes the Q-orbits in V and fixes 1, it stabilizes the orbit containing 1. Now NQ^V and G^V are both 3/2-transitive, and Q and G_0 have an orbit in common, so NQ^V and G^V have the same rank, namely 3 or 7.

If G^V has rank 7 then conclusion 2c holds, so assume that G^V (and NQ^V) has rank 3. Then e = 3 and there exists an element $h = (0\ 1\ x)\cdots \in NQ$. If $t \in V$ then $t^h = bt + c$ for some $b, c \in GF(p^d)$, so $c = 0^h = 1$ and $b + c = 1^h = x$, i.e., $t^h = (x - 1)t + 1$. Now $0 = x^h = x^2 - x + 1$, and $x \neq -1$ since $p \neq 3$. Therefore $0 = (x^2 - x + 1)(x + 1) = x^3 + 1$ and x is a primitive sixth root of unity. It is not difficult (but messy) to check that the images of $\{0,1,x\}$ under $O(\Sigma(p^d))$, which is of index two in $\Sigma(p^d)$, do form the blocks of a Steiner triple system. Therefore the theorem is true when $v \equiv 1 \pmod 6$.

Second, consider the case $v \equiv 3 \pmod 6$. By Lemma 3.3, either conclusion 1 holds or conclusion 2a holds. To show that $G^V \leq \Sigma(3^d)$, the same proof as in the case $v \equiv 1 \pmod 6$ works. This completes the proof of the theorem.

Note that the systems of types 2a and 2b are the only systems possessing groups of automorphisms which are flag-transitive (i.e., transitive on the set $\{(x,\beta)|x\epsilon\beta\epsilon B\}$) but not doubly transitive. Hence Theorem 3.4 strengthens the following theorem of Lüneburg:

<u>Theorem 3.5</u> [11] There exists a Steiner triple system of order v with a flag-transitive but not doubly transitive automorphism group if and only if v is a prime power congruent to 3 or 7 (mod 12).

The systems of type 2b were first described by Netto [13]. For each prime power $p^d \equiv 7 \pmod{12}$, there is exactly one Netto system, as the following proposition shows.

<u>Proposition 3.6</u> Let $V = GF(p^d)$, $p^d \equiv 7 \pmod{12}$, $G = O(\Sigma(p^d))$, and let x be a primitive sixth root of unity in $GF(p^d)$. Define $B = \{0,1,x\}^G$ and $C = \{0,1,x^{-1}\}^G$. Then $(V,B) \cong (V,C)$.

<u>Proof</u> Let s be a generator of the multiplicative group of $GF(p^d)$ such that $s^{(p^d-1)/6} = x$. If $h\epsilon\Sigma(p^d)$ satisfies $t^h = st$ for all $t\epsilon GF(p^d)$ then $h^2\epsilon G$ and h normalizes G. Hence $B^h = \{0,1,x\}^{Gh} = \{0,1,x\}^{hG} = \{0,s,sx\}^G$. But $sx = s^{(p^d+5)/6}$ is an even power of s since $p^d \equiv 7 \pmod{12}$, so $k = h^{-(p^d+5)/6}\epsilon G$. Now $t^k = (sx)^{-1}t$, so $B^h = \{0,sx,s\}^G$ $= \{0,sx,s\}^{kG} = \{0,1,x^{-1}\}^G = C$. As $V^h = V$, $(V,B) \cong (V,C)$.

4. Block-regular Steiner Triple Systems

It can be inferred from the proof of Theorem 3.4 that a system of type 2c has an automorphism group which acts regularly on the blocks. A Steiner triple system which has such an automorphism group (which need not be the full automorphism group) will be called block-regular. The Netto systems may or may not be block-regular; this will be discussed more explicitly later.

In this chapter, we will assume that (V,B) is a Steiner triple system with a group G of automorphisms which acts regularly on B. It follows from Theorem 3.4 that $V = GF(p^d)$, $p^d \equiv 7 \pmod{12}$, and $G = \{t \to f^{6k}t + b \mid b \in GF(p^d),\ 1 \leq k \leq (p^d - 1)/6\}$, where f is a generator of the multiplicative group of $GF(p^d)$.

Lemma 4.1 Let $x \in V$. Then $\{0,1,x\}^G$ is the set of blocks of a (necessarily block-regular) Steiner triple system if and only if x, $x - 1$, and $x^{-1} - 1$ are not cubes in $GF(p^d)$.

