Advanced Studies in Pure Mathematics 32, 2001
Groups and Combinatorics — in memory of Michio Suzuki
pp. 255–277

Steiner systems and Mathieu groups revisited

Helmut Bender

These notes about an old topic of Witt (Abh. Hbg. 1938) describe a further approach to the relevant existence and isomorphism theorems for Steiner systems. Some standard information about the automorphism groups is obtained along the way. Actually, I wish to proceed by group theoretic arguments as much as possible. Besides Sylow's Theorem, including

$$|G : N_G(P)| \equiv 1(p) \quad \text{for} \quad P \in Syl_p(G),$$

and the most obvious properties of the 2-dimensional linear groups over $GF(11)$ and $GF(9)$, they mainly require some formalities around transitive action of a group G on a set Ω, above all

$$|\Omega| = |G : G_\alpha| \quad \text{for} \quad \alpha \in \Omega.$$

I also mention the "Frattini argument", "Witt's Lemma", and the concept of a Frobenius group:

The first gives $G = HG_\alpha = G_\alpha H$ for any transitive subgroup H, the second states that the normalizer $N_G(X)$ of a subgroup (or subset) $X \subseteq G_\alpha$ is transitive on the set Ω_X of fixed points if (and only if) X is "very weakly closed" in G_α, that is all G-conjugates $X^g \subseteq G_\alpha$ are already conjugate to X in G_α. The standard X besides $X = G_\alpha$ is a Sylow subgroup of G_α. Trivially, Witt's Lemma implies the analogous result for n-fold transitive groups.

Thirdly, to say that G is a Frobenius group on Ω, means that $1 \neq G_\alpha \neq G$ and $G_{\alpha\beta} = 1$ for all $\beta \neq \alpha$. We ignore Frobenius' famous theorem and assume also that G_α has a complement K in G. Then K is regular on Ω, is the set of all elements of G not conjugate to an element $\neq 1$ of G_α, and is called the Frobenius kernel of G. Accordingly, an abstract Frobenius group is a semi-direct product $G = KA$ (with K normal) such that the above holds for a suitable "G-set" Ω and with $A = G_\alpha$, or equivalently no element of K commutes with an element

Received September 22, 1999.

outside, or equivalently no element of A commutes with an element outside.

For other treatments of our topic see Lüneburgs paper (J. Alg. 1968) related to Witt's, Aschbacher's book "Sporadic Groups", and the bibliography in the "Atlas".

This paper is dedicated to the memory of Michio Suzuki. In 1964 I had to study one of his papers (characterizing linear groups) as a participant of Reinhold Baer's seminar at Frankfurt university, under the supervision of Baer's assistant Bernd Fischer. It was my third seminar already, but the first time that I found the mathematics confronting me attractive. Reading Suzuki's papers then became the main occupation for the rest of my student life.

Suzuki was a pioneer of modern group theory which culminated in the classification of the finite simple groups, and he contributed crucially to quite a few rather different main topics. To describe his role for the classification I like to compare the Sylow 2-subgroups of a finite group with fortresses in an area to be forced under one's complete control. In order to exert such a control, our fortresses must be strong and must have good lines of communications (good coherence in more group theoretic language). Thus, Suzuki laid much of the basis for a powerful 2-local structure theory.

Pioneers will be followed by others, more convenient ways will be constructed, and after a while their foot steps are not so apparent any more. This does however not apply to the bulk of Suzuki's work, on certain types of permutation groups and related topics, which in its depth and beauty will forever remain a jewel in the field of finite groups.

§1. Steiner systems

1.1. **Lemma.** *Let Ω be a finite set, $0 \leq t \leq k \leq v = |\Omega|$, and $\mathcal{B}$ a set of k-subsets of Ω. Then, with*

$$\mathcal{B}(X) = \{B \in \mathcal{B} \mid X \subseteq B\} \text{ and } b(t,k,v) = \binom{v}{t} / \binom{k}{t},$$

the following conditions (a), (b), (c) *are equivalent*:

(a) $|\mathcal{B}(X)| = 1$ *for all t-subsets $X \subseteq \Omega$,*

(b) $|\mathcal{B}| = b(t,k,v)$ *and* $|\mathcal{B}(X)| \leq 1$ *for all t-subsets $X \subseteq \Omega$,*

(c) $|\mathcal{B}| = b(t,k,v)$ *and* $|\mathcal{B}(X)| \geq 1$ *for all t-subsets $X \subseteq \Omega$.*

Proof. There are $\binom{v}{t}$ t-subsets X of Ω, and each $B \in \mathcal{B}$ contains $\binom{k}{t}$ such subsets X. Thus the number of pairs (X, B) with $X \subseteq B$ equals both $|\mathcal{B}| \cdot \binom{k}{t}$ and $\sum_X |\mathcal{B}(X)|$, and this sum has $\binom{v}{t}$ summands. Q.E.D.

1.2. **Definition.** In the situation of Lemma 1.1, with one (hence each) of (a), (b), (c) valid, $\mathcal{B}$ is a Steiner system of type (t,k,v), or just (t,k), on Ω.

We write $\mathcal{B} \in S(t,k,v,\Omega)$ and drop Ω or v whenever suitable.

The sets $B \in \mathcal{B}$ are called blocks, sometimes lines, and the elements $\alpha \in \Omega$ points. The block containing a t-set X is denoted by $\langle X \rangle$. A collinear subset of Ω is contained in some block.

An isomorphism from $\mathcal{B}$ onto another Steiner system $\hat{\mathcal{B}}$ with point set $\hat{\Omega}$ is a bijective mapping φ from Ω onto $\hat{\Omega}$ such that $\mathcal{B}\varphi = \hat{\mathcal{B}}$.

1.3. Thus the automorphism group of $\mathcal{B} \in S(t,k,v,\Omega)$ is the stabilizer of $\mathcal{B}$ in the symmetric group $Sym(\Omega)$. The number of conjugates of $\mathcal{B}$ under $Sym(\Omega)$ is $v!/|Aut(\mathcal{B})|$. All (t,k,v)-systems are isomorphic if and only if all $\mathcal{B}$ are conjugate under $Sym(\Omega)$.

1.4. For $\mathcal{B} \in S(t,k,v,\Omega)$ and $J \subseteq \Omega$, with $j = |J| \leq t$, the set

$$\mathcal{B}((J)) = \{B \setminus J \mid B \in \mathcal{B}(J)\}$$

is a $(t-j, k-j, v-j)$-system on $\Omega \setminus J$. In particular,

$$|\mathcal{B}(J)| = |\mathcal{B}((J))| = b(t-j, k-j, v-j).$$

From $b(t,k,v) = \frac{v}{k} \cdot b(t-1,k-1,v-1)$ (for $t > 0$) we get the following table. There is no continuation to the right because neither $2 \cdot 66 \cdot \frac{13}{7}$ nor $23 \cdot 11 \cdot 3 \cdot \frac{25}{9}$ is an integer.

(t,k,v):	$(1,2,8)$	$(2,3,9)$	$(3,4,10)$	$(4,5,11)$	$(5,6,12)$
$b(t,k,v)$:	4	12	30	66	$2 \cdot 66$

(t,k,v):	$(1,4,20)$	$(2,5,21)$	$(3,6,22)$	$(4,7,23)$	$(5,8,24)$
$b(t,k,v)$:	5	21	77	$23 \cdot 11$	$23 \cdot 11 \cdot 3$

1.5. For $\alpha \in \Omega$ call $\mathcal{B}, \hat{\mathcal{B}} \in S(t,k,v,\Omega)$ α-equivalent if $\mathcal{B}(\alpha) = \hat{\mathcal{B}}(\alpha)$. We also say that $\mathcal{B}$ and $\hat{\mathcal{B}}$ agree on α. Clearly, the number of α-equivalence classes is at most $|S(t-1,k-1,\Omega \setminus \{\alpha\})|$ (assume $t \geq 1$).

So with $\ell(t,k,v)$ the maximal length of an α-equivalence class (where now α ranges over Ω, and $\ell(t,k,v) = 0$ if $S(t,k,v)$ is empty), we have

$$|S(t,k,\Omega)| \leq \ell(t,k,v) \cdot |S(t-1,k-1,\Omega \setminus \{\alpha\})|.$$

As an example, we consider the case $(t,k,v) = (5,6,12)$ and prove

$$\ell(5,6,12) \leq 1.$$

This means that any α-equivalent $\mathcal{B}, \hat{\mathcal{B}} \in S(t,k,v,\Omega)$ are actually equal. Assume $\mathcal{B} \neq \hat{\mathcal{B}}$, say some $B \in \hat{\mathcal{B}}$ does not belong to $\mathcal{B}$. Then $\alpha \notin B$, and each 5-set $X \subseteq B$ lies in a unique block $X \cup \{\beta\}$ of $\mathcal{B}$ (not in $\hat{\mathcal{B}}$). These (six) points $\beta = \beta(X)$ are pairwise distinct and distinct from α. Thus $\Omega \geq |B| + 6 + 1 = 13$, a contradiction. It is also true, though less obvious, that $\ell(5,8,24) \leq 1$.

