(1 2 ... 10 11); if $\tau = (1\ 11)(2\ 10)(3\ 9)(4\ 8)(5\ 7)$, then τ is an involution with $\tau\sigma\tau = \sigma^{-1}$ and $\tau \in N_{S_{11}}(P)$. But τ is an odd permutation, whereas $M_{11} \le A_{11}$, so that $|N_{M_{11}}(P)| = 11$ or 55. Now $P \le N_H(P) \le N_{M_{11}}(P)$, so that either $P = N_H(P)$ or $N_H(P) = N_{M_{11}}(P)$. The first paragraph eliminated the first possibility, and so $N_H(P) = N_{M_{11}}(P)$ (and their common order is 55). The Frattini argument now gives $M_{11} = HN_{M_{11}}(P) = HN_H(P) = H$ (for $N_H(P) \le H$), and so M_{11} is simple. ∎

EXERCISES

9.37. Show that the 4-group V has no transitive extension. (*Hint.* If $h \in S_5$ has order 5, then $\langle \mathbf{V}, h\rangle \ge A_5$.)

9.38. Let $W = \{g \in M_{12}: g \text{ permutes } \{\infty, \omega\ \Omega\}\}$. Show that there is a homomorphism of W onto S_3 with kernel $(M_{12})_{\infty,\omega,\Omega}$. Conclude that $|W| = 6 \times 72$.

9.39. Prove that Aut(2, 3), the group of all affine automorphisms of a two-dimensional vector space over $\mathbb{Z}_3$, is isomorphic to the subgroup W of M_{12} in the previous exercise. (*Hint.* Regard GF(9) as a vector space over $\mathbb{Z}_3$.)

9.40. Show that $\langle \mathrm{PSL}(3, 4), h_2, h_3\rangle \le M_{24}$ is isomorphic to $\mathrm{P\Gamma L}(3, 4)$. (*Hint.* Lemma 9.54.)

Steiner Systems

A Steiner system, defined below, is a set together with a family of subsets which can be thought of as generalized lines; it can thus be viewed as a kind of geometry, generalizing the notion of affine space, for example. If X is a set with $|X| = v$, and if $k \le v$, then a ***k-subset*** of X is a subset $B \subset X$ with $|B| = k$.

Definition. Let $1 < t < k < v$ be integers. A ***Steiner system*** of ***type*** $S(t, k, v)$ is an ordered pair $(X, \mathscr{B})$, where X is a set with v elements, $\mathscr{B}$ is a family of k-subsets of X, called ***blocks***, such that every t elements of X lie in a unique block.

EXAMPLE 9.12. Let X be an affine plane over the field GF(q), and let $\mathscr{B}$ be the family of all affine lines in X. Then every line has q points and every two points determine a unique line, so that $(X, \mathscr{B})$ is a Steiner system of type $S(2, q, q^2)$.

EXAMPLE 9.13. Let $X = \mathrm{P}^2(q)$ and let $\mathscr{B}$ be the family of all projective lines in X. Then every line has $q + 1$ points and every two points determine a unique line, so that $(X, \mathscr{B})$ is a Steiner system of type $S(2, q + 1, q^2 + q + 1)$.

EXAMPLE 9.14. Let X be an m-dimensional vector space over $\mathbb{Z}_2$, where $m \ge 3$, and let $\mathscr{B}$ be the family of all planes (affine 2-subsets of X). Since three distinct points cannot be collinear, it is easy to see that $(X, \mathscr{B})$ is a Steiner system of type $S(3, 4, 2^m)$.

One assumes strict inequalities $1 < t < k < v$ to eliminate uninteresting cases. If $t = 1$, every point lies in a unique block, and so X is just a set partitioned into k-subsets; if $t = k$, then every t-subset is a block; if $k = v$, then there is only one block. In the first case, all "lines" (blocks) are parallel; in the second case, there are too many blocks; in the third case, there are too few blocks.

Given parameters $1 < t < k < v$, it is an open problem whether there exists a Steiner system of type $S(t, k, v)$. For example, one defines a ***projective plane of order n*** to be a Steiner system of type $S(2, n + 1, n^2 + n + 1)$. It is conjectured that n must be a prime power, but it is still unknown whether there exists a projective plane of order 12. (There is a theorem of Bruck and Ryser (1949) saying that if $n \equiv 1$ or 2 mod 4 and n is not a sum of two squares, then there is no projective plane of order n; note that $n = 10$ is the first integer which neither satisfies this hypothesis nor is a prime power. In 1988, C. Lam proved, using massive amounts of computer time, that there is no projective plane of order 10.)

Definition. If $(X, \mathscr{B})$ is a Steiner system and $x \in X$, then

$$\textbf{\textit{star}}(x) = \{B \in \mathscr{B}: x \in \mathscr{B}\}.$$

Theorem 9.60. *Let $(X, \mathscr{B})$ be a Steiner system of type $S(t, k, v)$, where $t \ge 3$. If $x \in X$, define $X' = X - \{x\}$ and $\mathscr{B}' = \{B - \{x\}: B \in \mathrm{star}(x)\}$. Then $(X', \mathscr{B}')$ is a Steiner system of type $S(t - 1, k - 1, v - 1)$ (called the* **contraction** *of $(X, \mathscr{B})$* ***at*** *x).*

Proof. The routine proof is left to the reader. ∎

A contraction of $(X, \mathscr{B})$ may depend on the point x.

Let Y and Z be finite sets, and let $W \subset Y \times Z$. For each $y \in Y$, define $\#(y, \ ) = |\{z \in Z: (y, z) \in W\}|$ and define $\#(\ , z) = |\{y \in Y: (y, z) \in W\}|$. Clearly,

$$\sum_{y \in Y} \#(y, \ ) = |W| = \sum_{z \in Z} \#(\ , z).$$

We deduce a ***counting principle***: If $\#(y, \ ) = m$ for all $y \in Y$ and if $\#(\ , z) = n$ for all $z \in Z$, then

$$m|Y| = n|Z|.$$

Theorem 9.61. *Let $(X, \mathscr{B})$ be a Steiner system of type $S(t, k, v)$. Then the number of blocks is*

$$|\mathscr{B}| = \frac{v(v-1)(v-2)\dots(v-t+1)}{k(k-1)(k-2)\dots(k-t+1)};$$

if r is the number of blocks containing a point $x \in X$, then r is independent of x

and

$$r = \frac{(v-1)(v-2)\cdots(v-t+1)}{(k-1)(k-2)\cdots(k-t+1)}.$$

Proof. If Y is the family of all t-subsets of X, then $|Y| =$ "v choose t" $= v(v-1)\cdots(v-t+1)/t!$. Define $W \subset Y \times \mathscr{B}$ to consist of all $(\{x_1, \ldots, x_t\}, B)$ with $\{x_1, \ldots, x_t\} \subset B$. Since every t-subset lies in a unique block, $\#(\{x_1, \ldots, x_t\}, \ ) = 1$; since each block B is a k-subset, $\#(\ , B) =$ "k choose t" $= k(k-1)\cdots(k-t+1)/t!$. The counting principle now gives the desired formula for $|\mathscr{B}|$.

