9.33. Show that $M_{10} = \langle \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5 \rangle$, where

$$\sigma_1(\lambda) = -1/\lambda, \qquad \sigma_2(\lambda) = \lambda + 1, \qquad \sigma_3(\lambda) = \lambda + \pi,$$
$$\sigma_4(\lambda) = \pi^2\lambda, \qquad \sigma_5(\lambda) = \pi\lambda^3.$$

9.34. Prove that M_{10} consists of even permutations of $P^1(9)$. (*Hint.* Write each of the generators σ_i, $1 \le i \le 5$, as a product of disjoint cycles.)

9.35. Let σ_6 and σ_7 be the permutations of GF(9) defined by $\sigma_6(\lambda) = \pi^2\lambda + \pi\lambda^3$ and $\sigma_7(\lambda) = \lambda^3$. Regarding GF(9) as a vector space over $\mathbb{Z}_3$, prove that σ_6 and σ_7 are linear transformations.

9.36. Prove that $\mathrm{GL}(2, 3) \cong \langle \sigma_4, \sigma_5, \sigma_6, \sigma_7 \rangle$ (where σ_4 and σ_5 are as in Exercise 9.33, and σ_6 and σ_7 are as in Exercise 9.35). (*Hint.* Using the coordinates in Exercise 9.32, one has

$$\sigma_4 = \begin{bmatrix} 1 & -1 \\ -1 & -1 \end{bmatrix}, \qquad \sigma_5 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$
$$\sigma_6 = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}, \qquad \sigma_7 = \begin{bmatrix} 1 & -1 \\ 0 & -1 \end{bmatrix}.)$$

Mathieu Groups

We have already seen some doubly and triply transitive groups. In this section, we construct the five simple Mathieu groups; one is 3-transitive, two are 4-transitive, and two are 5-transitive. In 1873, Jordan proved there are no *sharply* 6-transitive groups (other than the symmetric and alternating groups). One consequence of the classification of all finite simple groups is that no 6-transitive groups exist other than the symmetric and alternating groups; indeed, all multiply transitive groups are now known (see the survey article [P.J. Cameron, Finite permutation groups and finite simple groups, *Bull. London Math. Soc.* **13** (1981), pp. 1–22]).

All G-sets in this section are faithful and, from now on, we shall call such groups G ***permutation groups***; that is, $G \le S_X$ for some set X. Indeed, we finally succumb to the irresistible urge of applying to groups G those adjectives heretofore reserved for G-sets. For example, we will say "G is a doubly transitive group of degree n" meaning that there is a (faithful) doubly transitive G-set X having n elements.

We know that if X is a k-transitive G-set and if $x \in X$, then $X - \{x\}$ is a $(k-1)$-transitive G_x-set. Is the converse true? Is it possible to begin with a k-transitive G_y-set X and construct a $(k+1)$-transitive G-set $X \cup \{y\}$?

Definition. Let G be a permutation group on X and let $\tilde{X} = X \cup \{\infty\}$, where $\infty \notin X$. A transitive permutation group $\tilde{G}$ on $\tilde{X}$ is a ***transitive extension*** of G if $G \le \tilde{G}$ and $\tilde{G}_\infty = G$.

Recall Lemma 9.5: If X is a k-transitive G-set, then $\tilde{X}$ is a $(k+1)$-transitive $\tilde{G}$-set (should $\tilde{X}$ exist).

Theorem 9.51. *Let G be a doubly transitive permutation group on a set X. Suppose there is $x \in X$, $\infty \notin X$, $g \in G$, and a permutation h of $\tilde{X} = X \cup \{\infty\}$ such that:*

(i) $g \in G_x$;
(ii) $h(\infty) \in X$;
(iii) $h^2 \in G$ *and* $(gh)^3 \in G$; *and*
(iv) $hG_xh = G_x$.

Then $\tilde{G} = \langle G, h \rangle \le S_{\tilde{X}}$ is a transitive extension of G.