Proof We may clearly assume that x is not 0 or 1. Since G^V is transitive, $\{0,1,x\}^G$ is the set of blocks of a Steiner triple system if and only if the union of those blocks containing 0 is all of $GF(p^d)$. The blocks containing 0 are

$$\{0,f^{6k},xf^{6k}\}, \{0,-f^{6k},(x - 1)f^{6k}\}, \{0,-xf^{6k},(1 - x)f^{6k}\}$$

for $1 \le k \le (p^d - 1)/6$, and their union is $GF(p^d)$ if and only if none of the following equalities occur for any k and ℓ:

$$f^{6k} = -f^{6\ell} \tag{1}$$

$$f^{6k} = -xf^{6\ell} \tag{2}$$

$$f^{6k} = (x - 1)f^{6\ell} \tag{3}$$

$$f^{6k} = -(x - 1)f^{6\ell} \tag{4}$$

$$xf^{6k} = -f^{6\ell} \tag{5}$$

$$xf^{6k} = (x - 1)f^{6\ell} \tag{6}$$

$$xf^{6k} = -xf^{6\ell} \tag{7}$$

$$xf^{6k} = -(x - 1)f^{6\ell} \tag{8}$$

$$-f6k = -xf^{6\ell} \tag{9}$$

$$-f^{6k} = -(x - 1)f^{6\ell} \tag{10}$$

$$(x - 1)f^{6k} = -xf^{6\ell} \tag{11}$$

$$(x - 1)f^{6k} = -(x - 1)f^{6\ell} \tag{12}$$

First of all, equations 1, 7, and 12 are equivalent to $f^{6m} = -1$ for some m, which is not the case since

$p^d \equiv 7 \pmod{12}$. So 1, 7, and 12 are impossible.

Second, 2 and 5 hold if and only if $x = -f^{6m}$ for some m and 9 holds if and only if $x - f^{6m}$ for some m. As -1 is a cube but not a sixth power in $GF(p^d)$, one of 2, 5, 9 is true if and only if $x = f^{3m}$ for some m.

Third, 3 and 10 hold if and only if $x - 1 = f^{6m}$ for some m, and 4 is equivalent to $x - 1 = -f^{6m}$ for some m. Hence one of 3, 4, 10 is true if and only if $x - 1$ is a cube.

Finally, one of 6, 8, 11 holds if and only $x^{-1} - 1$ is a cube. So the falsity of equations 1 to 12 is equivalent to the hypothesis that none of x, $x - 1$, $x^{-1} - 1$ are cubes, and this completes the proof.

We can use this lemma to characterize the block-regular Netto systems:

Proposition 4.2 A Netto system of order $v = p^d$ is block-regular if and only if $p^d \equiv 7$ or $31 \pmod{36}$.

Proof Let x be a primitive sixth root of unity in $GF(p^d)$. If $x - 1 = e^3$ for some $e \in GF(p^d)$, then $0 = x^2 - x + 1 = x(x - 1) + 1 = xe^3 + 1$ and $x = -e^{-3}$ is a cube. Thus Lemma 4.1 says that $\{0,1,x\}^G$ is the set of blocks of a Steiner triple system if and only if x is not a cube. But x is a cube if and only if $3 \mid (p^d - 1)/6$, i.e., $p^d \equiv 1 \pmod{18}$, so since $p^d \equiv 7 \pmod{12}$, $\{0,1,x\}^G$ is the set of blocks of a Steiner triple system if and only if $p^d \not\equiv 19 \pmod{36}$.

Let us define a basic element of $GF(p^d)$ to be an element x such that $\left(GF(p^d), \{0,1,x\}^G\right)$ is a Steiner triple system. Consider the following three sets:

$$A_1 = \{f^{3k} \mid 1 \le k \le (p^d - 1)/3\}$$

$$A_2 = \{f^{3k} + 1 \mid 1 \le k \le (p^d - 1)/3\}$$

$$A_3 = \{(f^{3k} + 1)^{-1} \mid 1 \le k \le (p^d - 1)/3,\ f^{3k} \ne -1\}$$

Then by Lemma 4.1, the set of basic elements is $GF(p^d) - (A_1 \cup A_2 \cup A_3)$. This set is not empty, as the following lemma shows.

Lemma 4.3 The number of basic elements in $GF(p^d)$ is $2 + 2|A_1 \cap A_2|$.

Proof First we prove that $A_1 \cap A_2 = A_1 \cap A_3 = A_2 \cap A_3 = A_1 \cap A_2 \cap A_3$, as follows: let $x \in A_1 \cap A_2$. Then $x = f^{3k} = f^{3\ell} + 1$ for some k and ℓ, so $1 = f^{3k} - f^{3\ell} = f^{3k}\left(1 - f^{3(\ell - k)}\right) = f^{3k}(1 + f^{3m})$ for some m (since -1 is a cube) and $x = f^{3k} = (f^{3m} + 1)^{-1} \in A_3$. Thus $A_1 \cap A_2 = A_1 \cap A_2 \cap A_3$. The proofs of the other equalities are similar.