The formula for r follows from that for $|\mathscr{B}|$ because r is the number of blocks in the contraction $(X', \mathscr{B}')$ (where $X' = X - \{x\}$), which is a Steiner system of type $S(t-1, k-1, v-1)$. It follows that r does not depend on the choice of x. ∎

Remarks. 1. The proof just given holds for all $t \geq 2$ (of course, $(X', \mathscr{B}')$ is not a Steiner system when $t = 2$ since $t - 1 = 1$).

2. The same proof gives a formula for the number of blocks in a Steiner system of type $S(t, k, v)$ containing two points x and y. If $(X', \mathscr{B}')$ is the contraction (with $X' = X - \{x\}$), then the number r' of blocks in $(X', \mathscr{B}')$ containing y is the same as the number of blocks in $(X, \mathscr{B})$ containing x and y. Therefore,

$$r' = \frac{(v-2)(v-3)\cdots(v-t+1)}{(k-2)(k-3)\cdots(k-t+1)}.$$

Similarly, the number $r^{(p)}$ of blocks in $(X, \mathscr{B})$ containing p points, where $1 \leq p \leq t$, is

$$r^{(p)} = \frac{(v-p)(v-p-1)\cdots(v-t+1)}{(k-p)(k-p-1)\cdots(k-t+1)}.$$

3. That the numbers $|\mathscr{B}| = r, r', \ldots r^{(p)}, \ldots, r^{(t)}$ are integers is, of course, a constraint on t, k, v.

Definition. If $(X, \mathscr{B})$ and $(Y, \mathscr{C})$ are Steiner systems, then an ***isomorphism*** is a bijection $f\colon X \to Y$ such that $B \in \mathscr{B}$ if and only if $f(B) \in \mathscr{C}$. If $(X, \mathscr{B}) = (Y, \mathscr{C})$, then f is called an ***automorphism***.

For certain parameters t, k, and v, there is a unique, to isomorphism, Steiner system of type $S(t, k, v)$, but there may exist nonisomorphic Steiner systems of the same type. For example, it is known that there are exactly four projective planes of order 9; that is, there are exactly four Steiner systems of type $S(2, 10, 91)$.

Theorem 9.62. *All the automorphisms of a Steiner system $(X, \mathscr{B})$ form a group* $\mathrm{Aut}(X, \mathscr{B}) \leq S_X$.

Proof. The only point needing discussion is whether the inverse of an automorphism h is itself an automorphism. But S_X is finite, and so $h^{-1} = h^m$ for some $m \geq 1$. The result follows, for it is obvious that the composite of automorphisms is an automorphism. ∎

Theorem 9.63. *If $(X, \mathscr{B})$ is a Steiner system, then* $\mathrm{Aut}(X, \mathscr{B})$ *acts faithfully on* $\mathscr{B}$.

Proof. If $\varphi \in \mathrm{Aut}(X, \mathscr{B})$ and $\varphi(B) = B$ for all blocks B, then it must be shown that $\varphi = 1_X$.

For $x \in X$, let $r = |\mathrm{star}(x)|$, the number of blocks containing x. Since φ is an automorphism, $\varphi(\mathrm{star}(x)) = \mathrm{star}(\varphi(x))$; since φ fixes every block, $\varphi(\mathrm{star}(x)) = \mathrm{star}(x)$, so that $\mathrm{star}(x) = \mathrm{star}(\varphi(x))$. Thus, $\varphi(x)$ and x lie in exactly the same blocks, and so the number r' of blocks containing $\{\varphi(x), x\}$ is the same as the number r of blocks containing x. If $\varphi(x) \neq x$, however, $r' = r$ gives $k = v$ (using the formulas in Theorem 9.61 and the remark thereafter), contradicting $k < v$. Therefore, $\varphi(x) = x$ for all $x \in X$. ∎

Corollary 9.64. *If $(X, \mathscr{B})$ is a Steiner system and $x \in X$, then* $\bigcap_{B \in \mathrm{star}(x)} B = \{x\}$.

Proof. Let $x, y \in X$. If $\mathrm{star}(x) = \mathrm{star}(y)$, then the argument above gives the contradiction $r' = r$. Therefore, if $y \neq x$, there is a block B with $x \in B$ and $y \notin B$, so that $y \notin \bigcap_{B \in \mathrm{star}(x)} B$. ∎

We are going to see that multiply transitive groups may determine Steiner systems.

Notation. If X is a G-set and $U \leq G$ is a subgroup, then

$$\mathscr{F}(U) = \{x \in X\colon gx = x \text{ for all } g \in U\}.$$

Recall that if $U \leq G$ and $g \in G$, then the conjugate gUg^{-1} may be denoted by U^g.

Lemma 9.65. *If X is a G-set and $U \leq G$ is a subgroup, then*

$$\mathscr{F}(U^g) = g\mathscr{F}(U) \qquad \text{for all} \quad g \in G.$$

Proof. The following statements are equivalent for $x \in X\colon x \in \mathscr{F}(U^g)$; $gug^{-1}(x) = x$ for all $u \in U$; $ug^{-1}(x) = g^{-1}(x)$ for all $u \in U$; $g^{-1}(x) \in \mathscr{F}(U)$; $x \in g\mathscr{F}(U)$. ∎

Theorem 9.66. *Let X be a faithful t-transitive G-set, where $t \geq 2$, let H be the stabilizer of t points $x_1, \ldots, x_t$ in X, and let U be a Sylow p-subgroup of H for some prime p.*

(i) $N_G(U)$ *acts t-transitively on* $\mathscr{F}(U)$.
(ii) (**Carmichael, 1931; Witt, 1938**). *If* $k = |\mathscr{F}(U)| > t$ *and U is a nontrivial normal subgroup of H, then* $(X, \mathscr{B})$ *is a Steiner system of type* $S(t, k, v)$, *where* $|X| = v$ *and*

$$\mathscr{B} = \{g\mathscr{F}(U): g \in G\} = \{\mathscr{F}(U^g): g \in G\}.$$

Proof. (i) Note that $\mathscr{F}(U)$ is a $N_G(U)$-set: if $g \in N_G(U)$, then $U = U^g$ and $\mathscr{F}(U) = \mathscr{F}(U^g) = g\mathscr{F}(U)$. Now $\{x_1, \ldots, x_t\} \subset \mathscr{F}(U)$ because $U \leq H$, the stabilizer of $x_1, \ldots, x_t$; hence $k = |\mathscr{F}(U)| \geq t$. If $y_1, \ldots, y_t$ are distinct elements of $\mathscr{F}(U)$, then t-transitivity of G gives $g \in G$ with $gy_i = x_i$ for all i. If $u \in U$, then $gug^{-1}x_i = guy_i = gy_i = x_i$ (because $y_i \in \mathscr{F}(U)$); that is, $U^g \leq H$. By the Sylow theorem, there exists $h \in H$ with $U^g = U^h$. Therefore $h^{-1}g \in N_G(U)$ and $(h^{-1}g)y_i = h^{-1}x_i = x_i$ for all i.

