36. Prove that if $N$ is a normal subgroup of $G$ then $n_p(G/N) \leq n_p(G)$.

37. Let $R$ be a normal $p$-subgroup of $G$ (not necessarily a Sylow subgroup).
   (a) Prove that $R$ is contained in every Sylow $p$-subgroup of $G$.
   (b) If $S$ is another normal $p$-subgroup of $G$, prove that $RS$ is also a normal $p$-subgroup of $G$.
   (c) The subgroup $O_p(G)$ is defined to be the group generated by all normal $p$-subgroups of $G$. Prove that $O_p(G)$ is the unique largest normal $p$-subgroup of $G$ and $O_p(G)$ equals the intersection of all Sylow $p$-subgroups of $G$.
   (d) Let $\overline{G} = G/O_p(G)$. Prove that $O_p(\overline{G}) = \overline{1}$ (i.e., $\overline{G}$ has no nontrivial normal $p$-subgroup).

38. Use the method of proof in Sylow's Theorem to show that if $n_p$ is not congruent to $1 \pmod{p^2}$ then there are distinct Sylow $p$-subgroups $P$ and $Q$ of $G$ such that $|P : P \cap Q| = |Q : P \cap Q| = p$.

39. Show that the subgroup of strictly upper triangular matrices in $GL_n(\mathbb{F}_p)$ (cf. Exercise 17, Section 2.1) is a Sylow $p$-subgroup of this finite group. [Use the order formula in Section 1.4 to find the order of a Sylow $p$-subgroup of $GL_n(\mathbb{F}_p)$.]

40. Prove that the number of Sylow $p$-subgroups of $GL_2(\mathbb{F}_p)$ is $p+1$. [Exhibit two distinct Sylow $p$-subgroups.]

41. Prove that $SL_2(\mathbb{F}_4) \cong A_5$ (cf. Exercise 9, Section 2.1 for the definition of $SL_2(\mathbb{F}_4)$).

42. Prove that the group of rigid motions in $\mathbb{R}^3$ of an icosahedron is isomorphic to $A_5$. [Recall that the order of this group is 60: Exercise 13, Section 1.2.]

43. Prove that the group of rigid motions in $\mathbb{R}^3$ of a dodecahedron is isomorphic to $A_5$. (As with the cube and the tetrahedron, the icosahedron and the dodecahedron are dual solids.) [Recall that the order of this group is 60: Exercise 12, Section 1.2.]

44. Let $p$ be the smallest prime dividing the order of the finite group $G$. If $P \in Syl_p(G)$ and $P$ is cyclic prove that $N_G(P) = C_G(P)$.

45. Find generators for a Sylow $p$-subgroup of $S_{2p}$, where $p$ is an odd prime. Show that this is an abelian group of order $p^2$.

46. Find generators for a Sylow $p$-subgroup of $S_{p^2}$, where $p$ is a prime. Show that this is a non-abelian group of order $p^{p+1}$.

47. Write and execute a computer program which
   (i) gives each odd number $n < 10,000$ that is not a power of a prime and that has some prime divisor $p$ such that $n_p$ is not forced to be 1 for all groups of order $n$ by the congruence condition of Sylow's Theorem, and
   (ii) gives for each $n$ in (i) the factorization of $n$ into prime powers and gives the list of all permissible values of $n_p$ for all primes $p$ dividing $n$ (i.e., those values not ruled out by Part 3 of Sylow's Theorem).

48. Carry out the same process as in the preceding exercise for all even numbers less than 1000. Explain the relative lengths of the lists versus the number of integers tested.

49. Prove that if $|G| = 2^n m$ where $m$ is odd and $G$ has a cyclic Sylow 2-subgroup then $G$ has a normal subgroup of order $m$. [Use induction and Exercises 11 and 12 in Section 2.]

50. Prove that if $U$ and $W$ are normal subsets of a Sylow $p$-subgroup $P$ of $G$ then $U$ is conjugate to $W$ in $G$ if and only if $U$ is conjugate to $W$ in $N_G(P)$. Deduce that two elements in the center of $P$ are conjugate in $G$ if and only if they are conjugate in $N_G(P)$. (A subset $U$ of $P$ is normal in $P$ if $N_P(U) = P$.)

51. Let $P$ be a Sylow $p$-subgroup of $G$ and let $M$ be any subgroup of $G$ which contains $N_G(P)$. Prove that $|G : M| \equiv 1 (\text{mod } p)$.