The number of basic elements is therefore

$$|GF(p^d) - (A_1 \cup A_2 \cup A_3)|$$

$$= p^d - |A_1 \cup A_2 \cup A_3|$$

$$= p^d - |A_1| - |A_2| - |A_3| + |A_1 \cap A_2| + |A_1 \cap A_3|$$

$$+ |A_2 \cap A_3| - |A_1 \cap A_2 \cap A_3|$$

$$= p^d - (p^d - 1)/3 - (p^d - 1)/3 - (p^d - 4)/3 + 2|A_1 \cap A_2|$$

$$= 2 + 2|A_1 \cap A_2| .$$

To every basic element $x \in GF(p^d)$ there corresponds a Steiner triple system (V,B_x), where $\{0,1,x\} \in B_x$. If x and y are basic elements, then (V,B_x) and (V,B_y) may or may not be isomorphic. Define $\eta(p^d)$ to be the number of non-isomorphic block-regular Steiner triple systems with p^d points. Then for $p^d \equiv 7 \pmod{12}$, Lemma 4.3 shows that $\eta(p^d) \geq 1$.

<u>Lemma 4.4</u> If p is a prime, $p \equiv 7 \pmod{12}$, then

$$\eta(p) = \begin{cases} (1 + |A_1 \cap A_2|)/3 & \text{if } p \equiv 19 \pmod{36} \\ 1 + |A_1 \cap A_2|/3 & \text{if } p \equiv 7 \text{ or } 31 \pmod{36} \end{cases}$$

<u>Proof</u> Let $x,y \in GF(p)$ be basic elements and let (V,B_x) and (V,B_y) be the corresponding Steiner triple systems. Note

that G is a group of automorphisms of both systems. Suppose that $(V,B_x) \cong (V,B_y)$. Then there exists g, a permutation of V, which maps B_x to B_y. Let $H = \mathrm{Aut}\ (V,B_y)$; then $G \leq H$ and $G^g \leq H$. Now $G \leq K \leq H$, where K is the normalizer of a Sylow p-group of H and has order dividing $p(p - 1)$. As all subgroups of K of order $p(p - 1)/6$ are conjugate in K, Sylow's theorem implies that $G = G^{gh}$ for some $h \in H$. Thus $gh \in \Sigma(p)$ and $(V,B_x)^{gh} = (V,B_y)$.

It follows that $\Sigma(p)$ permutes the set of block-regular Steiner triple systems of order p, and that two such systems are isomorphic if and only if they are in the same $\Sigma(p)$-orbit. If (V,B_y) is a Netto system then $|\Sigma(p) : \Sigma(p) \cap H| = 2$; otherwise, $|\Sigma(p) : \Sigma(p) \cap H| = 6$. Therefore the block-regular Netto systems (if any) form a $\Sigma(p)$-orbit of length 2 (see Proposition 3.6) and the rest form orbits of length 6.

If $p \equiv 19 \pmod{36}$ then, by Proposition 4.2, all of the $\Sigma(p)$-orbits have length 6. As there are $2 + 2|A_1 \cap A_2|$ basic elements, the number of $\Sigma(p)$-orbits is $\eta(p) = (1 + |A_1 \cap A_2|)/3$. If $p \not\equiv 19 \pmod{36}$ then there is one $\Sigma(p)$-orbit of length 2, and $\eta(p) = 1 + |A_1 \cap A_2|/3$.

Using Lemma 4.4 and a little number theory, we can now get a good estimate for $\eta(p)$.

<u>Theorem 4.5</u> Let p be prime, $p \equiv 7 \pmod{12}$, and let b and c be integers such that $4p = c^2 + 27b^2$ and $c \equiv 1 \pmod 3$.

Then:

1. $\eta(p) = \begin{cases} (p + c + 1)/27 & \text{if } p \equiv 19 \pmod{36} \\ (p + c + 19)/27 & \text{if } p \equiv 7 \text{ or } 31 \pmod{36} \end{cases}$

2. $\left(\sqrt{p} - 1\right)^2/27 < \eta(p) < 1 + \left(\sqrt{p} + 1\right)^2/27$

3. $\lim_{p\to\infty} \eta(p) = \infty$

<u>Proof</u> By [17; part I, Lemma 7], there exists a unique pair of integers b and c (except that the sign of b is ambiguous) such that $4p = c^2 + 27b^2$ and $c \equiv 1 \pmod 3$, and furthermore $|A_1 \cap A_2| = (p + c - 8)/9$. Thus by Lemma 4.4, result 1 holds.

As $b \neq 0$, we have $c^2 < 4p$ and $-2\sqrt{p} < c < 2\sqrt{p}$. Therefore $(\sqrt{p} - 1)^2 < p + c + 1 < (\sqrt{p} + 1)^2$ and result 2 holds. Finally, result 3 follows directly from 2.