Proof. Condition (ii) shows that $\tilde{G}$ acts transitively on $\tilde{X}$. It suffices to prove, as Theorem 9.4 predicts, that $\tilde{G} = G \cup GhG$, for then $\tilde{G}_\infty = G$ (because nothing in GhG fixes ∞).

By Corollary 2.4, $G \cup GhG$ is a group if it is closed under multiplication. Now

$$(G \cup GhG)(G \cup GhG) \subset GG \cup GGhG \cup GhGG \cup GhGGhG$$
$$\subset G \cup GhG \cup GhGhG,$$

because $GG = G$. It must be shown that $GhGhG \subset G \cup GhG$, and this will follow if we show that $hGh \subset G \cup GhG$.

Since G acts doubly transitively on X, Theorem 9.4 gives $G = G_x \cup G_xgG_x$ (for $g \notin G_x$). The hypothesis gives $\gamma, \delta \in G$ with $h^2 = \gamma$ and $(gh)^3 = \delta$. It follows that $h\gamma^{-1} = h^{-1} = \gamma^{-1}h$ and $hgh = g^{-1}h^{-1}g^{-1}\delta$. Let us now compute.

$$\begin{aligned} hGh &= h(G_x \cup G_xgG_x)h \\ &= hG_xh \cup hG_xgG_xh \\ &= hG_xh \cup (hG_xh)h^{-1}gh^{-1}(hG_xh) \\ &= G_x \cup G_xh^{-1}gh^{-1}G_x \qquad \text{(condition (iv))} \\ &= G_x \cup G_x(\gamma^{-1}h)g(h\gamma^{-1})G_x \\ &= G_x \cup G_x\gamma^{-1}(g^{-1}h^{-1}g^{-1}\delta)\gamma^{-1}G_x \\ &\subset G \cup Gh^{-1}G \\ &= G \cup G\gamma^{-1}hG \\ &= G \cup GhG. \quad \blacksquare \end{aligned}$$

One can say a bit about the cycle structure of h. If $h(\infty) = a \in X$, then $h^2 \in G = \tilde{G}_\infty$ implies $h(a) = h^2(\infty) = \infty$; hence, $h = (\infty\ a)h'$, where $h' \in G_{a,\infty}$ is disjoint from $(\infty\ a)$. Similarly, one can see that gh has a 3-cycle in its factorization into disjoint cycles.

The reader will better understand the choices in the coming constructions once the relation between the Mathieu groups and Steiner systems is seen.

Theorem 9.52. *There exists a sharply 4-transitive group M_{11} of degree 11 and order $7920 = 11 \cdot 10 \cdot 9 \cdot 8 = 2^4 \cdot 3^2 \cdot 5 \cdot 11$ such that the stabilizer of a point is M_{10}.*

Proof. By Theorem 9.49, M_{10} acts sharply 3-transitively on $X = \mathrm{GF}(9) \cup \{\infty\}$. We construct a transitive extension of M_{10} acting on $\tilde{X} = \{X, \omega\}$, where ω is a new symbol. If π is a primitive element of GF(9) with $\pi^2 + \pi = 1$, define

$$x = \infty,$$

$$g = (0\ \ \infty)(\pi\ \ \pi^7)(\pi^2\ \ \pi^6)(\pi^3\ \ \pi^5) = 1/\lambda,$$

and

$$h = (\infty\ \ \omega)(\pi\ \ \pi^2)(\pi^3\ \ \pi^7)(\pi^5\ \ \pi^6) = (\omega\ \ \infty)\sigma_6,$$

where $\sigma_6(\lambda) = \pi^2\lambda + \pi\lambda^3$ (use Exercise 9.32 to verify this).

The element g lies in M_{10}, for $\det(g) = -1 = \pi^4$, which is a square in GF(9). It is clear that $g \notin (M_{10})_\infty$ (for $g(\infty) = 0$), $h(\omega) = \infty \in X$, and $h^2 = 1 \in G$. Moreover, $(gh)^3 = 1$ because $gh = (\omega\ \ 0\ \ \infty)(\pi\ \ \pi^6\ \ \pi^3)(\pi^2\ \ \pi^7\ \ \pi^5)$.