(ii) The hypothesis gives $1 < t < k \leq v$. If $k = v$, then $\mathscr{F}(U) = X$; but $U \neq 1$, contradicting G acting faithfully on X. It is also clear that $k = |\mathscr{F}(U)| = |g\mathscr{F}(U)|$ for all $g \in G$.

If $y_1, \ldots, y_t$ are distinct elements of X, then there is $g \in G$ with $gx_i = y_i$ for all i, and so $\{y_1, \ldots, y_t\} \subset g\mathscr{F}(U)$. It remains to show that $g\mathscr{F}(U)$ is the unique block containing the y_i. If $\{y_1, \ldots, y_t\} \subset h\mathscr{F}(U)$, then there are $z_1, \ldots, z_t \in \mathscr{F}(U)$ with $y_i = hz_i$ for all i. By (i), there is $\sigma \in N_G(U)$ with $z_i = \sigma x_i$ for all i, and so $gx_i = y_i = h\sigma x_i$ for all i. Hence $g^{-1}h\sigma$ fixes all x_i *and* $g^{-1}h\sigma \in H$. Now $H \leq N_G(U)$, because $U \lhd H$, so that $g^{-1}h\sigma \in N_G(U)$ and $g^{-1}h \in N_G(U)$. Therefore, $U^g = U^h$ and $g\mathscr{F}(U) = \mathscr{F}(U^g) = \mathscr{F}(U^h) = h\mathscr{F}(U)$, as desired. ∎

Lemma 9.67. *Let* $H \leq M_{24}$ *be the stabilizer of the five points*

$$\infty, \omega, \Omega, [1, 0, 0], \text{ and } [0, 1, 0].$$

(i) *H is a group of order* 48 *having a normal elementary abelian Sylow* 2-*subgroup U of order* 16.
(ii) $\mathscr{F}(U) = \ell \cup \{\infty, \omega, \Omega\}$, *where* ℓ *is the projective line* $v = 0$, *and so* $|\mathscr{F}(U)| = 8$.
(iii) *Only the identity of* M_{24} *fixes more than* 8 *points.*

Proof. (i) Consider the group $\tilde{H}$ of all matrices over GF(4) of the form

$$A = \lambda \begin{bmatrix} 1 & 0 & \alpha \\ 0 & \gamma & \beta \\ 0 & 0 & \gamma^{-1} \end{bmatrix},$$

where $\lambda, \gamma \neq 0$. There are 3 choices for each of λ and γ, and 4 choices for each of α and β, so that $|\tilde{H}| = 3 \times 48$. Clearly $\tilde{H}/Z(3, 4)$ has order 48, lies in $PSL(3, 4) \leq M_{24}$, and fixes the five listed points, so that $H = \tilde{H}/Z(3, 4)$ (we know that $|H| = 48$ from Theorem 9.57). Define $\tilde{U} \leq \tilde{H}$ to be all those matrices A above for which $\gamma = 1$. Then $U = \tilde{U}/Z(3, 4)$ has order 16 and consists of involutions; that is, U is elementary abelian. But $\tilde{U} \lhd \tilde{H}$, being the kernel

of the map $\tilde{H} \to SL(3, 4)$ given by

$$A \mapsto \begin{bmatrix} \lambda & 0 & 0 \\ 0 & \lambda\gamma & 0 \\ 0 & 0 & \lambda^{-1} \end{bmatrix},$$

so that $U \lhd H$.

(ii) Assume that $[\lambda, \mu, v] \in \mathscr{F}(U)$. If $h \in U$, then $\gamma = 1$ and

$$h\begin{bmatrix} \lambda \\ \mu \\ v \end{bmatrix} = \begin{bmatrix} 1 & 0 & \alpha \\ 0 & 1 & \beta \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} \lambda \\ \mu \\ v \end{bmatrix} = \begin{bmatrix} \lambda + \alpha v \\ \mu + \beta v \\ v \end{bmatrix} = \begin{bmatrix} \xi\lambda \\ \xi\mu \\ \xi v \end{bmatrix}$$

for some $\xi \in GF(4)^\times$. If $v = 0$, then all projective points of the form $[\lambda, \mu, 0]$ (which form a projective line ℓ having $4 + 1 = 5$ points) are fixed by h. If $v \neq 0$, then these equations have no solution, and so h fixes no other projective points. Therefore, every $h \in U$ fixes ℓ, ∞, ω, Ω, and nothing else, so that $\mathscr{F}(U) = \ell \cup \{\infty, \omega, \Omega\}$ and $|\mathscr{F}(U)| = 8$.

(iii) By 5-transitivity of M_{24}, it suffices to show that $h \in H^\#$ can fix at most 3 projective points in addition to $[1, 0, 0]$ and $[0, 1, 0]$. Consider the equations for $\xi \in GF(4)^\times$:

$$h\begin{bmatrix} \lambda \\ \mu \\ v \end{bmatrix} = \begin{bmatrix} 1 & 0 & \alpha \\ 0 & \gamma & \beta \\ 0 & 0 & \gamma^{-1} \end{bmatrix}\begin{bmatrix} \lambda \\ \mu \\ v \end{bmatrix} = \begin{bmatrix} \lambda + \alpha v \\ \gamma\mu + \beta v \\ \gamma^{-1} v \end{bmatrix} = \begin{bmatrix} \xi\lambda \\ \xi\mu \\ \xi v \end{bmatrix}.$$

If $v = 0$, then we may assume that $\lambda \neq 0$ (for $[0, 1, 0]$ is already on the list of five). Now $\lambda = \lambda + \alpha v = \xi\lambda$ and $\mu = \gamma\mu + \beta v = \xi\mu$ give $\gamma = 1$; hence $h \in U$ and h fixes exactly 8 elements, as we saw in (ii). If $v \neq 0$, then $v = \gamma^{-1}v = \xi v$ implies $\xi = \gamma^{-1}$; we may assume that $\gamma \neq 1$ lest $h \in U$. The equations can now be solved uniquely for λ and μ ($\lambda = (\gamma^{-1} - 1)^{-1}\alpha v$ and $\mu = (\gamma^{-1} - \gamma)^{-1}\beta v$), so that $h \notin U$ can fix only one projective point other than $[1, 0, 0]$ and $[0, 1, 0]$; that is, such an h can fix at most 6 points. ∎

