By the exercises in Section 1.4, the latter group has order 6. But $\mathrm{Aut}(V_4)$ permutes the 3 nonidentity elements of V_4, and this action of $\mathrm{Aut}(V_4)$ on $V_4 - \{1\}$ gives an injective permutation representation of $\mathrm{Aut}(V_4)$ into S_3. By order considerations, the homomorphism is onto, so

$$\mathrm{Aut}(V_4) \cong GL_2(\mathbb{F}_2) \cong S_3.$$

Note that V_4 is abelian, so $\mathrm{Inn}(V_4) = 1$.

For any prime p, the elementary abelian group of order p^2 is $Z_p \times Z_p$. Its automorphism group, $GL_2(\mathbb{F}_p)$, has order $p(p-1)^2(p+1)$. Thus Corollary 9 implies that for p a prime

$$\text{if } |P| = p^2, \quad |\mathrm{Aut}(P)| = p(p-1) \text{ or } p(p-1)^2(p+1)$$

according to whether P is cyclic or elementary abelian, respectively.

Example

Suppose G is a group of order $45 = 3^2 5$ with a normal subgroup P of order 3^2. We show that G is necessarily abelian.

The quotient $G/C_G(P)$ is isomorphic to a subgroup of $\mathrm{Aut}(P)$ by Corollary 15, and $\mathrm{Aut}(P)$ has order 6 or 48 (according to whether P is cyclic or elementary abelian, respectively) by the preceding paragraph. On the other hand, since the order of P is the square of a prime, P is an abelian group, hence $P \leq C_G(P)$. It follows that $|C_G(P)|$ is divisible by 9, which implies $|G/C_G(P)|$ is 1 or 5. Together these imply $|G/C_G(P)| = 1$, i.e., $C_G(P) = G$ and $P \leq Z(G)$. Since then $G/Z(G)$ is cyclic, G must be an abelian group.

EXERCISES

Let G be a group.

1. If $\sigma \in \mathrm{Aut}(G)$ and φ_g is conjugation by g prove $\sigma\varphi_g\sigma^{-1} = \varphi_{\sigma(g)}$. Deduce that $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. (The group $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ is called the *outer automorphism group* of G.)
2. Prove that if G is an abelian group of order pq, where p and q are distinct primes, then G is cyclic. [Use Cauchy's Theorem to produce elements of order p and q and consider the order of their product.]
3. Prove that under any automorphism of D_8, r has at most 2 possible images and s has at most 4 possible images (r and s are the usual generators — cf. Section 1.2). Deduce that $|\mathrm{Aut}(D_8)| \leq 8$.
4. Use arguments similar to those in the preceding exercise to show $|\mathrm{Aut}(Q_8)| \leq 24$.
5. Use the fact that $D_8 \trianglelefteq D_{16}$ to prove that $\mathrm{Aut}(D_8) \cong D_8$.
6. Prove that characteristic subgroups are normal. Give an example of a normal subgroup that is not characteristic.
7. If H is the unique subgroup of a given order in a group G prove H is characteristic in G.
8. Let G be a group with subgroups H and K with $H \leq K$.
   (a) Prove that if H is characteristic in K and K is normal in G then H is normal in G.
   (b) Prove that if H is characteristic in K and K is characteristic in G then H is characteristic in G. Use this to prove that the Klein 4-group V_4 is characteristic in S_4.
   (c) Give an example to show that if H is normal in K and K is characteristic in G then H need not be normal in G.

9. If r, s are the usual generators for the dihedral group D_{2n}, use the preceding two exercises to deduce that every subgroup of $\langle r \rangle$ is normal in D_{2n}.

10. Let G be a group, let A be an abelian normal subgroup of G, and write $\overline{G} = G/A$. Show that $\overline{G}$ acts (on the left) by conjugation on A by $\overline{g} \cdot a = gag^{-1}$, where g is *any* representative of the coset $\overline{g}$ (in particular, show that this action is well defined). Give an explicit example to show that this action is not well defined if A is non-abelian.

11. If p is a prime and P is a subgroup of S_p of order p, prove $N_{S_p}(P)/C_{S_p}(P) \cong \text{Aut}(P)$. [Use Exercise 34, Section 3.]

12. Let G be a group of order 3825. Prove that if H is a normal subgroup of order 17 in G then $H \leq Z(G)$.

13. Let G be a group of order 203. Prove that if H is a normal subgroup of order 7 in G then $H \leq Z(G)$. Deduce that G is abelian in this case.

14. Let G be a group of order 1575. Prove that if H is a normal subgroup of order 9 in G then $H \leq Z(G)$.

15. Prove that each of the following (multiplicative) groups is cyclic: $(\mathbb{Z}/5\mathbb{Z})^\times$, $(\mathbb{Z}/9\mathbb{Z})^\times$ and $(\mathbb{Z}/18\mathbb{Z})^\times$.

16. Prove that $(\mathbb{Z}/24\mathbb{Z})^\times$ is an elementary abelian group of order 8. (We shall see later that $(\mathbb{Z}/n\mathbb{Z})^\times$ is an elementary abelian group if and only if $n \mid 24$.)

17. Let $G = \langle x \rangle$ be a cyclic group of order n. For $n = 2, 3, 4, 5, 6$ write out the elements of $\text{Aut}(G)$ explicitly (by Proposition 16 above we know $\text{Aut}(G) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, so for each element $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, write out explicitly what the automorphism ψ_a does to the elements $\{1, x, x^2, \ldots, x^{n-1}\}$ of G).