To satisfy the last condition of Theorem 9.51, observe that if $f \in (M_{10})_\infty$, then

$$hfh(\infty) = hf(\omega) = h(\omega) = \infty,$$

so that $h(M_{10})_\infty h = (M_{10})_\infty$ if we can show that $hfh \in M_{10}$. Now $(M_{10})_\infty = S_\infty \cup T_\infty$, so that either $f = \pi^{2i}\lambda + \alpha$ or $f = \pi^{2i+1}\lambda^3 + \alpha$, where $i \geq 0$ and $\alpha \in \mathrm{GF}(9)$. In the first case (computing with the second form of $h = (\omega\ \ \infty)\sigma_6$),

$$hfh(\lambda) = (\pi^{2i+4} + \pi^{6i+4})\lambda + (\pi^{2i+3} + \pi^{6i+7})\lambda^3 + \pi^2\alpha + \pi\alpha^3.$$

The coefficients of λ and λ^3 are $\pi^{2i+4}(1 + \pi^{4i})$ and $\pi^{2i+3}(1 + \pi^{4i+4})$, respectively. When $i = 2j$ is even, the second coefficient is 0 and the first coefficient is π^{4j+4}, which is a square; hence, $hfh \in S_\infty \leq M_{10}$ in this case. When $i = 2j + 1$ is odd, the first coefficient is 0 and the second coefficient is $\pi^{4j}\pi^5$, which is a nonsquare, so that $hfh \in T_\infty \subset M_{10}$. The second case ($f = \pi^{2i+1}\lambda^3 + \alpha$) is similar; the reader may now calculate that

$$hfh(\lambda) = \pi^{2i+6}(1 + \pi^{4i})\lambda + \pi^{2i+1}(1 + \pi^{4i+4})\lambda^3 + \pi^2\alpha + \pi\alpha^3,$$

an expression which can be treated as the similar expression in the first case.

It follows from Theorem 9.8(v) that M_{11}, defined as $\langle M_{10}, h\rangle$, acts sharply 4-transitively on $\tilde{X}$, and so $|M_{11}| = 7920$. ∎

Note, for later use, that both g and h are even permutations, so that Exercise 9.34 gives $M_{11} \leq A_{11}$.

This procedure can be repeated; again, the difficulty is discovering a good permutation to adjoin.

Theorem 9.53. *There exists a sharply 5-transitive group M_{12} of degree 12 and order $95{,}040 = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 = 2^6 \cdot 3^3 \cdot 5 \cdot 11$ such that the stabilizer of a point is M_{11}.*

Proof. By Theorem 9.52, M_{11} acts sharply 4-transitively on $Y = \{\mathrm{GF}(9), \infty, \omega\}$. We construct a transitive extension of M_{11} acting on $\tilde{Y} = \{Y, \Omega\}$, where Ω is a new symbol. If π is a primitive element of GF(9) with $\pi^2 + \pi = 1$, define

$$x = \omega,$$

$$h = (\infty\ \ \omega)(\pi\ \ \pi^2)(\pi^3\ \ \pi^7)(\pi^5\ \ \pi^6),$$

and

$$k = (\omega\ \ \Omega)(\pi\ \ \pi^3)(\pi^2\ \ \pi^6)(\pi^5\ \ \pi^7) = (\omega\ \ \Omega)\lambda^3 = (\omega\ \ \Omega)\sigma_7$$

(note that this is the same h occurring in the construction of M_{11}). Clearly $k(\Omega) = \omega \in Y$ and $h \notin (M_{11})_\omega = M_{10}$. Also, $k^2 = 1$ and $hk = (\omega\ \ \Omega\ \ \infty)(\pi\ \ \pi^7\ \ \pi^6)(\pi^2\ \ \pi^5\ \ \pi^3)$ has order 3. To satisfy the last condition of Theorem 9.51, observe first that if $f \in (M_{11})_\omega = M_{10} = S \cup T$, then kfk also fixes ω. Finally, $kfk \in M_{11}$: if $f(\lambda) = (a\lambda + b)/(c\lambda + d) \in S$, then $kfk(\lambda) = (a^3\lambda + b^3)/(c^3\lambda + d^3)$ has determinant $a^3d^3 - b^3c^3 = (ad - bc)^3$, which is a square because $ad - bc$ is; a similar argument holds when $f \in T$. Thus, $kM_{10}k = M_{10}$.