For appropriate primes less than 300, $\eta(p)$ is tabulated in Table I. The appearance of PG(2,2) and PG(4,2) as block-regular systems in this table does not indicate anything more general, as the following result shows.

<u>Proposition 4.6</u> No EG(n,3) is block-regular. If PG(n,2) is block-regular then n = 2 or n = 4.

<u>Proof</u> EG(n,3) has 3^n points, and $3^n \not\equiv 7 \pmod{12}$. If PG(n,2) is block-regular then $2^{n+1} - 1$ is a prime power by Theorem 3.4, and this must be a Mersenne prime $p = 2^q - 1$.

p	c	b	$\eta(p)$	Netto systems	Non-Netto systems	
7	1	1	1	1*		*PG(2,2)
19	7	1	1		1	
31	4	2	2	1	1**	**PG(4,2)
43	-8	2	2	1	1	
67	-5	3	3	1	2	
79	-17	1	3	1	2	
103	13	3	5	1	4	
127	-20	2	4		4	
139	-23	1	5	1	4	
151	19	3	7	1	6	
163	25	1	7		7	
199	-11	5	7		7	
211	-14	5	7	1	6	
223	28	2	10	1	9	
271	-29	3	9		9	
283	-32	2	10	1	9	

TABLE I

But the normalizer in $GL(q,2)$ of a Sylow p-group is of order pq, so we must have $(p - 1)/6 | q | p - 1$. If $q = p - 1$ then $q = 2$, if $q = (p - 1)/2$ then $q = 3$, and if $q = (p - 1)/6$ then $q = 5$. These correspond to $n = 1$, 2, and 4 respectively.

5. Corollaries of the Main Theorem

Let (V,B) be a Steiner triple system with an automorphism group G acting doubly transitively on V. The only such systems known are $EG(n,3)$ and $PG(n,2)$, where $n \geq 2$. They have the property that every subsystem is of the form $EG(k,3)$ or $PG(k,2)$, respectively, for $2 \leq k \leq n$, and therefore every subsystem has a doubly transitive automorphism group. In this chapter we will prove a limited version of this property, namely that the subsystems of (V,B) formed by the fixed points of certain subgroups of G have doubly transitive automorphism groups.

If p is a prime and $K \leq G$, define

$$Y_p(K) = \{U \leq K \mid U \text{ is a p-group, } |F(U)| > 3\}$$

Let $Y_p^*(K)$ be the set of maximal elements of $Y_p(K)$. Then if $U \epsilon Y_p^*(K)$ and $U < U_1 \leq K$, where U_1 is a p-group, it must follow that $|F(U_1)| \leq 3$.

Theorem 5.1 If p is an odd prime and $U \epsilon Y_p^*(G_{xy})$, then $N_G(U)$ acts transitively on $B|_{F(U)}$. Furthermore, one of the following two cases holds:

1. $N_G(U)^{F(U)}$ is doubly transitive;
2. $\left(F(U), B|_{F(U)}\right) \cong EG(p,3)$ and $N_G(U)^{F(U)} \cong O(\Sigma(3^p))$.

<u>Proof</u> Define $H = G_x$ and $J = G_{xy}$, and let $\{x,y,z\} \in B$. Also define $J^* = H_{(\{y,z\})}$. If $U \in Syl_p(J)$ then $N_G(U)^{F(U)}$ is doubly transitive by Lemma 2.8, so we may assume that $U < P \in Syl_p(N_J(U))$. By maximality of U, $F(P) = \{x,y,z\}$, so $N_H(P) \leq J^*$.

Suppose $P \notin Syl_p(N_H(U))$. Then $P < N_Q(P) \leq Q \in Syl_p(N_H(U))$ and $P < N_Q(P) \leq N_H(P) \leq J^*$. As p is odd and $|J^* : J| = 2$, we have $N_Q(P) \leq J$ and $P < N_Q(P) \leq N_J(U)$, which contradicts the assumption that $P \in Syl_p(N_J(U))$. Therefore $P \in Syl_p(N_H(U))$.

Let $h \in H$, $U^h \leq J$, and let $S \in Syl_p\left(N_G(U) \cap J^{h^{-1}}\right)$. Since $N_G(U) \cap J^{h^{-1}} \leq N_H(U)$, there exists $k \in N_H(U)$ such that $S^k \leq P$. Also $U \leq O_p\left(N_G(U) \cap J^{h^{-1}}\right) \leq S$, so $U = U^k \leq S^k \leq P$. If $U = S^k$ then $U = S$ and $U^h \in Syl_p\left(N_J(U^h)\right)$. But this implies that $N_G(U^h)^{F(U^h)}$, and hence $N_G(U)^{F(U)}$, is doubly transitive by Lemma 2.8. So we may assume that $U < S^k$. Then by maximality of U, $F(S^k) = \{x,y,z\}$. But $S \leq J^{h^{-1}}$, so we have

$$F(S) = \left\{x, y^{h^{-1}}, z^{h^{-1}}\right\} = \left\{x, y^{k^{-1}}, z^{k^{-1}}\right\}$$

Therefore $N_H(U)$ acts transitively on $B(x)|_{F(U)}$.