The following sequence of exercises leads to the classification of all numbers $n$ with the property that every group of order $n$ is cyclic (for example, $n = 15$ is such an integer). These arguments are a vastly simplified prototype for the proof that every group of odd order is solvable in the sense that they use the *structure* (commutativity) of the proper subgroups and their *embedding* in the whole group (we shall see that distinct maximal subgroups intersect in the identity) to obtain a contradiction by counting arguments. In the proof that groups of odd order are solvable one uses induction to reduce to the situation in which a minimal counterexample is a simple group — but here every proper subgroup is solvable (not abelian as in our situation). The analysis of the structure and embedding of the maximal subgroups in this situation is much more complicated and the counting arguments are (roughly speaking) replaced by character theory arguments (as will be discussed in Part VI).

52. Suppose $G$ is a finite simple group in which every proper subgroup is abelian. If $M$ and $N$ are distinct maximal subgroups of $G$ prove $M \cap N = 1$. [See Exercise 23 in Section 3.]
53. Use the preceding exercise to prove that if $G$ is any non-abelian group in which every proper subgroup is abelian then $G$ is not simple. [Let $G$ be a counterexample to this assertion and use Exercise 24 in Section 3 to show that $G$ has more than one conjugacy class of maximal subgroups. Use the method of Exercise 23 in Section 3 to count the elements which lie in all conjugates of $M$ and $N$, where $M$ and $N$ are nonconjugate maximal subgroups of $G$; show that this gives more than $|G|$ elements.]
54. Prove the following classification: if $G$ is a finite group of order $p_1p_2 \dots p_r$ where the $p_i$'s are distinct primes such that $p_i$ does not divide $p_j - 1$ for all $i$ and $j$, then $G$ is cyclic. [By induction, every proper subgroup of $G$ is cyclic, so $G$ is not simple by the preceding exercise. If $N$ is a nontrivial proper normal subgroup, $N$ is cyclic and $G/N$ acts as automorphisms of $N$. Use Proposition 16 to show that $N \leq Z(G)$ and use induction to show $G/Z(G)$ is cyclic, hence $G$ is abelian by Exercise 36 of Section 3.1.]
55. Prove the converse to the preceding exercise: if $n \geq 2$ is an integer such that every group of order $n$ is cyclic, then $n = p_1p_2 \dots p_r$ is a product of distinct primes and $p_i$ does not divide $p_j - 1$ for all $i, j$. [If $n$ is not of this form, construct noncyclic groups of order $n$ using direct products of noncyclic groups of order $p^2$ and $pq$, where $p \mid q - 1$.]
56. If $G$ is a finite group in which every proper subgroup is abelian, show that $G$ is solvable.

## 4.6 THE SIMPLICITY OF $A_n$

There are a number of proofs of the simplicity of $A_n$, $n \geq 5$. The most elementary involves showing $A_n$ is generated by 3-cycles. Then one shows that a normal subgroup must contain one 3-cycle hence must contain all the 3-cycles so cannot be a proper subgroup. We include a less computational approach.

Note that $A_3$ is an abelian simple group and that $A_4$ is not simple ($n_2(A_4) = 1$).

**Theorem 24.** $A_n$ is simple for all $n \geq 5$.

*Proof:* By induction on $n$. The result has already been established for $n = 5$, so assume $n \geq 6$ and let $G = A_n$. Assume there exists $H \trianglelefteq G$ with $H \neq 1$ or $G$.

For each $i \in \{1, 2, \ldots, n\}$ let $G_i$ be the stabilizer of $i$ in the natural action of $G$ on $i \in \{1, 2, \ldots, n\}$. Thus $G_i \leq G$ and $G_i \cong A_{n-1}$. By induction, $G_i$ is simple for $1 \leq i \leq n$.

Suppose first that there is some $\tau \in H$ with $\tau \neq 1$ but $\tau(i) = i$ for some $i \in \{1, 2, \ldots, n\}$. Since $\tau \in H \cap G_i$ and $H \cap G_i \trianglelefteq G_i$, by the simplicity of $G_i$ we must have $H \cap G_i = G_i$, that is

$$G_i \leq H.$$

By Exercise 2 of Section 1, $\sigma G_i \sigma^{-1} = G_{\sigma(i)}$, so for all $i$, $\sigma G_i \sigma^{-1} \leq \sigma H \sigma^{-1} = H$. Thus

