give automorphisms of $\mathcal{F}$, but we shall see that $\mathcal{F}$ has many more automorphisms than these.

Each $g \in G$ acts by conjugation on the set of points and lines, and this action preserves the incidence relation. Only the identity element in G fixes all points and so via this action the group G would be isomorphic to a subgroup of the group of $\mathrm{Aut}(\mathcal{F})$, the group of all automorphisms of $\mathcal{F}$.

Any automorphism of $\mathcal{F}$ that fixes two points on a line as well as a third point not on that line is easily seen to fix all points. Thus any automorphism of $\mathcal{F}$ is uniquely determined by its action on any three noncollinear points. Since one easily computes that there are 168 such triples, $\mathcal{F}$ has at most 168 automorphisms. This proves

if the simple group G exists it is unique and $G \cong \mathrm{Aut}(\mathcal{F})$.

Two steps in the classification process yet remain: to prove that $\mathcal{F}$ does have 168 automorphisms and to prove $\mathrm{Aut}(\mathcal{F})$ is indeed a simple group. Although one can do these graph-theoretically, we adopt an approach following ideas from the theory of "algebraic groups." Let V be a 3-dimensional vector space over the field of 2 elements, $\mathbb{F}_2$, so V is the elementary abelian 2-group $Z_2 \times Z_2 \times Z_2$ of order 8. By Proposition 17 in Section 4.4, $\mathrm{Aut}(V) = GL(V) \cong GL_3(\mathbb{F}_2)$ has order 168. Call the seven 1-dimensional subspaces (i.e., the nontrivial cyclic subgroups) of V *points*, call the seven 2-dimensional subspaces (i.e., the subgroups of order 4) *lines*, and say the point p is *incident to* the line L if $p \subset L$. Then the points and lines are easily seen to satisfy the same axioms (11) to (13) above, hence to represent the Fano Plane. Since $GL(V)$ acts faithfully on these points and lines preserving incidence, $\mathrm{Aut}(\mathcal{F})$ has order at least 168. In light of the established upper bound for $|\mathrm{Aut}(\mathcal{F})|$ this proves

$\mathrm{Aut}(\mathcal{F}) \cong GL(V) \cong GL_3(\mathbb{F}_2)$ *and* $\mathrm{Aut}(\mathcal{F})$ *has order 168.*

Finally we prove that $GL(V)$ is a simple group. By way of contradiction assume H is a proper nontrivial normal subgroup of $GL(V)$. Let Ω be the 7 points and let N be the stabilizer in $GL(V)$ of some point in Ω. Since $GL(V)$ acts transitively on Ω, N has index 7. Since the intersection of all conjugates of N fixes all points, this intersection is the identity. Thus $H \not\leq N$, and so $GL(V) = HN$. Since $|H : H \cap N| = |HN : N|$ we have $7 \mid |H|$. Since $GL(V)$ is isomorphic to a subgroup of S_7 and since Sylow 7-subgroups of S_7 have normalizers of order 42, $GL(V)$ does not have a normal Sylow 7-subgroup, so by Sylow's Theorem $n_7(GL(V)) = 8$. A normal Sylow 7-subgroup of H would be characteristic in H, hence normal in $GL(V)$, so also H does not have a unique Sylow 7-subgroup. Since $n_7(H) \equiv 1 \bmod 7$ and $n_7(H) \leq n_7(GL(V)) = 8$ we must have $n_7(H) = 8$. This implies $|H|$ is divisible by 8, so $56 \mid |H|$, and since H is proper we must have $|H| = 56$. By usual counting arguments (cf. Exercise 7(b) of Section 5.5) H has a normal, hence characteristic, Sylow 2-subgroup, which is therefore normal in $GL(V)$. But then $GL(V)$ would have a unique Sylow 2-subgroup. Since the set of upper triangular matrices and the set of lower triangular matrices are two subgroups of $GL_3(\mathbb{F}_2)$ each of order 8, we have a contradiction. In summary we have now proven the following theorem.

Theorem 15. Up to isomorphism there is a unique simple group of order 168, $GL_3(\mathbb{F}_2)$, which is also the automorphism group of the projective plane $\mathcal{F}$.

Note that we might just as well have called the W_j points and the U_i lines. This "duality" between points and lines together with the uniqueness of a simple group of order 168 may be used to prove the existence of an outer automorphism of G that interchanges points and lines i.e., conjugates U to W.

Many families of finite simple groups can be classified by analogous methods. In more general settings geometric structures known as *buildings* play the role of the projective plane (which is a special case of a building of type $\mathcal{A}_2$). In this context the subgroups $N_G(U)$ and $N_G(W)$ are *parabolic subgroups* of G, and U, W are their *unipotent radicals* respectively. In particular, all the simple linear groups (cf. Section 3.4) are characterized by the structure and intersections of their parabolic subgroups, or equivalently, by their action on an associated building.