Similarly, $N_{G_y}(U)$ and $N_{G_z}(U)$ act transitively on $B(y)|_{F(U)}$ and $B(z)|_{F(U)}$, respectively. Let $\{r,s,t\} \in B|_{F(U)}$. If $r = x$, there exists $g \in N_H(U)$ such that $\{r,s,t\}^g = \{x,y,z\}$. Otherwise, there exists $g \in N_H(U)$ such that $r^g = y$ or $r^g = z$. Without loss of generality, say $r^g = y$. Then $\{r,s,t\}^g = \{y,s_1,t_1\} \in B(y)|_{F(U)}$ and there exists $g_1 \in N_{G_y}(U)$

such that $\{r,s,t\}^{gg_1} = \{x,y,z\}$. Hence $N_G(U)$ acts transitively on $B|_{F(U)}$.

Suppose that $N_G(U)^{F(U)}$ is not doubly transitive. Then we may assume that $U < Q \leq N_J(U)$, where $|Q : U| = p$ and $|F(Q)| = 3$. By Theorem 3.4, $N_G(U)^{F(U)} \leq \Sigma(q^d)$ and $F(U)$ may be identified with $GF(q^d)$. Now (choosing $x = 0$ and $y = 1$) $N_J(U)^{F(U)}$ is a subgroup of $\mathrm{Aut}(GF(q^d))$; in particular, $F(Q) = GF\left(q^{d/p}\right)$. Hence $q = 3$ and $d = p$. This is conclusion 2a of Theorem 3.4, so case 2 holds and the proof is complete.

When $p = 2$, the situation is more complicated. However, the list of possible groups $N_G(U)^{F(U)}$ which are not doubly transitive is finite.

<u>Theorem 5.2</u> Let $U \in Y_2^*(G)$ and define $F = F(U)$, $N = N_G(U)$, and $D = B|_F$. Then one of the following seven cases occurs:

1. N^F is doubly transitive;
2. $(F,D) \cong PG(2,2)$ and $N^F \cong S_4$ is the stabilizer of a block in $\mathrm{Aut}PG(2,2)$;
3. $(F,D) \cong EG(2,3)$ and $N^F \cong E(9)*D_8$;
4. $(F,D) \cong EG(2,3)$ and N^F is the subgroup of $\mathrm{Aut}EG(2,3)$ which stabilizes a set of three parallel lines;
5. $(F,D) \cong PG(3,2)$ and N^F is the subgroup of $\mathrm{Aut}PG(3,2)$ which stabilizes a set of five disjoint blocks;
6. $(F,D) \cong EG(3,3)$ and N^F is contained in the subgroup of $\mathrm{Aut}EG(3,3)$ which stabilizes a set of three

parallel planes;

7. $(F,D) \cong EG(3,3)$ and N^F is contained in the subgroup of AutEG(3,3) which stabilizes a set of nine parallel lines.

Proof Let $\{x,y,z\} \in D$. If $U \in Syl_2(D)$ then N^F is doubly transitive by Lemma 2.8. So for every block $\beta \in D$, we may assume that there is a 2-group $P \leq N$ with $F(P) = \beta$. Also, $P^{F-\beta}$ must be semiregular by the maximality of U, so for every $\beta \in D$ there is an involution $g \in N$ with $F(g) = \beta$. Thus we are considering Steiner triple systems which satisfy the hypothesis of Lemma 2.3.

Suppose that all involutions of N which fix three points are conjugate in N. If $\beta_1, \beta_2 \in D$ then there exist involutions $g_1, g_2 \in N$ with $F(g_i) = \beta_i$. As $g_1^n = g_2$ for some $n \in N$, $\beta_1^n = \beta_2$, so N^D is transitive. Now Theorem 3.4 implies that N^F is doubly transitive, since $|N^F|$ is even. We may therefore assume that N has at least two classes of involutions fixing three points.

First let us assume that N_x acts transitively on D(x). Then either $N_x^{F-\{x\}}$ is transitive, in which case N^F is doubly transitive, or it has two orbits of equal size. In the latter case, either N^F is primitive of rank 3 or it has two orbits Γ and Δ. In the primitive rank-3 case, the only possibility from Lemma 2.11 is $N^F = E(9)*D_8$, which fails to satisfy the hypothesis that $N_x^{D(x)}$ is transitive.