$$G_j \leq H, \quad \text{for all } j \in \{1, 2, \ldots, n\}.$$

Any $\lambda \in A_n$ may be written as a product of an even number, $2t$, of transpositions, so

$$\lambda = \lambda_1 \lambda_2 \cdots \lambda_t,$$

where $\lambda_k$ is a product of two transpositions. Since $n > 4$ each $\lambda_k \in G_j$, for some $j$, hence

$$G = \langle G_1, G_2, \ldots, G_n \rangle \leq H,$$

which is a contradiction. Therefore if $\tau \neq 1$ is an element of $H$ then $\tau(i) \neq i$ for all $i \in \{1, 2, \ldots, n\}$, i.e., no nonidentity element of $H$ fixes any element of $\{1, 2, \ldots, n\}$.

It follows that if $\tau_1, \tau_2$ are elements of $H$ with

$$\tau_1(i) = \tau_2(i) \text{ for some } i, \text{ then } \tau_1 = \tau_2 \tag{4.2}$$

since then $\tau_2^{-1}\tau_1(i) = i$.

Suppose there exists a $\tau \in H$ such that the cycle decomposition of $\tau$ contains a cycle of length $\geq 3$, say

$$\tau = (a_1\, a_2\, a_3 \ldots)(b_1\, b_2\, \ldots) \ldots .$$

Let $\sigma \in G$ be an element with $\sigma(a_1) = a_1$, $\sigma(a_2) = a_2$ but $\sigma(a_3) \neq a_3$ (note that such a $\sigma$ exists in $A_n$ since $n \geq 5$). By Proposition 10

$$\tau_1 = \sigma\tau\sigma^{-1} = (a_1\, a_2\, \sigma(a_3)\, \ldots)(\sigma(b_1)\, \sigma(b_2)\, \ldots) \ldots$$

so $\tau$ and $\tau_1$ are distinct elements of $H$ with $\tau(a_1) = \tau_1(a_1) = a_2$, contrary to (2). This proves that only 2-cycles can appear in the cycle decomposition of nonidentity elements of $H$.

Let $\tau \in H$ with $\tau \neq 1$, so that

$$\tau = (a_1\, a_2)(a_3\, a_4)(a_5\, a_6) \ldots$$

(note that $n \geq 6$ is used here). Let $\sigma = (a_1\, a_2)(a_3\, a_5) \in G$. Then

$$\tau_1 = \sigma\tau\sigma^{-1} = (a_1\, a_2)(a_5\, a_4)(a_3\, a_6) \ldots,$$

hence $\tau$ and $\tau_1$ are distinct elements of $H$ with $\tau(a_1) = \tau_1(a_1) = a_2$, again contrary to (2). This completes the proof of the simplicity of $A_n$.

## EXERCISES

Let $G$ be a group and let $\Omega$ be an infinite set.

1. Prove that $A_n$ does not have a proper subgroup of index $< n$ for all $n \geq 5$.
2. Find all normal subgroups of $S_n$ for all $n \geq 5$.
3. Prove that $A_n$ is the only proper subgroup of index $< n$ in $S_n$ for all $n \geq 5$.
4. Prove that $A_n$ is generated by the set of all 3-cycles for each $n \geq 3$.
5. Prove that if there exists a chain of subgroups $G_1 \leq G_2 \leq \ldots \leq G$ such that $G = \cup_{i=1}^{\infty} G_i$ and each $G_i$ is simple then $G$ is simple.
6. Let $D$ be the subgroup of $S_\Omega$ consisting of permutations which move only a finite number of elements of $\Omega$ (described in Exercise 17 in Section 3) and let $A$ be the set of all elements $\sigma \in D$ such that $\sigma$ acts as an even permutation on the (finite) set of points it moves. Prove that $A$ is an infinite simple group. [Show that every pair of elements of $D$ lie in a finite simple subgroup of $D$.]
7. Under the notation of the preceding, exercise prove that if $H \trianglelefteq S_\Omega$ and $H \neq 1$ then $A \leq H$, i.e., $A$ is the unique (nontrivial) minimal normal subgroup of $S_\Omega$.
8. Under the notation of the preceding two exercises prove that $|D| = |A| = |\Omega|$. Deduce that

$$\text{if } S_\Omega \cong S_\Delta \text{ then } |\Omega| = |\Delta|.$$

[Use the fact that $D$ is generated by transpositions. You may assume that countable unions and finite direct products of sets of cardinality $|\Omega|$ also have cardinality $|\Omega|$.]