18. This exercise shows that for $n \neq 6$ every automorphism of S_n is inner. Fix an integer $n \geq 2$ with $n \neq 6$.
    (a) Prove that the automorphism group of a group G permutes the conjugacy classes of G, i.e., for each $\sigma \in \text{Aut}(G)$ and each conjugacy class $\mathcal{K}$ of G the set $\sigma(\mathcal{K})$ is also a conjugacy class of G.
    (b) Let $\mathcal{K}$ be the conjugacy class of transpositions in S_n and let $\mathcal{K}'$ be the conjugacy class of any element of order 2 in S_n that is not a transposition. Prove that $|\mathcal{K}| \neq |\mathcal{K}'|$. Deduce that any automorphism of S_n sends transpositions to transpositions. [See Exercise 33 in Section 3.]
    (c) Prove that for each $\sigma \in \text{Aut}(S_n)$

$$\sigma : (1\ 2) \mapsto (a\ b_2), \qquad \sigma : (1\ 3) \mapsto (a\ b_3), \quad \ldots, \quad \sigma : (1\ n) \mapsto (a\ b_n)$$

    for some distinct integers $a, b_2, b_3, \ldots, b_n \in \{1, 2, \ldots, n\}$.
    (d) Show that $(1\ 2)$, $(1\ 3)$, $\ldots$, $(1\ n)$ generate S_n and deduce that any automorphism of S_n is uniquely determined by its action on these elements. Use (c) to show that S_n has at most $n!$ automorphisms and conclude that $\text{Aut}(S_n) = \text{Inn}(S_n)$ for $n \neq 6$.

19. This exercise shows that $|\text{Aut}(S_6) : \text{Inn}(S_6)| \leq 2$ (Exercise 10 in Section 6.3 shows that equality holds by exhibiting an automorphism of S_6 that is not inner).
    (a) Let $\mathcal{K}$ be the conjugacy class of transpositions in S_6 and let $\mathcal{K}'$ be the conjugacy class of any element of order 2 in S_6 that is not a transposition. Prove that $|\mathcal{K}| \neq |\mathcal{K}'|$ unless $\mathcal{K}'$ is the conjugacy class of products of three disjoint transpositions. Deduce that $\text{Aut}(S_6)$ has a subgroup of index at most 2 which sends transpositions to transpositions.
    (b) Prove that $|\text{Aut}(S_6) : \text{Inn}(S_6)| \leq 2$. [Follow the same steps as in (c) and (d) of the preceding exercise to show that any automorphism that sends transpositions to transpositions is inner.]

The next exercise introduces a subgroup, $J(P)$, which (like the center of P) is defined for an arbitrary finite group P (although in most applications P is a group whose order is a power of a prime). This subgroup was defined by J. Thompson in 1964 and it now plays a pivotal role in the study of finite groups, in particular, in the classification of finite simple groups.

20. For any finite group P let $d(P)$ be the minimum number of generators of P (so, for example, $d(P) = 1$ if and only if P is a nontrivial cyclic group and $d(Q_8) = 2$). Let $m(P)$ be the maximum of the integers $d(A)$ as A runs over all *abelian* subgroups of P (so, for example, $m(Q_8) = 1$ and $m(D_8) = 2$). Define

$$J(P) = \langle A \mid A \text{ is an abelian subgroup of } P \text{ with } d(A) = m(P) \rangle.$$

($J(P)$ is called the *Thompson subgroup* of P.)

(a) Prove that $J(P)$ is a characteristic subgroup of P.

(b) For each of the following groups P list all abelian subgroups A of P that satisfy $d(A) = m(P)$: Q_8, D_8, D_{16} and QD_{16} (where QD_{16} is the quasidihedral group of order 16 defined in Exercise 11 of Section 2.5). [Use the lattices of subgroups for these groups in Section 2.5.]

(c) Show that $J(Q_8) = Q_8$, $J(D_8) = D_8$, $J(D_{16}) = D_{16}$ and $J(QD_{16})$ is a dihedral subgroup of order 8 in QD_{16}.

(d) Prove that if $Q \leq P$ and $J(P)$ is a subgroup of Q, then $J(P) = J(Q)$. Deduce that if P is a subgroup (not necessarily normal) of the finite group G and $J(P)$ is contained in some subgroup Q of P such that $Q \trianglelefteq G$, then $J(P) \trianglelefteq G$.

4.5 SYLOW'S THEOREM

In this section we prove a partial converse to Lagrange's Theorem and derive numerous consequences, some of which will lead to classification theorems in the next chapter.

Definition. Let G be a group and let p be a prime.

(1) A group of order p^α for some $\alpha \geq 1$ is called a *p-group*. Subgroups of G which are p-groups are called *p-subgroups*.

(2) If G is a group of order $p^\alpha m$, where $p \nmid m$, then a subgroup of order p^α is called a *Sylow p-subgroup* of G.

(3) The set of Sylow p-subgroups of G will be denoted by $Syl_p(G)$ and the number of Sylow p-subgroups of G will be denoted by $n_p(G)$ (or just n_p when G is clear from the context).

Theorem 18. *(Sylow's Theorem)* Let G be a group of order $p^\alpha m$, where p is a prime not dividing m.

(1) Sylow p-subgroups of G exist, i.e., $Syl_p(G) \neq \emptyset$.

(2) If P is a Sylow p-subgroup of G and Q is any p-subgroup of G, then there exists $g \in G$ such that $Q \leq gPg^{-1}$, i.e., Q is contained in some conjugate of P. In particular, any two Sylow p-subgroups of G are conjugate in G.

(3) The number of Sylow p-subgroups of G is of the form $1 + kp$, i.e.,

$$n_p \equiv 1 (\text{mod } p).$$

Further, n_p is the index in G of the normalizer $N_G(P)$ for any Sylow p-subgroup P, hence n_p divides m.