1.6. **The Trivial Isomorphism Theorem.** *For $1 \leq t \leq k \leq v$ assume some $\mathcal{B} \in S(t,k,v)$ exists. Write g for $|Aut(\mathcal{B})|$. Then all $\mathcal{B}$ are isomorphic, with $g = g'v/n$, provided*

(i) *all $\mathcal{B}' \in S(t-1,k-1,v-1)$ are isomorphic, with $|Aut(\mathcal{B}')| = g'$, and*

(ii) *n is an integer such that $\ell(t,k,v) < 2n$ and gn divides $g'v$ for all $\mathcal{B}$.*

Proof. We apply 1.3 and 1.5. Fix $\mathcal{B}$ with point set Ω for a moment. Write $g'v = gnq$. Then the $Sym(\Omega)$-orbit containing $\mathcal{B}$ has length

$$\frac{v!}{g} = \frac{nqv!}{g'v} = \frac{nq(v-1)!}{g'}.$$

With q minimal and r the number of all orbits it follows that

$$r\frac{nq(v-1)!}{g'} \leq |S(t,k,\Omega)| < 2n\frac{(v-1)!}{g'}$$

and hence $rnq < 2n$, thus $r = q = 1$. Q.E.D.

1.7. **The Trivial Induction Lemma.** *Assume $2 \leq t \leq k \leq |\Omega|$.*

(a) *For each $\alpha \in \Omega$ let $\mathcal{B}_\alpha \in S(t-1,k-1,\Omega \setminus \{\alpha\})$, and assume $\mathcal{B}_\alpha((\beta)) = \mathcal{B}_\beta((\alpha))$ for all points $\beta \neq \alpha$. Then*

$$\mathcal{B} = \{B \subseteq \Omega \mid B \setminus \{\alpha\} \in \mathcal{B}_\alpha \text{ for some } \alpha \in B\}$$

is a Steiner system of type (t,k) on Ω.

(b) *Assume (a group) G acts on Ω, for each $\alpha \in \Omega$ there is a unique G_α-invariant $\mathcal{B}_\alpha \in S(t-1,k-1,\Omega\setminus\{\alpha\})$, and for any two distinct points $\alpha, \beta \in \Omega$ there is a unique $G_{\alpha\beta}$-invariant $\mathcal{B}_{\alpha\beta} \in S(t-2,k-2,\Omega\setminus\{\alpha,\beta\})$, or, more generally, $\mathcal{B}_\alpha((\beta)) = \mathcal{B}_\beta((\alpha))$.*

Then there is a unique G-invariant $\mathcal{B} \in S(t,k,\Omega)$.

Proof. The point about the condition $\mathcal{B}_\alpha((\beta)) = \mathcal{B}_\beta((\alpha))$ in (a) is that $B \setminus \{\alpha\} \in \mathcal{B}_\alpha$ holds not only for some, but for every element α of a given $B \in \mathcal{B}$: Assume it holds for α and let $\alpha \neq \beta \in B$. Then $D = (B\setminus\{\alpha\})\setminus\{\beta\}$ lies in $\mathcal{B}_\alpha((\beta)) = \mathcal{B}_\beta((\alpha))$, that is $B\setminus\{\beta\} = D\cup\{\alpha\}$ lies in $\mathcal{B}_\beta$.

To prove (a), hence (b), we have to show that a unique $B \in \mathcal{B}$ contains a given t-subset $X \subseteq \Omega$. Existence: Choose $\alpha \in X$, $U \in \mathcal{B}_\alpha(X \setminus \{\alpha\})$, and let $B = \{\alpha\} \cup U$. Uniqueness: If $X \subseteq A \in \mathcal{B}$, then, by the first paragraph, $A \setminus \{\alpha\}$ is also a block in $\mathcal{B}_\alpha$ which contains $X \setminus \{\alpha\}$, hence is equal to U. Q.E.D.

1.8. **Lemma.** *Assume G is a Frobenius group on a 9-set Ω, and the Frobenius kernel of G is elementary abelian (of order 9).*

(a) *There exists a unique G-invariant $\mathcal{B} \in S(2,3,\Omega)$.*

(b) *For each $\alpha \in \Omega$, $\mathcal{B}((\alpha))$ consists of the four orbits of length 2 under the subgroup of order 2 in G_α.*

Proof. First we consider any G-invariant $\mathcal{B} \in S(2,3,\Omega)$. A subgroup T of order 2 has one fixed point α and four orbits X of length 2 in Ω. For each X, the block $\langle X \rangle$ is T-invariant and hence equals $X \cup \{\alpha\}$. This proves (b), hence gives uniqueness in (a).

For existence we apply 1.7(a). For each $\alpha \in \Omega$ let $\mathcal{B}_\alpha$ be the set of all T-orbits of length 2, where T is the subgroup of order 2 in G_α. For $\alpha \neq \beta \in \Omega$ let $D \simeq S_3$ be the subgroup generated by T and the analogous subgroup of order 2 in G_β. Then βD is a D-invariant 3-subset of Ω, hence contains a fixed point of T, that is α. Now the third point γ in $\alpha D = \beta D$ satisfies $\mathcal{B}_\alpha((\beta)) = \{\gamma\} = \mathcal{B}_\beta((\alpha))$. Q.E.D.

1.9. **Corollary** (by 1.7(b)). *Let G be a transitive group of order $9 \cdot 4 \cdot 10$ or $9 \cdot 8 \cdot 10$ on a 10-set Ω. For $\alpha \in \Omega$, assume G_α to be a Frobenius group on $\Omega \setminus \{\alpha\}$.*

Then G leaves a unique $\mathcal{B} \in S(3,4,\Omega)$ invariant.

1.10. **Theorem.** *Let $t \geq 2$, $v = t+7$, $k = t+1$, and G a sharply t-transitive group on a v-set Ω.*

Then $t \leq 5$ and G leaves a unique $\mathcal{B} \in S(t,k,\Omega)$ invariant. All blocks are conjugate, and a k-subset B is a block if and only if $G_B \simeq S_k$.

Proof. The unique $\mathcal{B}$ comes from 1.8(a) for $t = 2$, from 1.9 for $t = 3$, then from 1.7(b) for $t = 4, 5, 6, \ldots$. By 1.4, $S(t,k,v)$ is empty for $t \geq 6$.

We have $|G| = v \cdot (v-1) \cdots (v-(t-1))$ and $|G_B| \leq k!$ because G_B is faithful on B. Thus

$$|B^G| = |G : G_B| \geq \frac{|G|}{k!} = b(t,k,v)$$

whence $G_B \simeq S_k$ means $|B^G| = b(t,k,v)$, hence $B^G \in S(t,k,\Omega)$ by Lemma 1.1 because each t-subset of Ω is conjugate to a subset of B. Q.E.D.

1.11. **Lemma.** *Some G as in* 1.9 *is isomorphic to A_6, and then any subgroup $H \simeq A_5$ is transitive.*

Conversely, If $H \simeq A_5$ acts transitively on a 10*-set Ω, then there exists a unique H-invariant $\mathcal{B} \in S(3,4,\Omega)$ and for each $\alpha \in \Omega$, $\mathcal{B}((\alpha))$ is the only H_α-invariant (2,3)-system on $\Omega \setminus \{\alpha\}$.*

Proof. Let Λ be any 6-set, $G = Alt(\Lambda)$, and Ω the set of all sets $\{X, Y\}$, where X and Y are disjoint 3-subsets of Λ. Then $|\Omega| = 10$, $|G| = 6!/2 = 9 \cdot 4 \cdot 10$, and no element order 5, 3, or 2 in G fixes 1, 2, or 3 points in Ω, respectively. Thus G and Ω are as in 1.9.

Then any subgroup H of order 60 is transitive because any stabilizer $|H_\alpha|$ ($\alpha \in \Omega$), a subgroup of the Frobenius group G_α of order $9 \cdot 4$, has order at most 6.

All transitive H-sets of length 10 are isomorphic because all subgroups of order 6 in H are conjugate. As for uniqueness of $\mathcal{B}((\alpha))$, hence of $\mathcal{B}$, any such (2,3,9)-system consists of the 10 3-sets invariant under a subgroup of order 2 in $H_\alpha \simeq S_3$, and the two additional orbits under the subgroup of order 3. Q.E.D.

1.12. In analogy with $\ell(t,k,v) = \ell_1(t,k,v)$ defined in 1.5 we can define $\ell_p(t,k,v)$ for each integer $p \geq 1$ as the maximal length of a J-equivalence class in $S(t,k,v,\Omega)$, where J ranges over all p-subsets of Ω, and J-equivalence means α-equivalence for all $\alpha \in J$.

In other words, $\ell_p(t,k,v) \leq m$ means that not more than m (t,k,v)-systems $\mathcal{B}$ on Ω can "agree" on p points, in case $m = 1$ that any $\mathcal{B}$ is completely determined by any p 1-residues $\mathcal{B}((\alpha))$.

Obviously, the argument in 1.5 for $\ell(5,6,12) \leq 1$ also gives $\ell_2(4,5,11) \leq 1$ and $\ell_3(3,4,10) \leq 1$. In section 3 the latter will be improved to $\ell_2(3,4,10) \leq 1$ (actually to the stronger condition (*)(3,4,10) introduced below).

The condition $\ell_2(t,k,v) \leq 1$ is very convenient when we wish to get information on $\ell(t,k,v)$:

(a) To prove $\ell(t,k,v) \leq m$ it suffices to show that if $\mathcal{B}((\alpha))$ is given, there are at most m possibilities for any second 1-residue $\mathcal{B}((\beta))$.

More formally, with $\ell'(t,k,v)$ the maximal number of β-equivalence classes inside an α-equivalence class (in any case $\leq \ell(t,k,v)$),

$$\ell_2((t,k,v) \leq 1 \qquad \text{implies} \qquad \ell(t,k,v) = \ell'(t,k,v).$$

Below we also prove that for any $p \geq 1$,

(b) $\ell_2(t,k,v) \leq 1$ implies $\ell_p(t+1,k+1,v+1) \leq \ell_p(t,k,v)$.