So N^F has two orbits, Γ and Δ, such that $x\epsilon\Gamma$ and $|\Gamma| = |\Delta| + 1$. Also, N^Γ is doubly transitive. If $\{x,y,z\}\epsilon D$ and $y\epsilon\Gamma$ then $z\epsilon\Delta$, so an involution in N^Γ fixes 0 or 2 points. By [9], either $N^\Gamma = A_6$ or $|\Gamma| = q + 1$ and $PSL(2,q) \leq N \leq P\Gamma L(2,q)$. But A_6 cannot be represented faithfully on 5 points, so $PSL(2,q) \leq N$ and N^Δ is transitive of degree q. Inspecting the character tables of $PSL(2,q)$, q odd [16], for a possible permutation character of degree q, we see that either $q = 3$ or $PSL(2,q)^\Delta$ is doubly transitive. Thus $q\epsilon\{3,5,7,11\}$ by Lemma 2.10. But $PSL(2,q)$ has only one class of involutions, so $N \cong PGL(2,q)$ and $q = 3$ or 5. If $q = 5$ then $|F| = 11$, which is impossible, so $q = 3$, $|F| = 7$, and $N \cong PGL(2,3) \cong S_4$. This yields case 2 of the theorem.

From now on we may assume that $N_t^{D(t)}$ is intransitive for every $t\epsilon F$. We will first prove that N^F is transitive: let $x,y\epsilon F$ and $\{x,y,z\}\epsilon D$. If $P\epsilon Syl_2(N_{yz})$ then $F(P) = \{x,y,z\}$. If also $P\epsilon Syl_2(N_z)$, then the argument used in Theorem 4.1 shows that $N_z^{D(z)}$ is transitive, so $P < N_Q(P) \leq Q\epsilon Syl_2(N_z)$. But now any element of $N_Q(P) - P$ must interchange x and y, so N^F is transitive.

By Lemma 2.9, there exists a block $\alpha\epsilon D(x)$ such that every 2-group $P \leq N_x$ which fixes α fixes another block in $D(x)$. Let $\alpha = \{x,y,z\}$; then $P\epsilon Syl_2(N_{xy})$ is semiregular on $F - \alpha$. Now P fixes another block $\{x,t,u\}\epsilon D(x)$, so $|P| = 2$

and $P = \langle g \rangle$, where $g = (x)(y)(z)(t\ u)\cdots$ Also $P < N_Q(P) \leq Q \in Syl_2(N_x)$ as in the previous paragraph, so $\{y,z\}$ is an orbit of $N_Q(P) = C_Q(x)$. Therefore $|C_Q(x)| = 2|P| = 4$ and by Lemma 2.6, $Q \cong D_n$ or SD_n. Note that $Q \in Syl_2(N)$, since $F(Q) = \{x\}$.

It follows that N has at most three classes of involutions, and so N^D has at most three orbits. Now, the fact that $N_{(\beta)}^{\beta} = S_3$ for any $\beta \in D$ implies that the N-orbits in D are in one-to-one correspondence with the N-orbits of ordered pairs of distinct points of F. But the latter correspond exactly to the orbits of N_x other than $\{x\}$. Hence N^F has rank at most 4, and the rank equals 4 only if N has three classes of involutions. If N^F is primitive then Lemma 2.11 gives $N^F = E(9)*D_8$, which is case 3. So we may assume that N^F is imprimitive.

Let Γ be a minimal set of imprimitivity for N^F, and let $x \in \Gamma$. Assume for the moment that $|\Gamma| > 3$. Then clearly $(\Gamma, D|_\Gamma)$ is a subsystem of (F,D): if $y,z \in \Gamma$ then there is an involution $g \in N$ with $F(g) = \{y,z,w\} \in D$. But $\Gamma^g = \Gamma$ and $|\Gamma|$ is odd, so $w \in \Gamma$. Similarly, if $y \in \Gamma$ and $z \notin \Gamma$ then $w \notin \Gamma$. Therefore $N_{(\Gamma)}^{\Gamma}$ is a primitive permutation group, with involutions fixing one or three points but no more, which acts on a Steiner triple system. By Lemma 2.11, $N_{(\Gamma)}^{\Gamma} = E(9)*W$, where $W = D_8, SD_{16}$, or $GL(2,3)$. In particular, $|\Gamma| = 9$ and $N_x^{\Gamma - \{x\}} = W$. Let $\Delta = F - \Gamma$. If $W = D_8$

then $N^{\Gamma}_{(\Gamma)}$ has rank 3, so N^{Δ}_{x} is transitive. Otherwise, N has only two classes of involutions, so N^{F} has rank 3 and again N^{Δ}_{x} is transitive. But 9 divides $|\Delta|$, whereas it does not divide $|W|$, so $K = N_{\Gamma}$ is nontrivial (and of odd order). As $K \lhd N_x$, K^{Δ} is 1/2-transitive. Let $g \in Z(W)^{\#}$; then $L = \langle K, g \rangle \lhd N_x$, so L^{Δ} is also 1/2-transitive. Now g fixes exactly 2 points in Δ, whence it follows that K^{Δ} and L^{Δ} have the same orbits. Furthermore, since $|K|$ is odd, g fixes a point in every K^{Δ}-orbit. Therefore K^{Δ} has exactly two orbits, Δ_1 and Δ_2.