It follows from Theorem 9.8(v) that M_{12}, defined as $\langle M_{11}, k\rangle$, acts sharply 5-transitively on $\tilde{Y}$, and so $|M_{12}| = 95{,}040$. ∎

Note that k is an even permutation, so that $M_{12} \leq A_{12}$.

The theorem of Jordan mentioned at the beginning of this section can now be stated precisely: The only sharply 4-transitive groups are S_4, S_5, A_6, and M_{11}; the only sharply 5-transitive groups are S_5, S_6, A_7, and M_{12}; if $k \geq 6$, then the only sharply k-transitive groups are S_k, S_{k+1}, and A_{k+2}. We remind the reader that Zassenhaus (1936) classified all sharply 3-transitive groups (there are only PGL(2, q) and $M(p^{2n})$ for odd primes p). If p is a prime and $q = p^n$, then Aut(1, q) is a solvable doubly transitive group of degree q. Zassenhaus (1936) proved that every sharply 2-transitive group, with only finitely many exceptions, can be imbedded in Aut(1, q) for some q; Huppert (1957) generalized this by proving that any faithful doubly transitive solvable group can, with only finitely many more exceptions, be imbedded in Aut(1, q) for some q. Thompson completed the classification of sharply 2-transitive groups as certain Frobenius groups. The classification of all finite simple groups can be used to give an explicit enumeration of all faithful doubly transitive groups. The classification of all sharply 1-transitive groups, that is, of all regular groups, is, by Cayley's theorem, the classification of all finite groups.

The "large" Mathieu groups are also constructed as a sequence of transitive extensions, but now beginning with PSL(3, 4) (which acts doubly transitively on $P^2(4)$) instead of with M_{10}. Since $|P^2(4)| = 4^2 + 4 + 1 = 21$, one begins with a permutation group of degree 21. We describe elements of $P^2(4)$ by their homogeneous coordinates.

Lemma 9.54. *Let β be a primitive element of* GF(4). *The functions f_i: $P^2(4) \to P^2(4)$, for $i = 1, 2, 3$, defined by*

$$f_1[\lambda, \mu, \nu] = [\lambda^2 + \mu\nu, \mu^2, \nu^2],$$
$$f_2[\lambda, \mu, \nu] = [\lambda^2, \mu^2, \beta\nu^2],$$
$$f_3[\lambda, \mu, \nu] = [\lambda^2, \mu^2, \nu^2],$$

are involutions which fix $[1, 0, 0]$. *Moreover,*

$$\langle \mathrm{PSL}(3, 4), f_2, f_3 \rangle = \mathrm{P\Gamma L}(3, 4).$$

Proof. The proof is left as an exercise for the reader (with the reminder that all 3-tuples are regarded as column vectors). A hint for the second statement is that $\mathrm{PSL}(3, 4) \lhd \mathrm{P\Gamma L}(3, 4)$, $\mathrm{P\Gamma L}(3, 4)/\mathrm{PSL}(3, 4) \cong S_3$, and, if the unique nontrivial automorphism of GF(4) is σ: $\lambda \mapsto \lambda^2$, then $f_3 = \sigma_*$ and

$$f_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \beta \end{bmatrix} \sigma_*. \quad ■$$

Theorem 9.55. *There exists a 3-transitive group M_{22} of degree 22 and order* $443{,}520 = 22 \cdot 21 \cdot 20 \cdot 48 = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$ *such that the stabilizer of a point is* PSL(3, 4).