This suffices for the small cases (3,4,10), (4,5,11), and (5,6,12). For the large cases (3,6,22), (4,7,23), and (5,8,24) a finer distinction appears

to be appropriate. The following condition (*) lies between $\ell(t,k,v) \leq 1$ and $\ell_2(t,k,v) \leq 1$. For the small cases, when $k = t+1$, it means that two distinct (t,k,v)-systems on Ω which agree on a point α (are α-equivalent), have only those blocks in common which contain α, indeed a much stronger statement than $\ell_2(t,k,v) \leq 1$.

(*) Whenever distinct $\mathcal{B}_1, \mathcal{B}_2 \in S(t,k,v,\Omega)$ agree on a point $\alpha \in \Omega$, then $|B_1 \cap B_2| \leq t$ for all $B_1 \in \mathcal{B}_1$ and $B_2 \in \mathcal{B}_2$ not containing α.

We assume $2 < t < k < v$ and prove the following results.

(c) The above condition (*) is equivalent to the following condition

(**) Whenever $\mathcal{B}_1, \mathcal{B}_2 \in S(t,k,v,\Omega)$ agree on a point $\alpha \in \Omega$, and B_1, B_2 are blocks in $\mathcal{B}_1$, $\mathcal{B}_2$, respectively, which do not contain α and satisfy $|B_1 \cap B_2| > t$, then $\mathcal{B}_1(\beta) = \mathcal{B}_2(\beta)$ for all $\beta \in B_1 \cap B_2$.

(d) (*) implies the analogous condition $(*)(t+1, k+1, v+1)$.

Proof of (b): We rather assume $\ell_2(t-1,k-1,v-1) \leq 1$ and show that $m = \ell_p(t,k,v)$ is $\leq \ell_p(t-1,k-1,v-1)$.

Let $\mathcal{B}_1, \ldots, \mathcal{B}_m \in S(t,k,v,\Omega)$ be J-equivalent and pairwise distinct, with J a p-subset of Ω. For $\beta \in \Omega \setminus J$ the $(t-1,k-1,v-1)$-systems $\mathcal{B}_i((\beta))$ are J-equivalent. To show they are pairwise distinct (whence $m \leq \ell_p(t-1,k-1,v-1)$) assume $\mathcal{B}_1(\beta) = \mathcal{B}_2(\beta)$. For each further point $\gamma \in \Omega \setminus J$, the $(t-1,k-1,v-1)$-systems $\mathcal{B}_1((\gamma))$ and $\mathcal{B}_2((\gamma))$ agree on β and each of the $p \geq 1$ points $\alpha \in J$, hence are equal because $\ell_2(t-1,k-1,v-1) \leq 1$. It follows that $\mathcal{B}_1 = \mathcal{B}_2$, a contradiction.

Proof of (c): Trivially, (*) implies (**). So assume (**) and let B_1, B_2 contradict (*). Then $|B_1 \cap B_2| > t$ and (**) implies $\mathcal{B}_1(\beta) = \mathcal{B}_2(\beta)$ for all $\beta \in B_1 \cap B_2$. There exists $\gamma \in \Omega$ such that $\mathcal{B}_1(\gamma) \neq \mathcal{B}_2(\gamma)$, because $\mathcal{B}_1 \neq \mathcal{B}_2$. Fix β. There exists $B \in \mathcal{B}_1(\beta,\gamma) \setminus \mathcal{B}_1(\alpha,\beta,\gamma)$ because $t > 2$ and $v > k$. Then $B \in \mathcal{B}_2$, and we can apply (**) with B in place of B_1 and B_2 to get $\mathcal{B}_1(\gamma) = \mathcal{B}_2(\gamma)$, a contradiction.

Proof of (d): It suffices to derive (**) from $(*)(t-1,k-1,v-1)$. Assume the hypothesis of (**). For each $\beta \in B_1 \cap B_2$ apply $(*)(t-1,k-1,v-1)$ to $\mathcal{B}_i((\beta))$ to get $\mathcal{B}_1((\beta)) = \mathcal{B}_2((\beta))$.

Finally we combine most of the above to get

(e) $(**)(t,k,v)$ plus $\ell'(t,k,v) \leq m$ implies $(*)(t+i,k+i,v+i)$ and $\ell(t+i,k+i,v+i) \leq m$ for all $i \geq 0$.

§2. Affine planes of order 3 and 4

2.1. Let $L \in \mathcal{B} \in S(2,k,v,\Omega)$ and $\alpha \in \Omega \setminus L$. By 1.4 there are $b(1,k-1,v-1) = v-1/k-1$ blocks through α, and k of them meet B.

By definition, $\mathcal{B}$ is an affine plane (of order k) if (for all L and α) exactly one block through α does not meet L (is parallel to L). So this

means $v - 1/k - 1 = k + 1$, hence also $v = k^2$. In case of an affine plane, blocks will henceforth also be called lines, and parallelism of lines is an equivalence relation on $\mathcal{B}$.

Also by definition, $\mathcal{B}$ is a projective plane (of order $k-1$) if any two blocks intersect non-trivially, that is $v - 1/k - 1 = k$. This also means that the set $\mathcal{B}^L$ of all the sets $B \setminus B \cap L$, where $L \neq B \in \mathcal{B}$, is an affine plane of order $k-1$ on $\Omega \setminus L$.

2.2. If $\mathcal{B}$ in 2.1 is an affine plane, any two non-parallel lines $H = \{a_{11}, \ldots, a_{1k}\}$ and $V = \{a_{11}, \ldots, a_{k1}\}$ yield a $k \times k$-matrix $A = (a_{ij})$ whose rows and columns are the parallels of H and V respectively. Just define a_{ij} to be the unique point on the parallel of H through a_{i1}, and the parallel of V through a_{1j} . Any further line contains exactly one point from each row and each column.

2.3. Assume $k = 3$ in 2.2, that is $\mathcal{B} \in S(2, 3, 9, \Omega)$, and write ij for a_{ij}. Quite obviously, the additional $b(2, 3, 9) - (3 + 3) = 6$ lines are the two diagonals 11 22 33, 13 22 31, and the four triangles

$$\begin{pmatrix} 11 & \cdot & \cdot \\ \cdot & \cdot & 23 \\ \cdot & 32 & \cdot \end{pmatrix} \begin{pmatrix} \cdot & \cdot & 13 \\ 21 & \cdot & \cdot \\ \cdot & 32 & \cdot \end{pmatrix} \begin{pmatrix} \cdot & 12 & \cdot \\ \cdot & \cdot & 23 \\ 31 & \cdot & \cdot \end{pmatrix} \begin{pmatrix} \cdot & 12 & \cdot \\ 21 & \cdot & \cdot \\ \cdot & \cdot & 33 \end{pmatrix}.$$

So if another $\hat{\mathcal{B}} \in S(2, 3, 9)$ is analogously represented by a matrix $\hat{A} = (\hat{a}_{ij})$, then the mapping $a_{ij} \to \hat{a}_{ij}$ is an isomorphism from $\mathcal{B}$ onto $\hat{\mathcal{B}}$.

It follows that all $\mathcal{B}$'s are isomorphic, with $Aut(\mathcal{B})$ sharply transitive on the set of triples (a, b, x) of non-collinear points (each (a, b, x) equals $(11, 12, 21)$ for some unique A).

Thus $Aut(\mathcal{B})$ has order $9 \cdot 8 \cdot 6$, is doubly transitive on the points, and the stabilizer of two points a, b fixes the third point on the line through a and b, and is sharply transitive on the remaining 6 points.

2.4. If $k = 4$ in 2.2, that is $\mathcal{B} \in S(2, 4, 16)$, the lines are not determined by the matrix $A = (a_{ij}) = (ij)$. The line through 11 and 22 might be the diagonal 11 22 33 44 or the set 11 22 34 43. Interchanging the last two points in the sequence V however, results in interchanging the last two rows of the matrix. The diagonal of the new matrix is a line if and only if the diagonal of A is not.

So for a quadruple (a, b, c, x) of pairwise distinct non-collinear points, with a, b, c collinear, there is a unique matrix A with $(a, b, c, x) = (11, 12, 13, 21)$ and the diagonal 11 22 33 44 a line.

We show that such a "regular" quadruple determines $\mathcal{B}$ via its matrix. The only point sets containing exactly one point from each row, each column, and the diagonal, are

11 23 34 42 13 22 34 41 12 24 33 41 12 23 31 44
11 24 32 43 14 22 31 43 14 21 33 42 13 21 32 44

and all these sets must be lines because each point (on the diagonal) lies on exactly $v - 1/k - 1 = 5$ lines. Now there are only $b(2,5,21) - (4 + 4 + 1 + 8) = 3$ lines left, and the only candidates are 12 21 34 43, 13 24 31 42, and 14 23 32 41.

So in analogy with 2.3 all $\mathcal{B}$'s are isomorphic, with $Aut(\mathcal{B})$ sharply transitive on regular quadruples, hence of order $16 \cdot 15 \cdot 2 \cdot 12$.