Theorem 9.68. *Neither* M_{12} *nor* M_{24} *has a transitive extension.*

Proof. In order to show that M_{12} has no transitive extension, it suffices to show that there is no sharply 6-transitive group G of degree 13. Now such a group G would have order $13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$. If $g \in G$ has order 5, then g is a product of two 5-cycles and hence fixes 3 points (g cannot be a 5-cycle lest it fix $8 > 6$ points). Denote these fixed points by $\{a, b, c\}$, and let $H = G_{a,b,c}$. Now $\langle g \rangle$ is a Sylow 5-subgroup of H ($\langle g \rangle$ is even a Sylow 5-subgroup of G), so that Theorem 9.66(i) gives $N = N_G(\langle g \rangle)$ acting 3-transitively on $\mathscr{F}(\langle g \rangle) = \{a, b, c\}$; that is, there is a surjective homomorphism $\varphi: N \to S_3$. We claim that $C = C_G(\langle g \rangle) \nleq \ker \varphi$. Otherwise, φ induces a surjective map $\varphi_*: N/C \to S_3$. By Theorem 7.1, $N/C \leq \text{Aut}(\langle g \rangle)$, which is abelian, so that N/C and hence S_3 are abelian, a contradiction. Now $C \lhd N$ forces $\varphi(C) \lhd \varphi(N) = S_3$, so that $\varphi(C) = A_3$ (we have just seen that $\varphi(C) \neq 1$) and so 3 divides $|C|$. There is thus an element $h \in C$ of order 3. Since g and h commute, the element gh has order 15. Now gh cannot be a 15-cycle (G has degree 13), and so its cycle structure is either (5, 5, 3), (5, 3, 3), or (5, 3). Hence $(gh)^5$, being either a 3-cycle or a product of 2 disjoint 3-cycles, fixes more than 6 points. This contradiction shows that no such G can exist.

A transitive extension G of M_{24} would have degree 25 and order $25 \cdot 24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48$. If $g \in G$ has order 11, then g is a product of 2 disjoint 11-cycles (it cannot be an 11-cycle lest it fix $14 > 8$ points, contradicting Lemma 9.67(iii)). Arguing as above, there is an element $h \in G$ of order 3 commuting with g, and so gh has order 33. Since G has degree 25, gh is not a 33-cycle, and so its cycle structure is either of the form (11, 11, 3) or one 11-cycle and several 3-cycles. In either case, $(gh)^{11}$ has order 3 and fixes more than 8 points, contradicting Lemma 9.67. ▩

Theorem 9.69.

(i) *Let $X = \mathrm{P}^2(4) \cup \{\infty, \omega, \Omega\}$ be regarded as an M_{24}-set, let U be a Sylow 2-subgroup of H (the stabilizer of 5 points), and let $\mathscr{B} = \{g\mathscr{F}(U): g \in M_{24}\}$. Then $(X, \mathscr{B})$ is a Steiner system of type $S(5, 8, 24)$.*

(ii) *If $g\mathscr{F}(U)$ contains $\{\infty, \omega, \Omega\}$, then its remaining 5 points form a projective line. Conversely, for every projective line ℓ', there is $g \in \mathrm{PSL}(3, 4) \leq M_{24}$ with $g\mathscr{F}(U) = \ell' \cup \{\infty, \omega, \Omega\}$.*

Proof. (i) Lemma 9.67 verifies that the conditions stated in Theorem 9.66 do hold.

(ii) The remark after Theorem 9.61 gives a formula for the number r'' of blocks containing 3 points; in particular, there are 21 blocks containing $\{\infty, \omega, \Omega\}$. If $\ell \subset \mathscr{F}(U)$ is the projective line $v = 0$, and if $g \in \mathrm{PSL}(3, 4) = (M_{24})_{\infty,\omega,\Omega}$, then $g\mathscr{F}(U) = g(\ell) \cup \{\infty, \omega, \Omega\}$. But $\mathrm{PSL}(3, 4)$ acts transitively on the lines of $\mathrm{P}^2(4)$ (Exercise 9.23) and $\mathrm{P}^2(4)$ has exactly 21 lines (Theorem 9.40(ii)). It follows that the 21 blocks containing the 3 infinite points ∞, ω, Ω are as described. ▩

The coming results relating Mathieu groups to Steiner systems are due to R.D. Carmichael and E. Witt.

Theorem 9.70. *$M_{24} \cong \mathrm{Aut}(X, \mathscr{B})$, where $(X, \mathscr{B})$ is a Steiner system of type $S(5, 8, 24)$.*

Remark. There is only one Steiner system with these parameters.

Proof. Let $(X, \mathscr{B})$ be the Steiner system of Theorem 9.69: $X = \mathrm{P}^2(4) \cup \{\infty, \omega, \Omega\}$ and $\mathscr{B} = \{g\mathscr{F}(U): g \in M_{24}\}$, where $\mathscr{F}(U) = \ell \cup \{\infty, \omega, \Omega\}$ (here ℓ is the projective line $v = 0$).

It is clear that every $g \in M_{24}$ is a permutation of X that carries blocks to blocks, so that $M_{24} \leq \mathrm{Aut}(X, \mathscr{B})$. For the reverse inclusion, let $\varphi \in \mathrm{Aut}(X, \mathscr{B})$. Multiplying φ by an element of M_{24} if necessary, we may assume that φ fixes $\{\infty, \omega, \Omega\}$ and, hence, that $\varphi|\mathrm{P}^2(4)\colon \mathrm{P}^2(4) \to \mathrm{P}^2(4)$. By Theorem 9.69(ii), φ carries projective lines to projective lines, and so φ is a collineation of $\mathrm{P}^2(4)$. But M_{24} contains a copy of $\mathrm{P\Gamma L}(3, 4)$, the collineation group of $\mathrm{P}^2(4)$, by Exercise 9.40. There is thus $g \in M_{24}$ with $g|\mathrm{P}^2(4) = \varphi|\mathrm{P}^2(4)$, and $\varphi g^{-1} \in \mathrm{Aut}(X, \mathscr{B})$ (because $M_{24} \leq \mathrm{Aut}(X, \mathscr{B})$). Now φg^{-1} can permute only ∞, ω, Ω. Since every block has 8 elements φg^{-1} must fix at least 5 elements; as each block is determined by any 5 of its elements, φg^{-1} must fix every block, and so Theorem 9.63 shows that $\varphi g^{-1} = 1$; that is, $\varphi = g \in M_{24}$, as desired. ▩

We interrupt this discussion to prove a result mentioned in Chapter 8.