Let C be the system of imprimitivity containing Γ, and let $\Gamma_1 \in C - \{\Gamma\}$. Then $\Gamma_1 \subseteq \Delta$. If $\Delta_i \cap \Gamma_1$ is non-empty then $L_{(\Gamma_1)}$ acts transitively on it, since it is a set of imprimitivity for L^{Δ_i}. Since for any $y \in \Delta_i$ there exists an involution $h \in L$ with $F(h) \cap \Delta_i = \{y\}$, it follows that $|\Delta_i \cap \Gamma_1|$ is odd or zero. But now as $|\Gamma_1| = 9$ and $\Gamma_1 \subseteq \Delta_1 \cup \Delta_2$, either $\Gamma_1 \subseteq \Delta_1$ or $\Gamma_1 \subseteq \Delta_2$. Also, g has one fixed point in Δ_1 and one in Δ_2, and it permutes the elements of $C - \{\Gamma\}$, so $|\Delta_1| = |\Delta_2| \equiv 9 \pmod{18}$. Hence $|F| = 9 + |\Delta_1| + |\Delta_2| \equiv 27 \pmod{36}$ and $|C| = |F|/9 \equiv 3 \pmod 4$. If $|C| > 3$ then N^{C} contains involutions fixing both one and three points (i.e., elements of C) but no more, and N^{C} is doubly transitive since N^{Δ}_{x} is transitive. Thus Lemma 2.11 implies that $|C| = 5$ or 9. But then $|C| \equiv 1 \pmod 4$, a contradiction, so $|C| = 3$ and $|F| = 27$. Applying

Lemmas 2.3 and 2.4, together with the fact that $(\Gamma, D|_\Gamma)$ has nine points, we see that $(F,D) \cong EG(3,3)$, and clearly N is a group of the kind described in case 6 of the theorem.

We must now consider the case where $|\Gamma| = 3$. Evidently $\Gamma \epsilon D$. As before, let C be the system of imprimitivity containing Γ. Then either $|C| = 3$ or N^C contains involutions fixing both one and three points, but no more. Assume that N_C is primitive; then by Lemma 2.11, $|C| \epsilon \{3,5,9\}$.

First case: $|C| = 3$ and $|F| = 9$. Here it is clear that $(F,D) \cong EG(2,3)$ and $N \leq N_4$, the group described in case 4 of the theorem. N_4 is the normalizer in $E(9)*GL(2,3)$ of a cyclic subgroup of the regular normal $E(9)$; since there are 4 such subgroups, $|E(9)*GL(2,3) : N_4| = 4$ and $|N_4| = 108$. A Sylow 2-group of N must be of order 4 (since otherwise Sylow's theorem would imply that N had only one class of involutions), and hence must be a Sylow 2-group of N_4. But N_4 contains an involution fixing only one point, so N has two classes of involutions which fix three points. Thus N^F has rank 3, and its subdegrees are those of N_4^F, namely $1 + 2 + 6$, so both 4 and 54 divide $|N|$. Therefore $N = N_4$.

Second case: $|C| = 5$ and $|F| = 15$. By Lemma 2.2, (F,D) cannot contain a subsystem with nine points, so Lemmas 2.3 and 2.5 imply that $(F,D) \cong PG(3,2)$. Now by

Lemma 2.11, $N^C \cong S_5$. If $N \cong S_5$ then it has two classes of involutions, so N^F has rank 3 and subdegrees 1 + 2 + 12. But this is impossible, since $|N_x| = 8$. As involutions fix no more than three points, N_C must therefore be a nontrivial 3-group, and in fact $|N_C| = 3$ because $|GL(4,2)| = 168|S_5|$. Clearly $N \leq N_5$, the group described in case 5 of the theorem, and it is not hard to see that the only elements of GL(4,2) which stabilize all five blocks of C are in N_C. Therefore $N = N_5$.

Third case: $|C| = 9$, $|F| = 27$. By Lemma 2.3, either every triangle of (F,D) generates a subsystem isomorphic to PG(2,2) or every triangle generates a subsystem isomorphic to EG(2,3). In the former case, $(F,D) \cong PG(n,2)$ for some n by Lemma 2.5. But $27 \neq 2^{n+1} - 1$, so the latter case holds, and $(F,D) \cong EG(3,3)$ by Lemma 2.4. As every set of imprimitivity in C is a block in D, N is a group of the type described in case 7 of the theorem.