§3. Steiner systems of type (3,4,10), (4,5,11) and (5,6,12)

3.1. Let $\mathcal{B} \in S(3,4,10,\Omega)$. Choose a block $\{a', a, b, c\}$ and a further point x. Apply 2.3 to the (2,3,9)-systems $\mathcal{B}((a'))$ and $\mathcal{B}((a))$ with the non-collinear triples (a,b,x) and (a',b,x). We get matrices

$$A = \begin{pmatrix} a & b & c \\ x & y & z \\ u & v & w \end{pmatrix} \qquad A' = \begin{pmatrix} a' & b & c \\ x & y' & z' \\ u & v' & w' \end{pmatrix}$$

such that the blocks through a', without a', are the rows, columns, diagonals, and the four triangles of the matrix A, likewise for a and A'. Given A, that is $\mathcal{B}(a')$, A' is one of

$$\begin{pmatrix} a' & b & c \\ x & w & v \\ u & z & y \end{pmatrix} \quad \begin{pmatrix} a' & b & c \\ x & v & y \\ u & w & z \end{pmatrix} \quad \begin{pmatrix} a' & b & c \\ x & z & w \\ u & y & v \end{pmatrix}$$

because $\{y,w\}$ and $\{y',w'\}$ are equal or disjoint ($a'ayw$ and $aa'y'w'$ are blocks),
$w' \neq w$ ($a'bxw$ and $abxw'$ are blocks),
$v' \neq v$ ($a'xvc$ and $axv'c$ are blocks), and
$\{y',v'\} \neq \{y,v\}$ ($a'byv$ and $aby'v'$ are blocks).

Accordingly, the fourth point in $B = \langle a,b,x\rangle$ is $w' = y, z$, or v. So if B is also a block in another $\hat{\mathcal{B}} \in S(3,4,\Omega)$ with $\hat{\mathcal{B}}(a') = \mathcal{B}(a')$, then the matrix $A'(\hat{\mathcal{B}})$ analogous to $A' = A'(\mathcal{B})$ (again with respect to (a',a,b,c,x)) is equal to A' (because one of the three above), and this means $\hat{\mathcal{B}}(a) = \mathcal{B}(a)$.

3.2. **Lemma.** (a) *Condition* 1.12(**)(3,4,10) *holds.*
(b) *We have* $\ell'(3,4,10) \leq 3$.
(c) *We have* $\ell(3,4,10) \leq 3$.
(d) *We have* $\ell(4,5,11) \leq 3$.
(e) *We have* $\ell(5,6,12) \leq 1$.

Proof. (a) Write $\mathcal{B}$ and $\hat{\mathcal{B}}$ for $\mathcal{B}_1$ and $\mathcal{B}_2$, respectively, and B for B_1 and $B_2 = B_1$. For $\beta \in B$ we have to verify $\mathcal{B}(\beta) = \hat{\mathcal{B}}(\beta)$. Apply 3.1 with $a' = \alpha$, $a = \beta$, and $b, x \in B$.

(b) In 3.1 we have seen that for arbitrary points $a' \neq a$, once $\mathcal{B}(a')$ is given, there are at most three possibilities for $\mathcal{B}(a)$

Now (c) and (d) follow from 1.12(e), and (e) has been proved in 1.5. Q.E.D.

3.3. **Lemma.** *For $\mathcal{B}$ as in* 3.1, *the stabilizer of three points in $G = Aut(\mathcal{B})$ has at most order* 2. *In particular, $|G|$ divides* $10 \cdot 9 \cdot 8 \cdot 2$.

Proof. Otherwise 2.3 shows that $\Omega_X \in \mathcal{B}$ for some subgroup X of order 3. For each of the four $\alpha \in \Omega_X$ there are two more X-invariant $B \in \mathcal{B}(\alpha)$ because $|\mathcal{B}(\alpha)| = b(2,3,9) = 12$. However, there are only two X-orbits of length 3 in Ω. Q.E.D.

3.4. **Theorem.** *All $\mathcal{B} \in S(3,4,10)$ are isomorphic, with $Aut(\mathcal{B})$ of order* $10 \cdot 9 \cdot 8 \cdot 2$, *triply transitive on the points, and isomorphic to $P\Gamma L_2(9)$.*

Proof. By 2.3 all $\mathcal{B}' \in S(2,3,9)$ are isomorphic, with $g' = Aut(\mathcal{B}') = 9 \cdot 8 \cdot 6$. Thus 3.2(c) and 3.3 allow to apply 1.6 with $n = 3$.

The group $P\Gamma L_2(9)$ acts faithfully on a 10-set, and we can apply 1.9 to the (sharply 3-transitive) normal subgroup $PGL_2(9)$ of index 2 (also to the normal subgroup $L_2(9) = PSL_2(9)$ of index 4). Q.E.D.

3.5. **Corollary** (by 1.11). *The alternating group A_6 is isomorphic to $L_2(9)$.*

3.6. **Theorem.** *All $\mathcal{B} \in S(4,5,11)$ are isomorphic, with $Aut(\mathcal{B})$ of order* $11 \cdot 10 \cdot 9 \cdot 8$ *and sharply* 4*-transitive on the points.*

Proof. Let $\mathcal{B} \in S(4,5,11,\Omega)$. First we show that the stabilizer X of four points is trivial, so that in particular $g = |Aut(\mathcal{B})|$ divides $11 \cdot 10 \cdot 9 \cdot 8$. Otherwise $|X| = 2$ by 3.3, and $|\Omega_X| = 5$ by 2.3. Let J be an X-orbit of length 2. Again by 2.3, X fixes only 3 points of $\mathcal{B}((J))$, a contradiction.

Now 3.2(d) and 3.4 allow to apply 1.6 with $g' = 10 \cdot 9 \cdot 8 \cdot 2$ and $n = 2$. Q.E.D.

3.7. **Theorem.** *All $\mathcal{B} \in S(5,6,12)$ are isomorphic, with $Aut(\mathcal{B})$ of order* $12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$ *and sharply* 5*-transitive on the points.*

Proof. 3.2(e) and 3.6 allow to apply 1.6 with $n = 1$. Q.E.D.

Existence of a (5,6,12)-system (hence of a (4,5,11)-system) will be proved in 3.9 below. Then M_{12} (and M_{11}) will denote the automorphism group of such a Steiner system.

3.8. **Lemma.** *Let L be a group "of type $L_2(11)$", in the sense that L has order $11 \cdot 5 \cdot 12$ and a non-normal subgroup E of order 11.*

(a) *$N_L(E)$ has order $11 \cdot 5$.*

(b) *L acts transitively on some 12-set Ω such that $N_L(E) = L_\alpha$ for some $\alpha \in \Omega$.*

(c) *A subgroup $D \subseteq L_\alpha$ of order 5 fixes only one additional point $\beta \in \Omega$.*

(d) *$N_L(D) = D\langle t \rangle$ with $t \notin C_L(D)$ an involution.*

(e) *Any $11'$-subgroup containing D lies in $N_L(D)$ or is isomorphic to A_5.*

Proof. By Sylow's Theorem, $|L : N_L(E)| \equiv 1$ modulo 11. This yields (a), hence (b). D is not normal in L because otherwise L/D were a Frobenius group of order $11 \cdot 12$. Thus ED is a Frobenius group on $\Omega \setminus \{\alpha\}$. This implies (c) and $|N_L(D)| = 10$. If an involution t would centralize D, $C_L(t)/\langle t \rangle$ were a Frobenius group of order $5 \cdot 6$. Finally, a subgroup of order 60 is simple by (d). Q.E.D.

3.9. **Theorem.** *In the situation of* 3.8, *L leaves some $\mathcal{B} \in S(5,6,\Omega)$ invariant. In particular, M_{12} has a (point$-$) transitive subgroup isomorphic to L.*

Proof. No element of order 2 or 3 fixes a point. So t interchanges the two fixed points of D, as well as the two orbits X_1, X_2 of length 5. Furthermore, each 5-set $X \subseteq \Omega$ with $L_X \neq 1$ is conjugate to X_1 (and X_2) and satisfies $|L_X| = 5$. Hence there are $|L|/5 = 11 \cdot 12$ such 5-sets X and each other 5-set $X' \subseteq \Omega$ has $|L| = 11 \cdot 12 \cdot 5$ conjugates. Since the latter number equals $\binom{12}{5} - 11 \cdot 12$, all X' are conjugate.

The (global) stabilizer of any of the two 6-sets $B_i = X_i \cup \{\alpha\}$ is D because L has no subgroup of order $5 \cdot 6$. It follows that the L-invariant sets $\mathcal{B}_i = B_i{}^G$ are disjoint and have $11 \cdot 12 = b(5,6,12)$ elements.

We verify that $\mathcal{B}_1$ or $\mathcal{B}_2$ is as required. Define $f_i = \mathcal{B}_i(X)$ and $f_i' = \mathcal{B}_i(X')$ with X and X' as above. Then the number of pairs (Z,B) with $B \in \mathcal{B}_i$ and Z a 5-subset of B, equals both $11 \cdot 12 \cdot f_i + 11 \cdot 12 \cdot 5 f_i'$ and $11 \cdot 12 \cdot 6$. It follows that $f_i + 5f_i' = 6$. However, $f_1 + f_2 \leq 7$ because a 5-subset of Ω lies in only seven 6-subsets. Thus $f_i' \neq 0$ for some i, and then $f_i = f_i' = 1$.

By the way, if $L = L_2(11)$ and Ω is a $PGL_2(11)$-set, then both $\mathcal{B}_i$ are conjugate under $PGL_2(11)$, hence are (5,6,12)-systems on Ω. Q.E.D.