Proof. We show that $G = \mathrm{PSL}(3, 4)$ acting on $X = P^2(4)$ has a transitive extension. Let

$$x = [1, 0, 0],$$
$$g[\lambda, \mu, \nu] = [\mu, \lambda, \nu],$$
$$h_1 = (\infty \;\; [1, 0, 0])f_1.$$

In matrix form,

$$g = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

so that $\det(g) = -1 = 1 \in \mathrm{GF}(4)$ and $g \in \mathrm{PSL}(3, 4)$. It is plain that g does not fix $x = [1, 0, 0]$ and, by the lemma, that $h_1^2 = 1$. The following computation shows that $(gh_1)^3 = 1$. If $[\lambda, \mu, \nu] \neq \infty$, $[1, 0, 0]$, or $[0, 1, 0]$, then

$$(gh_1)^3[\lambda, \mu, \nu] = [\lambda\nu + \mu^2(\nu^3 + 1), \mu\nu + \lambda^2(\nu^3 + 1), \nu^2].$$

If $\nu \neq 0$, then $\nu^3 = 1$ and $\nu^3 + 1 = 0$, so that the right side is $[\lambda\nu, \mu\nu, \nu^2] =$

$[\lambda, \mu, \nu]$. If $\nu = 0$, then the right side is $[\mu^2, \lambda^2, 0]$; since $\lambda\mu \neq 0$, by our initial choice of $[\lambda, \mu, \nu]$, we have $[\mu^2, \lambda^2, 0] = [(\lambda\mu)\mu^2, (\lambda\mu)\lambda^2, 0] = [\lambda, \mu, 0]$. The reader may show that $(gh_1)^3$ also fixes ∞, $[1, 0, 0]$, and $[0, 1, 0]$, so that $(gh_1)^3 = 1$.

Finally, assume that $k \in G_x \leq \mathrm{PSL}(3, 4)$, so that k is the coset (mod scalar matrices) of

$$k = \begin{bmatrix} 1 & * & * \\ 0 & a & b \\ 0 & c & d \end{bmatrix}$$

(because k fixes $[1, 0, 0]$). Now $\det(k) = 1 = ad - bc$. The reader may now calculate that $h_1 k h_1$, mod scalars, is

$$h_1 k h_1 = \begin{bmatrix} 1 & * & * \\ 0 & a^2 & b^2 \\ 0 & c^2 & d^2 \end{bmatrix}$$

which fixes $[1, 0, 0]$ and whose determinant is $a^2d^2 - b^2c^2 = (ad - bc)^2 = 1$. Thus $h_1 G_x h_1 = G_x$, and Theorem 9.51 shows that $M_{22} = \langle \mathrm{PSL}(3, 4), h_1 \rangle$ acts 3-transitively on $\tilde{X} = P^2(4) \cup \{\infty\}$ with $(M_{22})_\infty = \mathrm{PSL}(3, 4)$.

By Theorem 9.7, $|M_{22}| = 22 \cdot 21 \cdot 20 \cdot |H|$, where H is the stabilizer in M_{22} of three points. Since $(M_{22})_\infty = \mathrm{PSL}(3, 4)$, we may consider H as the stabilizer in PSL(3, 4) of two points, say, $[1, 0, 0]$ and $[0, 1, 0]$. If $A \in \mathrm{SL}(3, 4)$ sends $(1, 0, 0)$ to $(\alpha, 0, 0)$ and $(0, 1, 0)$ to $(0, \beta, 0)$, then A has the form

$$A = \begin{bmatrix} \alpha & 0 & \gamma \\ 0 & \beta & \delta \\ 0 & 0 & \eta \end{bmatrix},$$

where $\eta = (\alpha\beta)^{-1}$. There are 3 choices for each of α and β, and 4 choices for each of γ and δ, so that there are 144 such matrices A. Dividing by SZ(3, 4) (which has order 3), we see that $|H| = 48$. ■

Theorem 9.56. *There exists a 4-transitive group M_{23} of degree 23 and order* $10{,}200{,}960 = 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48 = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$ *such that the stabilizer of a point is M_{22}.*

Proof. The proof is similar to that for M_{22}, and so we only provide the necessary ingredients. Adjoin a new symbol ω to $P^2(4) \cup \{\infty\}$, and let

$$x = \infty,$$
$$g = (\infty \;\; [1, 0, 0])f_1 = \text{the former } h_1,$$
$$h_2 = (\omega \;\; \infty)f_2.$$