We have now eliminated every possibility except the following situation: N^F has two sets of imprimitivity Γ and Δ where $\Gamma \subseteq \Delta$, $|\Gamma| = 3$, and $|\Delta| > 3$. Let the corresponding systems of imprimitivity be C and E, respectively. Then N^C and $N^{\Delta}_{(\Delta)}$ are both imprimitive and have rank 3, N^F has rank 4, and N^E is doubly transitive. Also, if C* is the set of elements of C which are contained in Δ, then $N_{(\Delta)}$ acts doubly transitively on C*.

By the same argument as before, $|C^*|$ and $|C|$ are 3,5, or 9. If either is 9 then N involves SD_{16}; but N has at least three classes of involutions, so its Sylow 2-groups are dihedral. Hence $|C^*|$, $|E| \in \{3,5\}$ and $|F| = 3|C| = 3|C^*||E| \in \{27,45,75\}$.

First case: $|F| = 45$. Here N^F has for subdegrees either $1 + 2 + 6 + 36$ or $1 + 2 + 12 + 30$. Let $Q \in Syl_2(N)$; as $30 \equiv 6 \equiv 2 \pmod 4$, Q must have at least two orbits of length 2. This implies that $|Q| \leq 4$. But N involves S_5, so $|Q| \geq 8$ and we have a contradiction.

Second case: $|F| = 75$. Here $N^E = S_5$ and N_E is normal in N and of odd order, so $N/O(N) \cong S_5$. Thus N has only two classes of involutions, which is a contradiction.

Last case: $|F| = 27$. By the same argument as before, $(F,D) \cong EG(3,3)$. Clearly Γ and Δ correspond to a line and a plane, respectively, so N satisfies both case 6 and case 7. This completes the proof of Theorem 5.2.

In view of the fact that PG(n,2) and EG(n,3) both have doubly transitive automorphism groups, Theorems 5.1 and 5.2 can be combined to yield the following result.

Corollary 5.3 Let p be a prime and let $U \in Y_p^*(G)$. Then $\left(F(U), B|_{F(U)}\right)$ has a doubly transitive automorphism group.

REFERENCES

[1] G. D. Birkhoff and H. S. Vandiver, On the Integral Divisors of $a^n - b^n$, Ann. of Math. (2nd Series) 5 (1904), 173-180.

[2] F. Buekenhout, Transitive Groups in Which Involutions Fix One or Three Points, J. Alg. 23 (1972), 438-451.

[3] P. Dembowski, Finite Geometries, Springer, New York, 1968.

[4] J. Doyen, Systèmes Triples de Steiner non Engendrés Par Tous Leurs Triangles, Math. Z. 118 (1970), 197-206.

[5] W. Feit and J. G. Thompson, Solvability of Groups of Odd Order, Pac. J. Math. 13 (1963), 775-1029.

[6] D. Gorenstein, Finite Groups, Harper and Row, New York, 1968.

[7] J. Hall, Steiner Triple Systems and 2-Transitive Groups, to appear in Quart. J. Math. Oxford.

[8] M. Hall, Jr., Automorphisms of Steiner Triple Systems, Proc. Sympos. Pure Math. VI, Amer. Math. Soc., Providence (1962), 47-66.

[9] C. Hering, Zweifach Transitive Permutationsgruppen, in Denen 2 Die Maximale Anzahl von Fixpunkten von Involutionen ist, Math. Z. 104 (1968), 150-174.

[10] D. G. Higman, Intersection Matrices for Finite Permutation Groups, J. Alg. 6 (1967), 22-42.

[11] H. Lüneburg, Steinersche Tripelsysteme mit Fahnentransitiven Kollineationsgruppe, Math. Ann. 149 (1963), 261-270.

[12] H. Lüneburg, Charakterisierungen der Endlichen Desarguesschen Projektiven Ebenen, Math. Z. 85 (1964), 419-450.

[13] E. Netto, Zur Theorie der Tripelsysteme, Math. Ann. 42 (1893), 143-152.

[14] D. Passman, Permutation Groups, Benjamin, New York, 1968.

[15] D. Passman, Exceptional 3/2-Transitive Permutation Groups, Pac. J. Math. 29 (1969), 669-713.

[16] J. Schur, Untersuchung über die Darstellung der Endlichen Gruppen Durch Gebrochene Lineare Substitutionen, J. fur Math. 132 (1907), 85-137.

[17] T. Storer, Cyclotomy and Difference Sets, Markham, Chicago, 1967.

[18] M. Suzuki, A Characterisation of Simple Groups LF(2,p). J. Fac. Sci. Univ. Tokyo, Sect. I, 6 (1951), 259-293.

[19] H. Wielandt, Finite Permutation Groups, Academic Press, New York, 1964.

[20] E. Witt, Die 5-Fach Transitiven Gruppen von Mathieu, Abh. Math. Sem. Univ. Hamburg 12 (1937), 256-264.