3.10. Assume the notation of 3.8 and 3.9 with $L \subseteq G = Aut(\mathcal{B}) \simeq M_{12}$. Let $H = G_\alpha \simeq M_{11}$. Then

(a) $N_G(E) = N_H(E) = ED$,
(b) $N_G(D)$ has order $5 \cdot 8$,
(c) $N_H(D)$ is a Frobenius group of order $5 \cdot 4$ fixing two blocks in $\mathcal{B}$,
(d) the groups L, H, and G are simple,
(e) L has a subgroup isomorphic to A_5,
(f) L acts transitively on some 11-set Λ, and then leaves a unique (4,5)-system on Λ invariant,
(g) $M_{11} \simeq H$ has a subgroup isomorphic to L,
(h) H acts transitively on some 12-set Δ, and then leaves a unique (5,6)-system on Δ invariant.

Proof. (a) follows from $|G| = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$, $|G : N_G(E)| \equiv 1(11)$, and $C_G(E) = E$ (whence $|N_G(E) : E|$ divides 10). The same argument proves (b) and (c) because no $5'$-element $\neq 1$ of $C_G(D)$ fixes the two D-orbits of length 5, and D fixes exactly one of the $b(4,5,11) = 66$ blocks in $\mathcal{B}(\alpha)$.

For (d) note that a proper normal subgroup K of the group X in question satisfies $N_K(E) = K \cap ED = 1$ if $E \not\subseteq K$, and $X = N_X(E)K = DK$ (by the Frattini argument) if $E \subseteq K$. The second case contradicts $N_X(D) \neq C_X(D)$. In the first case, $|K| - 1$ is divisible by 11, but $|K|$ is not equal to 12. Define $(X_0, X_1, X_2, X_3) = (ED, L, H, G)$ and let $X = X_{i+1}$ with $i = 0$ or X_i simple. Then $K \cap X_i = 1$, hence $|K| \leq |X : X_i| = 12$, that is $|K| = 1$.

(e) Since $|G : L| = 12 \cdot 12 = 144$, G acts transitively on some 144-set Λ such that $G_\lambda = L$ for some $\lambda \in \Lambda$. Since $N_G(E) \subseteq L$, λ is the only fixed point of E, by Witt's Lemma. So if (e) is false, 3.8(e) implies that the length of any other L-orbit is divisible by $11 \cdot 5$ or $11 \cdot 6$, contrary to $2 \cdot 66 < 143$ and $3 \cdot 55 > 143$.

(f) Existence comes from (e) because $|L| = 60 \cdot 11$. Conversely, for any Λ, a one-point-stabilizer $A = L_\lambda$ is isomorphic to A_5 by 3.8(e). A Sylow 2- or 5-subgroup S of A satisfies $N_L(S) \subseteq A$, hence fixes no second point in Λ, by Witt's Lemma. Thus A is transitive on $\Lambda \setminus \{\lambda\}$, and the second part of 1.11 allows to apply 1.7(b).

(g) follows from (f) and implies existence in (h). Conversely, for any Δ, a one-point-stabilizer H_δ is of type $L_2(11)$ and (trivially) transitive on the 11-set $\Delta \setminus \{\delta\}$. Thus

(f) and the fact (from 1.11) that A in the proof of (f) leaves a unique (3,4)-system on $\Lambda \setminus \{\lambda\}$ invariant, allow to apply 1.7(b) again. Q.E.D.

Remarks. (i) By 3.10(b)(c), $N_G(D)/D$ is the direct product of the cyclic groups $N_H(D)/D$ and $C_G(D)/D$ of order 4 and 2. Thus $N_G(D)$ has only two Frobenius subgroups of order $5 \cdot 4$. Since $H = \langle E, N_H(D) \rangle$, it follows that all transitive subgroups $\simeq M_{11}$ are conjugate in G, that is those not conjugate to H. Similarly, because $N_G(D)$ has only two non-abelian subgroups of order 10, G has exactly two classes of subgroups of type $L_2(11)$, and H has only one. In particular, all groups of type $L_2(11)$ are isomorphic. Conjugacy of transitive subgroups $\simeq M_{11}$ will also follow from 4.5 and 4.7.

(ii) Our existence proof for $S(5,6,12)$ is a slight variation (avoiding explicit calculations) of what Carmichael suggests in section 115 of his book "Groups of Finite Order" (1937). He suggests an analogous procedure for $S(5,8,24)$, based on the transitive action of $L_2(23)$ on 24 points. We will follow a different line in 4.11. It gives the inclusion of $Aut(M_{12})$ in M_{24} as a by-result, and has the inclusion of $L_2(23)$ as a consequence.

(iii) From 1.10 and the isomorphism theorems of this section one easily obtains all sharply t-transitive finite permutation groups for $t \geq 4$. Proceeding by induction on t, one only has to show that in case $t = 4$ the degree v equals 4, 6, or 11.

(iv) As indicated in 1.12, 1.12(a)(b) suffices for this section. Indeed, it suffices to have $\ell_2(3,4,10) \leq 1$ in place of 3.2(a). Here is a direct proof for $\ell_2(3,4,10) \leq 1$: It suffices to show (in 3.1) that $\mathcal{B}(a')$ and $\mathcal{B}(a)$ determine $\mathcal{B}(\gamma)$ for any third point γ, say $\gamma = b$. Let

$$A'' = \begin{pmatrix} a' & a & c \\ x & y'' & z'' \\ u'' & v'' & w'' \end{pmatrix}$$

be the matrix describing $\mathcal{B}((b))$ relative to the non-collinear triple (a', a, x). Then

u'' = fourth point on the block through a', x, b $(= w)$,
w'' = fourth point on the block through a, x, b $(= w')$,
z'' = fourth point on the block through a, u'', b,
y'' = fourth point on the block through a', w'', b, and
v'' = fourth point on the block through a, y'', b.

(v) In accordance with the three possibilities for the matrix A' in 3.1, there are three types of non-collinear quadruples. Each type occurs, and (hence) $Aut(\mathcal{B})$ permutes the quadruples of each type sharply transitively.

§4. The automorphism group of M_{12}

$G^* = Aut(M_{12})$ has a normal subgroup $G = Inn(M_{12}) \simeq M_{12}$ and acts transitively on a set Ω^* such that $M_{11} \simeq G^*_\alpha \subseteq G$ for some $\alpha \in \Omega^*$, and there exists a G-invariant (5,6,12)-system $\mathcal{B}$ on the G-orbit $\Omega = \alpha^G$ of length 12.

The set of subgroups $H \simeq M_{11}$ in G is denoted by $\mathcal{H}$. By 3.10(h) some H is transitive on Ω, that is not conjugate to $G_1 = G_\alpha$.

4.1. For $j = 1, 2, 3, 4$ the stabilizer G_j of j points $\alpha, \beta, \ldots$ is sharply $(5-j)$-transitive on the set Ω_j of the remaining points.

The global stabilizer N_j of $\Omega^j = \{\alpha, \beta, \ldots\}$ is equal to $N_G(G_j)$, and N_j/G_j is sharply j-transitive on Ω^j, hence isomorphic to S_j.

Acting faithfully on $\mathcal{B}_j = \mathcal{B}((\Omega^j)) \in S(5-j, 6-j, 12-j, \Omega_j)$, and having the right order, N_j induces the full automorphism group on $\mathcal{B}_j$ for $j \leq 3$.

In particular, N_2 is isomorphic to $P\Gamma L_2(9)$ (by 3.4).

4.2. **Corollary.** (a) *G_3 is a Frobenius group of order $9 \cdot 8$.*
(b) *$Q = G_4$ has order 8 and contains only one involution.*
(c) *$N_G(Q)/Q \simeq S_4$ and $N_{G_1}(Q)/Q \simeq S_3$.*
(d) *G_2 has a normal subgroup $G_2' \simeq L_2(9) \simeq A_6$ of index 2.*

4.3. **Lemma.** (a) *G_2 is not isomorphic to S_6.*
(b) *If G_1 acts transitively on some 11-set, then G_2 fixes a point and (hence) G_1 is sharply 4-transitive.*

Proof. (a) Q contains only one involution and has index 2 in some Sylow 2-subgroup of G_2, whereas S_6 has an elementary subgroup of order 8.

(b) Otherwise G_2' has an orbit X of length 6 and five orbits of length 1 ($L_2(9)$ cannot act transitively on $11, 9, 8, 7, 5, 4, 3,$ *or* 2 *points*). This contradicts (a) because X is G_2-invariant. Q.E.D.

4.4. **Corollary** (of 4.3(b) and 1.10). *If G acts transitively on a 12-set Ω', with $G_{\alpha'} \in \mathcal{H}$ for $\alpha' \in \Omega'$, then G is sharply 5-transitive and leaves a unique $\mathcal{B}' \in S(5, 6, \Omega')$ invariant.*

G is block-transitive, and a set B of six points is a block if and only if $G_B \simeq S_6$.

4.5. **Theorem.** *$Aut(G)$ is transitive on $\mathcal{H}$.*

Proof. For each $H \in \mathcal{H}$ there exist Ω' and α' as in 4.4 such that $H = G_{\alpha'}$. Since $\mathcal{B}'$ is isomorphic to $\mathcal{B}$, there exists a monomorphism

from G into $M = Aut(\mathcal{B})$ which maps $G_{\alpha'}$ into M_α. Apply this also to $\mathcal{B}$ and α in place of $\mathcal{B}'$ and α', and recall that $M \simeq M_{12} \simeq G$. Q.E.D.