The reader may apply Theorem 9.51 to show that $M_{23} = \langle M_{22}, h_2 \rangle$ is a transitive extension of M_{22}. ■

Theorem 9.57. *There exists a 5-transitive group M_{24} of degree 24 and order* $244{,}823{,}040 = 24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48 = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$ *such that the stabilizer of a point is M_{23}.*

Proof. Adjoin a new symbol Ω to $P^2(4) \cup \{\infty, \omega\}$, and define

$$x = \omega,$$

$$g = (\omega\ \infty)f_2 = \text{the former } h_2,$$

$$h_3 = (\Omega\ \omega)f_3.$$

The reader may check that Theorem 9.51 gives $M_{24} = \langle M_{23}, h_3 \rangle$ a transitive extension of M_{23}. ∎

Theorem 9.58 (Miller, 1900). *The Mathieu groups M_{22}, M_{23}, and M_{24} are simple groups.*

Proof. Since M_{22} is 3-transitive of degree 22 (which is not a power of 2) and since the stabilizer of a point is the simple group PSL(3, 4), Theorem 9.25(ii) gives simplicity of M_{22}. The group M_{23} is 4-transitive and the stabilizer of a point is the simple group M_{22}, so that Theorem 9.25(i) gives simplicity of M_{23}. Finally, M_{24} is 5-transitive and the stabilizer of a point is the simple group M_{23}, so that Theorem 9.25(i) applies again to give simplicity of M_{24}. ∎

Theorem 9.59 (Cole, 1896; Miller, 1899). *The Mathieu groups M_{11} and M_{12} are simple.*

Proof. Theorem 9.25(i) will give simplicity of M_{12} once we prove that M_{11} is simple. The simplicity of M_{11} cannot be proved in this way because the stabilizer of a point is M_{10}, which is not a simple group.

Let H be a nontrivial normal subgroup of M_{11}. By Theorem 9.17, H is transitive of degree 11, so that $|H|$ is divisible by 11. Let P be a Sylow 11-subgroup of H. Since $(11)^2$ does not divide $|M_{11}|$, P is also a Sylow 11-subgroup of M_{11}, and P is cyclic of order 11.

We claim that $P \neq N_H(P)$. Otherwise, P abelian implies $P \leq C_H(P) \leq N_H(P)$ and $N_H(P)/C_H(P) = 1$. Burnside's normal complement theorem (Theorem 7.50) applies: P has a normal complement Q in H. Now $|Q|$ is not divisible by 11, so that $Q \operatorname{char} H$; as $H \lhd M_{11}$, Lemma 5.20(ii) gives $Q \lhd M_{11}$. If $Q \neq 1$, then Theorem 9.17 shows that $|Q|$ is divisible by 11, a contradiction. If $Q = 1$, then $P = H$. In this case, H is abelian, and Exercise 9.10 gives H a regular normal subgroup, contradicting Lemma 9.24.

Let us compute $N_{M_{11}}(P)$. In S_{11}, there are $11!/11 = 10!$ 11-cycles, and hence 9! cyclic subgroups of order 11 (each of which consists of 10 11-cycles and the identity). Therefore $[S_{11} : N_{S_{11}}(P)] = 9!$ and $|N_{S_{11}}(P)| = 110$. Now $N_{M_{11}}(P) = N_{S_{11}}(P) \cap M_{11}$. We may assume that $P = \langle \sigma \rangle$, where $\sigma = (1\ 2\ \ldots\ 10\ 11)$; 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 $M_{11} \leq A_{11}$, so that $|N_{M_{11}}(P)| = 11$ or 55. Now $P \leq N_H(P) \leq N_{M_{11}}(P)$, 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 $N_H(P) \leq H$), 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 $\langle \mathbf{V}, h \rangle \geq A_5$.)

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 $\langle \mathrm{PSL}(3, 4), h_2, h_3 \rangle \leq M_{24}$ 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 $k \leq v$, 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 $X = P^2(q)$ 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 $m \geq 3$, and let $\mathscr{B}$ be the family of all planes (affine 2-subsets of X). Since three