Theorem 9.71. $\mathrm{PSL}(4, 2) \cong A_8$.

Proof. The Sylow 2-subgroup U in H, the stabilizer of 5 points in M_{24}, is elementary abelian of order 16; thus, U is a 4-dimensional vector space over $\mathbb{Z}_2$. Therefore, $\mathrm{Aut}(U) \cong \mathrm{GL}(4, 2)$ and, by Theorem 8.5, $|\mathrm{Aut}(U)| = (2^4 - 1)(2^4 - 2)(2^4 - 4)(2^4 - 8) = 8!/2$.

Let $N = N_{M_{24}}(U)$. By Theorem 9.66(ii), N acts 5-transitively (and faithfully) on $\mathscr{F}(U)$, a set with 8 elements. Therefore, $|N| = 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot s$, where $s \leq 6 = |S_3|$. If we identify the symmetric group on $\mathscr{F}(U)$ with S_8, then $[S_8 : N] = t \leq 6$ (where $t = 6/s$). By Exercise 9.3(ii), S_8 has no subgroups of index t with $2 < t < 8$. Therefore, $t = 1$ or $t = 2$; that is, $N = S_8$ or $N = A_8$. Now there is a homomorphism $\varphi\colon N \to \mathrm{Aut}(U)$ given by $g \mapsto \gamma_g$ = conjugation by g. Since A_8 is simple, the only possibilities for im φ are S_8, A_8, $\mathbb{Z}_2$, or 1. We cannot have im $\varphi \cong S_8$ (since $|\mathrm{Aut}(U)| = 8!/2$); we cannot have $|\mathrm{im}\ \varphi| \leq 2$ (for $H \leq N$, because $U \lhd H$, and it is easy to find $h \in H$ of odd order and $u \in U$ with $huh^{-1} \neq u$). We conclude that $N = A_8$ and that $\varphi\colon N \to \mathrm{Aut}(U) \cong \mathrm{GL}(4, 2)$ is an isomorphism. ▩

Theorem 9.72. *$M_{23} \cong \mathrm{Aut}(X', \mathscr{B}')$, where $(X', \mathscr{B}')$ is a Steiner system of type $S(4, 7, 23)$.*

Remark. There is only one Steiner system with these parameters.

Proof. Let $X' = \mathrm{P}^2(4) \cup \{\infty, \omega\}$, let $B' = B'(\ell) = \ell \cup \{\infty, \omega\}$, where ℓ is the projective line $v = 0$, and let $\mathscr{B}' = \{g(B'): g \in M_{23}\}$. It is easy to see that $(X', \mathscr{B}')$ is the contraction at Ω of the Steiner system $(X, \mathscr{B})$ in Theorem 9.69, so that it is a Steiner system of type $S(4, 7, 23)$.

It is clear that $M_{23} \leq \mathrm{Aut}(X', \mathscr{B}')$. For the reverse inclusion, let $\varphi \in \mathrm{Aut}(X', \mathscr{B}')$, and regard φ as a permutation of X with $\varphi(\Omega) = \Omega$. Multiplying by an element of M_{23} if necessary, we may assume that φ fixes ∞ and ω.

Since $(X', \mathscr{B}')$ is a contraction of $(X, \mathscr{B})$, a block in $\mathscr{B}'$ containing ∞ and ω has the form $\ell' \cup \{\infty, \omega\}$, where ℓ' is a projective line. As in the proof of Theorem 9.70, $\varphi|P^2(4)$ preserves lines and hence is a collineation of $P^2(4)$. Since M_{24} contains a copy of $P\Gamma L(3, 4)$, there is $g \in M_{24}$ with $g|P^2(4) = \varphi|P^2(4)$. Therefore, g and φ can only disagree on the infinite points ∞, ω, and Ω.

If $B \in \text{star}(\Omega)$ (i.e., if B is a block in $\mathscr{B}$ containing Ω), then $\varphi(B)$ and $g(B)$ are blocks; moreover, $|\varphi(B) \cap g(B)| \geq 5$, for blocks have 8 points, while φ and g can disagree on at most 3 points. Since 5 points determine a block, however, $\varphi(B) = g(B)$ for all $B \in \text{star}(\Omega)$. By Corollary 9.64,

$$\begin{aligned}\{\Omega\} = \{\varphi(\Omega)\} &= \varphi\left(\bigcap_{\text{star}(\Omega)} B\right) \\ &= \bigcap_{\text{star}(\Omega)} \varphi(B) \\ &= \bigcap_{\text{star}(\Omega)} g(B) = g\left(\bigcap_{\text{star}(\Omega)} B\right) = \{g(\Omega)\}.\end{aligned}$$

Hence $g(\Omega) = \Omega$ and $g \in (M_{24})_\Omega = M_{23}$. The argument now ends as that in Theorem 9.70: $\varphi g^{-1} \in \text{Aut}(X', \mathscr{B}')$ since $M_{23} \leq \text{Aut}(X', \mathscr{B}')$, φg^{-1} fixes $\mathscr{B}'$, and $\varphi = g \in M_{23}$. ∎

Theorem 9.73. *M_{22} is a subgroup of index 2 in $\text{Aut}(X'', \mathscr{B}'')$, where $(X'', \mathscr{B}'')$ is a Steiner system of type $S(3, 6, 22)$.*

Remark. There is only one Steiner system with these parameters.

Proof. Let $X'' = X - \{\Omega, \omega\}$, let $b'' = \mathscr{F}(U) - \{\Omega, \omega\}$, and let $\mathscr{B}'' = \{gb'': g \in M_{22}\}$. It is easy to see that $(X'', \mathscr{B}'')$ is doubly contracted from $(X, \mathscr{B})$, so that it is a Steiner system of type $S(3, 6, 22)$.

Clearly $M_{22} \leq \text{Aut}(X'', \mathscr{B}'')$. For the reverse inclusion, let $\varphi \in \text{Aut}(X'', \mathscr{B}'')$ be regarded as a permutation of X which fixes Ω and ω. As in the proof of Theorem 9.72, we may assume that $\varphi(\infty) = \infty$ and that $\varphi|P^2(4)$ is a collineation. There is thus $g \in M_{24}$ with $g|P^2(4) = \varphi|P^2(4)$. Moreover, consideration of star(ω), as in the proof of Theorem 9.72, gives $g(\omega) = \omega$. Therefore, φg^{-1} is a permutation of X fixing $P^2(4) \cup \{\omega\}$. If φg^{-1} fixes Ω, then $\varphi g^{-1} = 1_X$ and $\varphi = g \in (M_{24})_{\Omega,\omega} = M_{22}$. The other possibility is that $\varphi g^{-1} = (\infty\ \ \Omega)$.