4.6. **Lemma.** *For $E \subseteq G$ of order 11, $C_{G^*}(E) = E$.*

Proof. By 3.10, $C_G(E) = E$ and $N_G(E) = ED$ with D of order 5. Assume $E \subset V = C_{G^*}(E)$. Choose $d \neq 1$ in D. Then the $|V : C_V(d)|$-set $[V, d]$ of commutators $[v, d] = v^{-1}d^{-1}vd$ with $v \in V$ lies in $C_G(E) = E$. It follows that $U = C_V(d) = C_V(D)$ is not trivial. By 3.10, $C_G(D)$ is cyclic of order 10, hence lies in $K = C_G(U)$.

By Sylow's Theorem, $|X : Y| \equiv 1$ modulo 11 for all subgroups $X \supseteq Y \supseteq ED$ of G. So $|K : ED|$ equals 12 or $12 \cdot 12$ because $|G : ED| = 12 \cdot 12 \cdot 12$. In the first case K is of type $L_2(11)$, contrary to 3.8(d).

Hence $|K : ED| = 12 \cdot 12$ and $|[G, u]| = |G : C_G(u)| = |G : K| = 12$ for each $u \neq 1$ in U. Since $[G, u]$ is invariant under $C_G(u)$, hence under ED, the 11 non-identity elements in $[G, u]$ are conjugate under E, and one of them is centralized by D. Thus all the commutators $[g, u]$ with $g \in G$ and $u \in U$ lie in K. However, the subgroup $[G, U]$ generated by them is normal in G, contrary to simplicity of $G \simeq M_{12}$. Q.E.D.

4.7. **Theorem.** *We have $|G^* : G| = 2$, $N_{G^*}(G_1) \subseteq G$, and G^* is transitive on $\mathcal{H}$.*

Proof. Since $|N_G(E) : E| = 5$ and $G^* = N_{G^*}(E)G$ by the Frattini argument, this follows from 4.5 and 4.6 because G is not transitive on $\mathcal{H}$. Q.E.D.

4.8. **Corollary.** (a) *There is exactly one G-orbit $\Omega' \neq \Omega$ in Ω^*.*

(b) *For (each) $f \in G^* \setminus G$ and $\mathcal{B}'$ as in 4.4 we have $\Omega' = \Omega^f$ and $\mathcal{B}' = \mathcal{B}^f$.*

(c) *Furthermore, G_1^f is transitive on Ω, and (hence) $G_1^f \cap G_1$ is of type $L_2(11)$.*

4.9. **Lemma.** *Each 4-subset of Ω is fixed elementwise by exactly one involution in G. The set J of these involutions has (therefore) $\binom{12}{4}$ elements and is invariant under G^* (whence $|\Omega_t'| = 4$ for each $t \in J$).*

Proof. $Q = G_4$ has only one involution by 4.2(b). Let $Q \simeq P \subseteq G$. Then the involution t in P is trivial on each P-orbit of length $< |P| = 8$. Thus one P-orbit has length 8, and the remaining four points in Ω are fixed by t. Q.E.D.

4.10. **Lemma.** *For each block $B \in \mathcal{B}$,*

(a) *$C = \Omega \setminus B \in \mathcal{B}$ and $L = G_B = G_C \simeq S_6$,*

(b) *L has a unique orbit $F = F(B)$ of length 2 in $\Omega^*(itliesin\Omega')$,*

(c) $F = F(A)$ *with* $A \in \mathcal{B}$ *implies* $A \in \{B, C\}$,
(d) $t \in G_F$ *with* Ω_t *not empty implies* $t \in L$,
(e) $|(A \cup F(A)) \cap (B \cup F)| \geq 5$ *implies* $A = B$,
(f) $|\Omega_t^* \cap (B \cup F)| \leq 4$ *for* $t \in J$, J *as in* 4.9, *and*
(g) $|\Omega_s \cap \Omega_t| \leq 2$ *for distinct* $s, t \in J$ *fixing* F *elementwise.*

Proof. The last assertion of 4.4 yields (a). The subgroup $M = G_2' \simeq L_2(9) \simeq A_6$ of $G_2 \subseteq G_1$ does not fix two points in Ω' because otherwise M^f ($f \in G^* \setminus G$) were conjugate to M in G, contrary to 4.8(c). Hence Ω' has two M-orbits of length 6, say U and $V = \Omega' \setminus U$. Since M has order $6!/2$ and index 4 in $N = N_2 = N_G(M)$, it follows that U and V are interchanged by N and fixed by some subgroup $S \simeq S_6$ of index 2 (G_U is faithful on U). Then U is a block in the unique G-invariant $\mathcal{B}' \in S(5, 6, \Omega')$, hence conjugate to B by some $f \in G^* \setminus G$, and this completes the proof of (b) because $S = G_U$ leaves $\{\alpha, \beta\}$ invariant and is distinct from G_2 by 4.3(a).

The subgroup $L_0 \simeq A_6$ of L is the unique subgroup of index 4 in $G_F \simeq N_2$, and the only L_0-orbits in Ω are B and C. This yields (c), and for (d) note that t cannot interchange B and C.

Let $Y = A \cap B$ in (e). The case $|Y| \geq 5$ is trivial, also the case $|Y| = 3$ because then $F = F(A)$. Assume $|Y| = 4$. There still exists $x \in F \cap F(A)$. By 4.9, a unique involution $t \in G$ fixes Y elementwise. Since L induces $Sym(B)$ on B, t lies in L, but (as a transposition on B) not in L_0. Hence $\{x, x^t\}$ equals F and by symmetry also $F(A)$.

Let $Y = \Omega_t \cap B$ in (f). If $|Y| = 4$, then as above t does not fix a point in F. If $|Y| = 3$ and t fixes F elementwise, then $t \in L_0$ by (d), a contradiction because $Y \subseteq B_t$ implies t is a transposition on B.

Let $Y = \Omega_s \cap \Omega_t$ in (g) and assume $|Y| = 3$. Again s and t lie in L_0, and $\langle s, t \rangle$ is dihedral of order 6 by 4.2(a). Action on B and C shows that $|B \cap Y| \neq 2, 3$ and $|C \cap Y| \neq 2, 3$, a contradiction. Q.E.D.

4.11. **Theorem.** $G^* = Aut(M_{12})$ *leaves a Steiner system* $\mathcal{B}^*$ *of type* $(5, 8, 24)$ *on* Ω^* *invariant, namely* $\mathcal{B}^* = \mathcal{B}_1 \cup \mathcal{B}_2$ *where* $\mathcal{B}_1$ *is the set of all* 8*-sets* $B \cup F(B)$, *with* $B \in \mathcal{B} \cup \mathcal{B}'$ *and* $F(B)$ *defined by* 4.10(b) *and* $\mathcal{B}_2$ *is the set of all* 8*-sets* Ω_t^*, *with* $t \in J$, J *as in* 4.9.

Proof. From $|\mathcal{B}_1| = |\mathcal{B}| + |\mathcal{B}'| = 2 \cdot b(5, 6, 12) = 4 \cdot 66$ and $|\mathcal{B}_2| = |J| = \binom{12}{4} = 11 \cdot 5 \cdot 9$ we get $|\mathcal{B}^*| = |\mathcal{B}_1| + |\mathcal{B}_2| = 11 \cdot 3 \cdot (8+15) = b(5, 8, 24)$. So by 1.1 it suffices to verify $|\mathcal{B}^*(X)| \leq 1$ for each 5-set $X \subseteq \Omega$. Without loss, $|X \cap \Omega| \geq 3$. Thus 4.10(e)(f)(g) does the job. Note that the condition about F in (g) means no loss of generality because G is doubly transitive on Ω'. Q.E.D.

4.12. **Corollary.** *Assume (what will be shown in* 8.2*) that* $M = Aut(\mathcal{B}^*)$ *has order* $24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48$. *Then* M *has a subgroup isomorphic to* $L_2(23)$, *and all these subgroups are conjugate.*

Proof. Regard G^* as a subgroup of M. A subgroup $L \simeq L_2(23)$ of $S = Sym(\Omega^*)$ is generated by a subgroup P of order 23, a subgroup $E \subseteq N_S(P)$ of order 11, and an involution $t \in N_L(E)$. Let $P \subseteq M$. Then $|N_M(P)| = 23 \cdot 11$ and (hence) $E \subseteq M$ because $|M : N_M(P)| \equiv 1(23)$ and $|N_S(P) : PE| = 2$. Let $E \subseteq G$. Then 4.6 yields an involution $f \in G^* \setminus G$ which inverts E (recall that $|N_G(E)| = 11 \cdot 5$). Interchanging Ω and Ω', f is fixed-point-free on $\Omega^* = \Omega \cup \Omega'$. However, because $|\Omega_E^*| = 2$, the elements of Et are the only fixed-point-free involutions of S which invert E (the product of any two such involutions x, y centralizes E, is inverted by x and y, and leaves the two fixed points of E and the two orbits of length 11 invariant). Q.E.D.

§5. Steiner systems of type (2,5,21)

5.1. Assume $\mathcal{B} \in S(2, 5, 21, \Omega)$ and $L \in \mathcal{B}$. By 2.1, $\mathcal{B}$ is a projective plane of order 4. For each line X of the affine plane $\mathcal{B}^L$ of order 4 defined in 2.1 there is a unique point $p = p(X)$ in L such that $X \cup \{p\} \in \mathcal{B}$, and a line Y is parallel to X if and only if $p(X) = p(Y)$.

Thus each isomorphism from $\mathcal{B}^L$ on a similar affine plane $\hat{\mathcal{B}}^{\hat{L}}$ extends uniquely to an isomorphism from $\mathcal{B}$ on $\hat{\mathcal{B}}$. Since $\mathcal{B}$ has 21 blocks, and by 2.4 there are $16 \cdot 15 \cdot 24$ isomorphisms between any two affine planes of order 4, it follows that all projective planes of order 4 are isomorphic and $Aut(\mathcal{B})$ has order $21 \cdot 16 \cdot 15 \cdot 24$.