Remarks on the Existence Problem for Groups

As in other areas of mathematics (such as the theory of differential equations) one may hypothesize the existence of a mathematical system (e.g., solution to an equation) and derive a great deal of information about this proposed system. In general, if after considerable effort no contradiction is reached based on the initial hypothesis one begins to suspect that there actually is a system which does satisfy the conditions hypothesized. However, no amount of consistent data will *prove* existence. Suppose we carried out an analysis of a hypothetical simple group G of order $3^3 \cdot 7 \cdot 13 \cdot 409$ analogous to our analysis of a simple group of order 168 (which we showed to exist). After a certain amount of effort we could show that there are unique possible Sylow numbers:

$$n_3 = 7 \cdot 409 \qquad n_7 = 3^2 \cdot 13 \cdot 409 \qquad n_{13} = 3^2 \cdot 7 \cdot 409 \qquad n_{409} = 3^2 \cdot 7 \cdot 13.$$

We could further show that such a G would have no elements of order pq, p and q distinct primes, no elements of order 9, and that distinct Sylow subgroups would intersect in the identity. We could then count the elements in Sylow p-subgroups for all primes p and we would find that these would total to exactly $|G|$. At this point we would have the complete subgroup structure and class equation for G. We might then guess that there *is* a simple group of this order, but the Feit–Thompson Theorem asserts that there are *no* simple groups of odd composite order. (Note, however, that the configuration for a possible simple group of order $3^3 \cdot 7 \cdot 13 \cdot 409$ is among the cases that must be dealt with in the *proof* of the Feit-Thompson Theorem, so quoting this result in this instance is actually circular. We prove no simple group of this order exists in Section 19.3; see also Exercise 29.) The point is that even though we have as much data in this case as we had in the order 168 situation (i.e., Proposition 14), we cannot prove existence without some new techniques.

When we are dealing with nonsimple groups we have at least one method of building larger groups from smaller ones: semidirect products. Even though this method is fairly restrictive it conveys the notion that nonsimple groups may be built up from smaller groups in some constructive fashion. This process breaks down completely for simple groups; and so this demarcation of techniques reinforces our appreciation for the Hölder

Program: determining the simple groups, and finding how these groups are put together to form larger groups.

The study of simple groups, as illustrated in the preceding discussion of groups of order 168, uses many of the same tools as the study of nonsimple groups (to unravel their subgroup structures, etc.) but also requires other techniques for their construction. As we mentioned at the end of that discussion, these often involve algebraic or geometric methods which construct simple groups as automorphisms of mathematical structures that have intrinsic interest, and thereby link group theory to other areas of mathematics and science in fascinating ways. Thus while we have come a long way in the analysis of finite groups, there are a number of different areas in this branch of mathematics on which we have just touched.

The analysis of infinite groups generally involves quite different methods, and in the next section we introduce some of these.

EXERCISES

Counting elements:

1. Prove that for fixed $P \in Syl_p(G)$ if $P \cap R = 1$ for all $R \in Syl_p(G) - \{P\}$, then $P_1 \cap P_2 = 1$ whenever P_1 and P_2 are distinct Sylow p-subgroups of G. Deduce in this case that the number of nonidentity elements of p-power order in G is $(|P| - 1)|G : N_G(P)|$.
2. In the group $S_3 \times S_3$ exhibit a pair of Sylow 2-subgroups that intersect in the identity and exhibit another pair that intersect in a group of order 2.
3. Prove that if $|G| = 380$ then G is not simple. [Just count elements of odd prime order.]
4. Prove that there are no simple groups of order 80, 351, 3875 or 5313.
5. Let G be a solvable group of order pm, where p is a prime not dividing m, and let $P \in Syl_p(G)$. If $N_G(P) = P$, prove that G has a normal subgroup of order m. Where was the solvability of G needed in the proof? (This result is true for nonsolvable groups as well — it is a special case of *Burnside's N/C-Theorem*.)

Exploiting subgroups of small index:

6. Prove that there are no simple groups of order 2205, 4125, 5103, 6545 or 6435.

Permutation representations:

7. Prove that there are no simple groups of order 1755 or 5265. [Use Sylow 3-subgroups to show $G \leq S_{13}$ and look at the normalizer of a Sylow 13-subgroup.]
8. Prove that there are no simple groups of order 792 or 918.
9. Prove that there are no simple groups of order 336.

Playing p-subgroups off against each other:

10. Prove that there are no simple groups of order 4095, 4389, 5313 or 6669.
11. Prove that there are no simple groups of order 4851 or 5145.
12. Prove that there are no simple groups of order 9555. [Let $Q \in Syl_{13}(G)$ and let $P \in Syl_7(N_G(Q))$. Argue that $Q \trianglelefteq N_G(P)$ — why is this a contradiction?]

Normalizers of Sylow intersections:

13. Let G be a group with more than one Sylow p-subgroup. Over all pairs of distinct Sylow p-subgroups let P and Q be chosen so that $|P \cap Q|$ is maximal. Show that $N_G(P \cap Q)$