We claim that $[\text{Aut}(X'', \mathscr{B}''): M_{22}] \leq 2$. If $\varphi_1, \varphi_2 \in \text{Aut}(X'', \mathscr{B}'')$ and $\varphi_1, \varphi_2 \notin M_{22}$, then we have just seen that $\varphi_i = (\infty\ \ \Omega)g_i$ for $i = 1, 2$, where $g_i \in M_{24}$. But $g_1^{-1}g_2 = \varphi_1^{-1}\varphi_2 \in (M_{24})_{\Omega,\omega} = M_{22}$ (since both φ_i fix Ω and ω); there are thus at most two cosets of M_{22} in $\text{Aut}(X'', \mathscr{B}'')$.

Recall the definitions of the elements h_2 and h_3 in M_{24}: $h_2 = (\omega\ \ \infty)f_2$ and $h_3 = (\Omega\ \ \omega)f_3$, where f_2, f_3 act on $P^2(4)$ and fix ∞, ω, and Ω. Note that h_2 fixes Ω and h_3 fixes ∞. Define $g = h_3h_2h_3 = (\Omega\ \ \infty)f_3f_2f_3$, and define $\varphi: X'' \to X''$ to be the function with $\varphi(\infty) = \infty$ and $\varphi|P^2(4) = f_3f_2f_3$. By Lemma 9.54, $\varphi|P^2(4)$ is a collineation; since φ fixes ∞, it follows that $\varphi \in \text{Aut}(X'', \mathscr{B}'')$. On the other hand, $\varphi \notin M_{22}$, lest $\varphi g^{-1} = (\Omega\ \ \infty) \in M_{24}$, contradicting Lemma 9.67(iii). We have shown that M_{22} has index 2 in $\text{Aut}(X'', \mathscr{B}'')$. ∎

Corollary 9.74. *M_{22} has an outer automorphism of order 2 and $\text{Aut}(X'', \mathscr{B}'') \cong M_{22} \rtimes \mathbb{Z}_2$.*

Proof. The automorphism $\varphi \in \text{Aut}(X'', \mathscr{B}'')$ with $\varphi \notin M_{22}$ constructed at the end of the proof of Theorem 9.73 has order 2, for both f_2 and f_3 are involutions (Lemma 9.54), hence the conjugate $f_3f_2f_3$ is also an involution. It follows that $\text{Aut}(X'', \mathscr{B}'')$ is a semidirect product $M_{22} \rtimes \mathbb{Z}_2$. Now φ is an automorphism of M_{22}: if $a \in M_{22}$, then $a^\varphi = \varphi a \varphi^{-1} \in M_{22}$. Were φ an inner automorphism, there would be $b \in M_{22}$ with $\varphi a \varphi^{-1} = bab^{-1}$ for all $a \in M_{22}$; that is, φa^{-1} would centralize M_{22}. But a routine calculation shows that φ does not commute with $h_1 = (\infty\ \ [1, 0, 0])f_1 \in M_{22}$, and so φ is an outer automorphism of M_{22}. ∎

The "small" Mathieu groups M_{11} and M_{12} are also intimately related to Steiner systems, but we cannot use Theorem 9.66 because the action is now sharp.

Lemma 9.75. *Regard $X = GF(9) \cup \{\infty, \omega, \Omega\}$ as an M_{12}-set. There is a subgroup $\Sigma \leq M_{12}$, isomorphic to S_6, having two orbits of size 6, say, Z and Z', and which acts sharply 6-transitively on Z. Moreover,*

$$\Sigma = \{\mu \in M_{12}: \mu(Z) = Z\}.$$

Proof. Denote the 5-set $\{\infty, \omega, \Omega, 1, -1\}$ by Y. For each permutation τ of Y, sharp 5-transitivity of M_{12} provides a unique $\tau^* \in M_{12}$ with $\tau^*|Y = \tau$. It is easy to see that the function $S_Y \to M_{12}$, given by $\tau \mapsto \tau^*$, is an injective homomorphism; we denote its image (isomorphic to S_5) by Q.

Let us now compute the Q-orbits of X. One of them, of course, is Y. If τ is the 3-cycle $(\infty\ \ \omega\ \ \Omega)$, then $\tau^* \in Q$ has order 3 and fixes 1 and -1. Now τ^* is a product of three disjoint 3-cycles (fewer than three would fix too many points of X), so that the $\langle\tau^*\rangle$-orbits of the 7-set $X - Y$ have sizes (3, 3, 1). Since the Q-orbits of X (and of $X - Y$) are disjoint unions of $\langle\tau^*\rangle$-orbits (Exercise 9.4), the Q-orbits of $X - Y$ have possible sizes (3, 3, 1), (6, 1), (3, 4), or 7. If Q has one orbit of size 7, then Q acts transitively on $X - Y$; this is impossible, for 7 does not divide $|Q| = 120$. Furthermore, Exercise 9.3(i) says that Q has no orbits of size t, where $2 < t < 5$. We conclude that $X - Y$ has two Q-orbits of sizes 6 and 1, respectively. There is thus a unique point in $X - Y$, namely, the orbit of size 1, that is fixed by every element of Q. If $\sigma \in S_Y$ is the transposition $(1\ \ -1)$, then its correspondent $\sigma^* \in Q$ fixes ∞, ω, Ω and interchanges 1 and -1. But $\zeta\colon \mathrm{GF}(9) \to \mathrm{GF}(9)$, defined by $\zeta\colon \lambda \mapsto -\lambda$, lies in M_{10} (for -1 is a square in GF(9)) and $\zeta | Y = \sigma$, so that $\zeta = \sigma^*$. Since the only other point fixed by ζ is 0, the one-point Q-orbit of $X - Y$ must be $\{0\}$.

Define $Z = Y \cup \{0\} = \{\infty, \omega, \Omega, 1, -1, 0\}$. We saw, in Exercise 9.33, that $M_{10} \leq M_{12}$ contains $\sigma_1\colon \mathrm{P}^1(9) \to \mathrm{P}^1(9)$, where $\sigma_1\colon \lambda \mapsto -1/\lambda$ is $(0\ \infty)(1\ -1)(\pi^3\ \pi)(\pi^5\ \pi^7)$. Let us see that the subgroup $\Sigma = \langle Q, \sigma_1 \rangle \cong S_6$. The set Z is both a Q-set and a $\langle \sigma_1 \rangle$-set, hence it is also a Σ-set. As Σ acts transitively on Z and the stabilizer of 0 is Q (which acts sharply 5-transitively on $Z - \{0\} = Y$), we have Σ acting sharply 6-transitively on the 6-point set Z, and so $\Sigma \cong S_6$. Finally, the 6 points $X - Z$ comprise the other Σ-orbit of X (for we have already seen that $X - Z$ is a Q-orbit).