5.2. More precisely, $G = Aut(\mathcal{B})$ is block-transitive and the block stabilizer G_L is sharply transitive on the set of regular quadruples (a, b, c, x) of $\mathcal{B}^L$ in the sense of 2.4.

So if a subgroup $T \neq 1$ of G_L fixes a block $B \neq L$ elementwise, then $\Omega_T \subseteq L \cup B$ and hence B is unique.

5.3. Assume a subgroup $T \subseteq G$ of order 2 fixes a block B elementwise. Then T fixes no additional point α.

Proof. Otherwise a second point $\beta \in \Omega \setminus B$ is fixed by T because $|\Omega \setminus B| = 16$ is even. By 5.2, β lies in each of the five blocks $L = \langle \alpha, \lambda \rangle$ ($\lambda \in B$), a contradiction. Q.E.D.

5.4. Using the description of $\mathcal{B}^L$ by a 4×4-matrix $A = (ij)$ in 2.4, based on a regular quadruple $(a, b, c, x) = (11, 12, 13, 21)$, we get the following list of blocks:

H_1 : 11 12 13 14 h	V_1 : 11 21 31 41 v	L : $h\ v\ u\ t\ s$
H_2 : 21 22 23 24 h	V_2 : 12 22 32 42 v	
H_3 : 31 32 33 34 h	V_3 : 13 23 33 43 v	
H_4 : 41 42 43 44 h	V_4 : 14 24 34 44 v	
U_1 : 11 22 33 44 u	T_1 : 11 23 34 42 t	S_1 : 11 24 32 43 s
U_2 : 12 21 34 43 u	T_2 : 12 24 33 41 t	S_2 : 12 23 31 44 s
U_3 : 13 24 31 42 u	T_3 : 13 21 32 44 t	S_3 : 13 22 34 41 s
U_4 : 14 23 32 41 u	T_4 : 14 22 31 43 t	S_4 : 14 21 33 42 s

§6. Steiner systems of type (3,6,22)

Although a little less straightforward, this section is totally analogous to the first part of section 3.

6.1. Let $\mathcal{B} \in S(3,6,22,\Omega)$. We begin with a sequence (call it regular)

$$q = (a', L, a, b, c, x)$$

such that $a' \in L \in \mathcal{B}$ and a, b, c, x are non-collinear points outside L, with a', a, b, c however collinear.

Existence of q is quite obvious. Actually, for any four non-collinear points a', a, b, x there exists a block $L \in \mathcal{B}(a')$ containing none of them, because

$$|\mathcal{B}(a')| = 21 > 5 + 5 + 5 = |\mathcal{B}(a'a)| + |\mathcal{B}(a', b)| + |\mathcal{B}(a', x)|;$$

then choose the fifth point c in $\langle a', a, b\rangle$ outside L.

We apply 5.4 to $\mathcal{B}((a')) \in S(2,5,21)$ and get a matrix

$$A = \begin{pmatrix} 11 & 12 & 13 & 14 \\ 21 & 22 & 23 & 24 \\ 31 & 32 & 33 & 34 \\ 41 & 42 & 43 & 44 \end{pmatrix} = \begin{pmatrix} a & b & c & 14 \\ x & 22 & 23 & 24 \\ 31 & 32 & 33 & 34 \\ 41 & 42 & 43 & 44 \end{pmatrix}$$

and points $h, v, u, t, s \in L$ such that the blocks in $\mathcal{B}(a')$ are given by the list in 5.4 (add a' everywhere). The blocks H_1, V_1, U_1, T_1, S_1 constitute $\mathcal{B}(a, a')$ and are also denoted by H, V, U, T, S. Note that

$$H = h\ a'\ a\ b\ c\ 14 \quad \text{and} \quad V = v\ a'\ a\ x\ 31\ 41.$$

It follows that the sequence $q' = (a, L', a', b, c, x)$ with $L' = \langle a, h, v\rangle$ is regular too. It yields an analogous description of $\mathcal{B}(a)$ involving a matrix

$$A' = \begin{pmatrix} 11' & 12' & 13' & 14' \\ 21' & 22' & 23' & 24' \\ 31' & 32' & 33' & 34' \\ 41' & 42' & 43' & 44' \end{pmatrix} = \begin{pmatrix} a' & 12 & 13 & 14 \\ 21 & 22' & 23' & 24' \\ 31' & 32' & 33' & 34' \\ 41' & 42' & 43' & 44' \end{pmatrix}$$

and points $h', v', u', t', s' \in L'$. We have $h' = h$, $v' = v$, and $31\ 41 = 31'\ 41'$.

The fact that q'' equals q constitutes a useful symmetry in our situation.

6.2. Since $\mathcal{B}(a, a')$ also consists of $H' = H$, $V' = V$, U', T' and S', it follows that

$$\{U, T, S\} = \{U', T', S'\}$$

and that $X_i' \neq Y_j$ for any two letters X, Y among H, V, U, T, S and any two numbers i, j among 1, 2, 3, 4 not both 1.

6.3. Since $L' \cap L = h\ v = h'\ v'$, each of u', t', s' equals some ij $(i, j \in \{2, 3, 4\})$. No two of them lie in the same row or column of the matrix A.

Otherwise the block H_i or V_j corresponding to that row or column would have three points in common with L', namely those two plus h or v.

6.4. **Lemma.** *We have* $31' = 31$ *and* $41' = 41$.

Proof. Assume this key result is false, that is $31' = 41$ and $41' = 31$. Then $U_4' \cap T_4 = 14\ 31$, $U_3' \cap S_3 = 13\ 41$, and $S_2' \cap T_2 = 12\ 41$. This implies

$$u' \neq 22, 43, 34 \qquad \text{and} \qquad s' \neq 24, 33$$

as well as $t \neq 23', 32', 44'$ and $s \neq 42'$, hence, by symmetry,

$$t' \neq 23, 32, 44 \qquad \text{and} \qquad s' \neq 42.$$

The remaining possibilities for u', t', and s' are listed in the three tables below. They contain also the corresponding values for U', T', and S' which follow from 6.2. The addition $[t']$ for example to the value $u' = 32$ means that in this case a look at t' immediately yields a contradiction: Indeed, the values 24 and 43 for t' violate $U' \neq T'$, and

the remaining values 22, 33, 34, 42 violate 6.3.

u' :	$33[s']$	$44[t']$	$23[t']$	$42[s']$	$24[s']$	$32[t']$
U' :	U	U	T	T	S	S
t' :	22	33	34	42	24	43
T' :	U	U	T	T	S	S
s' :	22	44	23	34	32	43
S' :	U	U	T	T	S	S

Q.E.D.

6.5. **Lemma.** *We have $U' = U$, $T' = T$, and $S' = S$, that is*

$$u'\ 22'\ 33'\ 44' = u\ 22\ 33\ 44, \qquad t'\ 23'\ 34'\ 24' = t\ 23\ 34\ 24,$$

and

$$s'\ 24'\ 32'\ 43' = s\ 24\ 32\ 43.$$

Proof. This is now very easy. From $U_2' \cap U_2 = 12\ 21$, $U_3' \cap U_3 = 13\ 31$, and $U_4' \cap U_4 = 14\ 41$ it follows that u' is distinct from 34, 43, 24, 42, 23, and 32, hence equal to 22, 33, or 44. This implies $U' = U$ by 6.2, and the same argument, now exploiting the intersections $T_i' \cap T_i$ $(i = 2, 3, 4)$, yields $T' = T$. Q.E.D.

6.6. Obviously, only three possibilities for (u', t', s') are compatible with 6.3 and 6.5, and analogously for (u, t, s):

u'	t'	s'	u	t	s
22	34	43	$22'$	$34'$	$43'$
33	42	24	$33'$	$42'$	$24'$
44	23	32	$44'$	$23'$	$32'$

Moreover, $u' = nn$ implies $u = nn'$:

To prove this addition, assume first the case $u' = 22$. Then $U_4' \cap T_4 = 14\ 22$ and hence $t \neq 23'$. Also, $U_3' \cap S_3 = 13\ 22$ and hence $s \neq 24'$. Thus the second table leaves only the case $(u, t, s) = (22', 34', 43')$.

By symmetry, $u = 22'$ implies $u' = 22$. So to complete the proof it suffices to verify $s \neq 32'$ in case $u' = 33$, and this follows from $U_4' \cap S_4 = 14\ 33$.

6.7. **Theorem.** *The matrix $A' = (ij')$ is one of the following:*

$$\begin{pmatrix} 11 & 12 & 13 & 14 \\ 21 & u & 42 & 32 \\ 31 & 24 & 44 & t \\ 41 & 23 & s & 33 \end{pmatrix} \quad \begin{pmatrix} 11 & 12 & 13 & 14 \\ 21 & 44 & 34 & s \\ 31 & 43 & u & 23 \\ 41 & t & 32 & 22 \end{pmatrix} \quad \begin{pmatrix} 11 & 12 & 13 & 14 \\ 21 & 33 & t & 43 \\ 31 & s & 22 & 42 \\ 41 & 34 & 24 & u \end{pmatrix}$$

Proof. Apply 6.4, 6.5, 6.6, and the fact that $ij' \neq ij$ for all $i, j \in \{2, 3, 4\}$ (otherwise $H_i = \langle h, i1, ij \rangle = H_i'$). Q.E.D.