If $\beta \in Q$, then $\beta(Y) = Y$ and $\beta(0) = 0$, so that $\beta(Z) = Z$. Since $\sigma_1(Z) = Z$, it follows that $\sigma(Z) = Z$ for all $\sigma \in \Sigma$. Conversely, suppose $\mu \in M_{12}$ and $\mu(Z) = Z$. Since Σ acts 6-transitively on Z, there is $\sigma \in \Sigma$ with $\sigma | Z = \mu | Z$. But $\mu\sigma^{-1}$ fixes 6 points, hence is the identity, and $\mu = \sigma \in \Sigma$. ∎

Theorem 9.76. *If $X = \mathrm{GF}(9) \cup \{\infty, \omega, \Omega\}$ is regarded as an M_{12}-set and $\mathscr{B} = \{gZ\colon g \in M_{12}\}$, where $Z = \{\infty, \omega, \Omega, 1, -1, 0\}$, then $(X, \mathscr{B})$ is a Steiner system of type $S(5, 6, 12)$.*

Proof. It is clear that every block gZ has 6 points. If $x_1, \ldots, x_5$ are any five distinct points in X, then 5-transitivity of M_{12} provides $g \in M_{12}$ with $\{x_1, \ldots, x_5\} \subset gZ$. It remains to prove uniqueness of a block containing five given points, and it suffices to show that if Z and gZ have five points in common, then $Z = gZ$. Now if $Z = \{z_1, \ldots, z_6\}$, then $gZ = \{gz_1, \ldots, gz_6\}$, where $gz_1, \ldots, gz_5 \in Z$. By Lemma 9.75, there is $\sigma \in \Sigma \leq M_{12}$ with $\sigma z_1 = gz_1, \ldots, \sigma z_5 = gz_5$. Note that $\sigma Z = Z$, for Z is a Σ-orbit. On the other hand, σ and g agree on five points of X, so that sharp 5-transitivity of M_{12} gives $\sigma = g$. Therefore $Z = \sigma Z = gZ$. ∎

If GF(9) is regarded as an affine plane over $\mathbb{Z}_3$, then the blocks of the Steiner system constructed above can be examined from a geometric viewpoint.

Lemma 9.77. *Let $(X, \mathscr{B})$ be the Steiner system constructed from M_{12} in Theorem 9.76. A subset B of X containing $T = \{\infty, \omega, \Omega\}$ is a block if and only if $B = T \cup \ell$, where ℓ is a line in GF(9) regarded as an affine plane over $\mathbb{Z}_3$.*

Proof. Note that $Z = T \cup \ell_0$, where $\ell_0 = \{1, -1, 0\}$, and ℓ_0 is the line consisting of the scalar multiples of 1. By Exercises 9.38 and 9.39, M_{12} contains a subgroup $W \cong \mathrm{Aut}(2, 3)$ each of whose elements permutes T. Hence, for every $g \in W$, $gZ = T \cup g\ell_0$, and $g\ell_0$ is an affine line. But one may count exactly 12 affine lines in the affine plane, so that there are 12 blocks of the form $T \cup \ell$. On the other hand, the remark after Theorem 9.61 shows that there exactly 12 blocks containing the 3-point set T. ∎

Theorem 9.78. *$M_{12} \cong \mathrm{Aut}(X, \mathscr{B})$, where $(X, \mathscr{B})$ is a Steiner system of type $S(5, 6, 12)$.*

Remark. There is only one Steiner system with these parameters.

Proof. Let $(X, \mathscr{B})$ be the Steiner system constructed in Theorem 9.76. Now $M_{12} \leq \mathrm{Aut}(X, \mathscr{B})$ because every $g \in M_{12}$ carries blocks to blocks. For the reverse inclusion, let $\varphi \in \mathrm{Aut}(X, \mathscr{B})$. Composing with an element of M_{12} if necessary, we may assume that φ permutes $T = \{\infty, \omega, \Omega\}$ and φ permutes GF(9). Regarding GF(9) as an affine plane over $\mathbb{Z}_3$, we see from Lemma 9.77 that $\varphi | \mathrm{GF}(9)$ is an affine automorphism. By Exercise 9.39, there is $g \in M_{12}$ which permutes T and with $g | \mathrm{GF}(9) = \varphi | \mathrm{GF}(9)$. Now $\varphi g^{-1} \in \mathrm{Aut}(X, \mathscr{B})$, for $M_{12} \leq \mathrm{Aut}(X, \mathscr{B})$, φg^{-1} permutes T, and φg^{-1} fixes the other 9 points of X. We claim that φg^{-1} fixes every block B in $\mathscr{B}$. This is clear if $|B \cap T| = 0$, 1, or 3. In the remaining case, say, $B = \{\infty, \omega, x_1, \ldots, x_4\}$, then $\varphi g^{-1}(B)$ must contain either ∞ or ω as well as the x_i, so that $|B \cap \varphi g^{-1}(B)| \geq 5$. Since 5 points determine a block, $B = \varphi g^{-1}(B)$, as claimed. Theorem 9.63 forces $\varphi g^{-1} = 1$, and so $\varphi = g \in M_{12}$, as desired. ∎

Theorem 9.79. *$M_{11} \cong \mathrm{Aut}(X', \mathscr{B}')$, where $(X', \mathscr{B}')$ is a Steiner system of type $S(4, 5, 11)$.*

Remark. There is only one Steiner system with these parameters.

Proof. Let $(X', \mathscr{B}')$ be the contraction at Ω of the Steiner system $(X, \mathscr{B})$ of Theorem 9.76. It is clear that $M_{11} \leq \mathrm{Aut}(X', \mathscr{B}')$. For the reverse inclusion, regard $\varphi \in \mathrm{Aut}(X', \mathscr{B}')$ as a permutation of X with $\varphi(\Omega) = \Omega$. Multiplying by an element of M_{11} if necessary, we may assume that φ permutes $\{\infty, \omega\}$. By Lemma 9.77, a block $B' \in \mathscr{B}'$ containing ∞ and ω has the form $B' = \{\infty, \omega\} \cup \ell$, where ℓ is a line in the affine plane over $\mathbb{Z}_3$. As in the proof of Theorem 9.78, $\varphi | \mathrm{GF}(9)$ is an affine isomorphism, so there is $g \in M_{12}$ with $g | \mathrm{GF}(9) = \varphi | \mathrm{GF}(9)$. As in the proof of Theorem 9.72, an examination of $g(\mathrm{star}(\Omega))$ shows that $g(\Omega) = \Omega$, so that $g \in (M_{12})_\Omega = M_{11}$. The argument now finishes as that for Theorem 9.78: $\varphi g^{-1} \in \mathrm{Aut}(X', \mathscr{B}')$; φg^{-1} fixes $\mathscr{B}'$; $\varphi = g \in M_{11}$. ∎

The subgroup structures of the Mathieu groups are interesting. There are other simple groups imbedded in them: for example, M_{12} contains copies of A_6, PSL(2, 9), and PSL(2, 11), while M_{24} contains copies of M_{12}, A_8, and PSL(2, 23). The copy Σ of S_6 in M_{12} leads to another proof of the existence of an outer automorphism of S_6.