6.8. **Corollary.** *In accordance with the three cases of* 6.7,

$$\langle a, b, x \rangle \setminus \{a, b, x\} = U_2' \setminus \{11, 12, 21\} = \{34', 43', u'\}$$

equals one of the pairwise disjoint sets t s 22, 23 32 33, *and* 42 24 44.

6.9. **Corollary.** *If* $\mathcal{B}_2 \in S(3, 6, \Omega)$ *satisfies* $\mathcal{B}_2(a') = \mathcal{B}(a')$ *and* $B_1 \cap B_2 \supset \{a, b, x\}$ *for some* $B_2 \in \mathcal{B}_2$ *and* $B_1 \in \mathcal{B}$, *then* $\mathcal{B}_2(a) = \mathcal{B}(a)$.

Proof. Apply all the above to $\mathcal{B}_2$ in place of $\mathcal{B}$, relative to the same regular sequence (a', L, a, b, c, x), hence the same matrix A. Again, the matrix A_2' analogous to A' is one of the three in 6.7, and the non-disjoint sets $B_1 \setminus \{a, b, x\}$ and $B_2 \setminus \{a, b, x\}$ are among the three sets listed in 6.8, hence are equal. This means $A_2' = A'$, that is $\mathcal{B}_2(a) = \mathcal{B}(a)$. Q.E.D.

6.10. **Lemma.** (a) *Condition* 1.12(**)(3, 6, 22) *holds.*
(b) *We have* $\ell'(3, 6, 22) \leq 3$.

Proof. (a) Write $\mathcal{B}$ for $\mathcal{B}_1$, a' for α, and a for $\beta \in B_1 \cap B_2$. Choose further points b and x in $B_1 \cap B_2$. Then a', a, b, x are not collinear because $a' \notin B_i$. Thus q as in 3.1 exists, and we can apply 6.9.

(b) Recall that any two points can play the role of a' and a in 3.1. Thus (b) means that in 3.1, once $\mathcal{B}(a')$ is given, that is A is given, there are at most three possibilities for $\mathcal{B}(a)$, that is for A'. Now apply 6.7. Q.E.D.

6.11. **Lemma.** *Let* W *be the pointwise stabilizer in* $G = Aut(\mathcal{B})$ *of a block* B. *Then* $W_\alpha = 1$ *for all* $\alpha \in \Omega \setminus B$. *In particular,* $|W|$ *divides* 16, *the order of any three-point-stabilizer divides* $16 \cdot 6$, *and (hence)* $|G|$ *divides* $22 \cdot 21 \cdot 20 \cdot 16 \cdot 6$.

Proof. Assume $T \subseteq W_\alpha$ has prime order p. The 15 2-sets X of the 6-set B yield 15 T-invariant blocks $\langle X, \alpha \rangle$. Only two of them may lie in Ω_T, by 5.2 applied to $\mathcal{B}((\alpha))$. Thus Ω has 13 T-orbits of length p, a contradiction. Q.E.D.

6.12. **Theorem.** *All Steiner systems of type* (3, 6, 22) *are isomorphic, and their automorphism group has order* $22 \cdot 21 \cdot 20 \cdot 16 \cdot 6$.

Proof. Recall from 5.1 that Steiner systems of type (2,5,21) are isomorphic and have $g' = 21 \cdot 20 \cdot 16 \cdot 6 \cdot 3$ automorphisms. By 6.10 and 1.12(e) we have $\ell(3, 6, 22) \leq 3$. This together with 6.11 allows to apply 1.6 with $n = 3$. Q.E.D.

6.13. **Corollary.** (a) *$G = Aut(\mathcal{B})$ is 3-transitive on Ω, and the stabilizer of three points has order $16 \cdot 6$.*

(b) *G is block-transitive, and the stabilizer $H = G_B$ of a block B is 3-transitive (actually 6−transitive by (c)) on B, and has order $6 \cdot 5 \cdot 4 \cdot 16 \cdot 6 = 6! \cdot 16$.*

(c) *W as in 6.11 has order 16, and H/W is isomorphic to S_6.*

(d) *A subgroup $D \subseteq H$ of order 5 fixes exactly two points and two (disjoint) blocks.*

(e) *D satisfies $C_H(D) = 1$, $|N_H(D)| = 5 \cdot 4$, $|N_G(D)| = 5 \cdot 8$, the involution s in $C_G(D)$ interchanges the two D-invariant points and blocks, and s has (therefore) no fixed-point.*

(f) *W is elementary abelian, sharply transitive on $\Omega \setminus B$, and equal to $C_G(W)$.*

(g) *If $E \subseteq G$ has order 11, then $N_G(E)$ is a Frobenius group of order $11 \cdot 10$ transitive on Ω.*

For (g) note that $|C_G(E) : E| \leq 2$, $|G : N_G(E)| \equiv 1(11)$, and in case $s \in C_G(E)$ also $|C_G(s) : N_G(E)| \equiv 1 \equiv |G : C_G(s)|$ modulo $11 \cdot 5$.

6.14. **Corollary.** *$G = Aut(\mathcal{B})$ has a subgroup isomorphic to $PGL_2(11)$, and all these subgroups are conjugate.*

Proof. Analogous to 4.12. A subgroup $L \simeq PGL_2(11)$ of $S = Sym(\Omega)$ is generated by a transitive Frobenius subgroup F of order $11 \cdot 10$, and an involution t which inverts a subgroup $D^* \subseteq F$ of order 10 and fixes the two D^*-orbits of length 10 as well as the two remaining points.

By 6.13(g), F is conjugate in S to a subgroup of G. Let $F \subseteq G$. By 6.13(e), G contains an involution like t. Obviously, the product of any two such involutions in S lies in D^*. Q.E.D.

§7. The Isomorphism Theorem for S(4,7,23)

7.1. Let $B \in \mathcal{B} \in S(4, 7, 23, \Omega)$ and $G = Aut(\mathcal{B})$. First we show that the order of the stabilizer of any four points (without loss in B) divides $16 \cdot 3$, and (hence) $|G|$ divides $23 \cdot 22 \cdot 21 \cdot 20 \cdot 16 \cdot 3$.

By 6.11, that order k divides $16 \cdot 6$. So if the assertion is false, then some subgroup $T \subseteq G_B$ of order 2 fixes a 5-set $X \subseteq B$ elementwise, and also some α in the 16-set $\Omega \setminus B$. This contradicts 5.3, applied to $\mathcal{B}((B \setminus X))$.

7.2. **Theorem.** *All Steiner systems of type $(4, 7, 23)$ are isomorphic and their automorphism group has order $23 \cdot 22 \cdot 21 \cdot 20 \cdot 16 \cdot 3$.*

Proof. We have $\ell(4,7,23) \leq 3$ by 6.10 and 1.12(e). This together with 7.1 allows to apply 1.6 with $n = 2$. Q.E.D.

7.3. **Corollary** (by 6.13). (a) *G is 4-transitive on Ω, and the stabilizer of four points has order $16 \cdot 3$.*

(b) *G is block-transitive, and the stabilizer $H = G_B$ of a block B is 4-transitive (actually 5-transitive by (c)) on B of order $7 \cdot 6 \cdot 5 \cdot 4 \cdot 16 \cdot 3 = 16 \cdot 7!/2$.*

(c) *The pointwise stabilizer W of B is sharply transitive on $\Omega \setminus B$, and H/W is isomorphic to A_7.*

(d) *W equals $C_G(W)$ and is elementary abelian of order 16.*

§8. The Isomorphism Theorem for $S(5,8,24)$

8.1. **Lemma.** *We have $\ell(5,8,24) \leq 1$.*

Proof. Let Ω be a 24-set, $\alpha \in \Omega$, $\mathcal{B}' \in S(4,7,\Omega \setminus \{\alpha\})$, and

$$\{\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_m\} = \{\mathcal{B} \in S(5,8,\Omega) \mid \mathcal{B}((\alpha)) = \mathcal{B}'\}.$$

The claim is $m \leq 1$. By 6.10 and 1.12(e) we have $\ell(5,8,24) \leq 3$, that is $m \leq 3$. Thus each $\mathcal{B}_i$ is fixed by any subgroup $D \subseteq Sym(\Omega)$ of order 5 which fixes α and $\mathcal{B}'$. Such a D exists because $|Aut(\mathcal{B}')|$ is divisible by 5 (Theorem 7.2).

Since $|\mathcal{B}'| = b(4,7,23) = 23 \cdot 11 \equiv 3(5)$ and $|\Omega_D| = 4$, some D-orbit $X \subseteq \Omega$ of length 5 is not contained in a block of $\mathcal{B}'$. The block $B_i \in \mathcal{B}_i$ which contains X is D-invariant, and hence contains 3 fixed points of D. This implies $|B_i \cap B_j| > 5$ for all i, j, hence $\mathcal{B}_i = \mathcal{B}_j$ because $(t,k,v) = (5,8,24)$ satisfies 1.12(*), again by 6.10 and 1.12(e). Q.E.D.

8.2. **Theorem.** *All Steiner systems of type $(5,8,24)$ are isomorphic and their automorphism group has order $24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 16 \cdot 3$.*

Proof. By 8.1 and 7.2, 1.6 applies with $n = 1$. Q.E.D.

Remark. $S(5,8,24)$ is not empty by 4.11. From 8.2 and 7.3 the corollary analogous to 7.3, with $A_8 \simeq H/W$ in place of A_7, follows immediately. Faithful action on W shows that A_8 is isomorphic to $L_4(2)$.

Math. Seminar
Universität Kiel
24098 Kiel
Germany