Theorem 9.80. *S_6 has an outer automorphism of order 2.*

Remark. See Corollary 7.13 for another proof.

Proof. Recall from Lemma 9.75 that if $X = \{\infty, \omega, \Omega\} \cup \mathrm{GF}(9)$ and Σ ($\cong S_6$) is the subgroup of M_{12} in Lemma 9.75, then X has two Σ-orbits, say, $Z = Y \cup \{0\}$ and $Z' = Y' \cup \{0'\}$, each of which has 6 points. If $\sigma \in \Sigma$ has order 5, then σ is a product of two disjoint 5-cycles (only one 5-cycle fixes too many points), hence it fixes, say, 0 and 0'. It follows that if $U = \langle\sigma\rangle$, then each of Z and Z' consists of two U-orbits, one of size 5 and one of size 1. Now $H = (M_{12})_{0,0'} \cong M_{10}$, and U is a Sylow 5-subgroup of H. By Theorem 9.66, $N = N_{M_{12}}(U)$ acts 2-transitively on $\mathscr{F}(U) = \{0, 0'\}$, so there is $\alpha \in N$ of order 2 which interchanges 0 and 0'.

Since α has order 2, $\alpha = \tau_1 \ldots \tau_m$, where the τ_i are disjoint transpositions and $m \leq 6$. But M_{12} is sharply 5-transitive, so that $4 \leq m$; also, $M_{12} \leq A_{12}$, so that $m = 4$ or $m = 6$.

We claim that α interchanges the sets $Z = Y \cup \{0\}$ and $Z' = Y' \cup \{0'\}$. Otherwise, there is $y \in Y$ with $\alpha(y) = z \in Y$. Now $\alpha\sigma\alpha = \sigma^i$ for some i (because α normalizes $\langle\sigma\rangle$). If $\sigma^i(y) = u$ and $\sigma(z) = v$, then $u, v \in Y$ because $Y \cup \{0\}$ is a Σ-orbit. But $u = \sigma^i(y) = \alpha\sigma\alpha(y) = \alpha\sigma(z) = \alpha(v)$, and it is easy to see that y, z, u, and v are all distinct. Therefore, the cycle decomposition of α involves $(0\ 0')$, $(y\ z)$, and $(v\ u)$. There is only one point remaining in Y, say a, and there are two cases: either $\alpha(a) = a$ or $\alpha(a) \in Y'$. If α fixes a, then there is $y' \in Y'$ moved by α, say, $\alpha(y') = z' \in Y'$. Repeat the argument above: there are points $u', v' \in Y'$ with transpositions $(y'\ z')$ and $(v'\ u')$ involved in the cycle decomposition of α. If a' is the remaining point in Y', then the transposition $(a\ a')$ must also occur in the factorization of α because α is not a product of 5 disjoint transpositions. In either case, we have $a \in Y$ and $a' \in Y'$ with $\alpha = (0\ 0')(y\ z)(v\ u)(a\ a')\beta$, where β permutes $Y' - \{a'\}$. But $\alpha\sigma\alpha(a) = \sigma^i(a) \in Z$; on the other hand, if $\sigma(a') = b' \in Y'$, say, then $\alpha\sigma\alpha(a) = \alpha\sigma(a') = \alpha(b')$, so that $\alpha(b') \in Y$. Since a' is the only element of Y' that α moves to Y, $b' = a'$ and $\sigma(a') = b' = a'$; that is, σ fixes a'. This is a contradiction, for σ fixes only 0 and 0'.

It is easy to see that α normalizes Σ. Recall that $\sigma \in \Sigma$ if and only if $\sigma(Z) = Z$ (and hence $\sigma(Z') = Z'$). Now $\alpha\sigma\alpha(Z) = \alpha\sigma(Z') = \alpha(Z') = Z$, so that $\alpha\sigma\alpha \in \Sigma$. Therefore, $\gamma = \gamma_\alpha$ (conjugation by α) is an automorphism of Σ.

Suppose there is $\beta \in \Sigma$ with $\alpha\sigma^*\alpha = \beta\sigma^*\beta^{-1}$ for all $\sigma^* \in \Sigma$; that is, $\beta^{-1}\alpha \in C = C_{M_{12}}(\Sigma)$. If $C = 1$, then $\alpha = \beta \in \Sigma$, and this contradiction would show that γ is an outer automorphism. If $\sigma^* \in \Sigma$, then $\sigma^* = \sigma\sigma'$, where σ permutes Z and fixes Z' and σ' permutes Z' and fixes Z. Schematically,

$$\sigma^* = (z\ x\ \ldots)(z'\ x'\ \ldots);$$

if $\mu \in M_{12}$, then (as any element of S_{12}),

$$\mu\sigma^*\mu^{-1} = (\mu z\ \mu x\ \ldots)(\mu z'\ \mu x'\ \ldots).$$

In particular, if $\mu \in C$ (so that $\mu\sigma^*\mu^{-1} = \sigma^*$), then either $\mu(Z) = Z$ and $\mu(Z') = Z'$ or μ switches Z and Z'. In the first case, $\mu \in \Sigma$, by Lemma 9.75, and $\mu \in C \cap \Sigma = Z(\Sigma) = 1$. In the second case, $\mu\sigma\mu^{-1} = \sigma'$ (and $\mu\sigma'\mu^{-1} = \sigma$), so that σ and σ' have the same cycle structure for all $\sigma^* = \sigma\sigma' \in \Sigma$. But there

is $\sigma^* \in \Sigma$ with σ a transposition. If such μ exists, then σ^* would be a product of two disjoint transpositions and hence would fix 8 points, contradicting M_{12} being sharply 5-transitive. ∎

There is a similar argument, using an imbedding of M_{12} into M_{24}, which exhibits an outer automorphism of M_{12}. There are several other proofs of the existence of the outer automorphism of S_6; for example, see Conway and Sloane (1993).

The Steiner systems of types $S(5, 6, 12)$ and $S(5, 8, 24)$ arise in algebraic coding theory, being the key ingredients of (ternary and binary) ***Golay codes***. The Steiner system of type $S(5, 8, 24)$ is also used to define the ***Leech lattice***, a configuration in $\mathbb{R}^{24}$ arising in certain sphere-packing problems as well as in the construction of other simple sporadic groups.