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 $N_{S_p}(P)/C_{S_p}(P) \cong \operatorname{Aut}(P)$. [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 $\operatorname{Aut}(G)$ explicitly (by Proposition 16 above we know $\operatorname{Aut}(G) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, so for each element $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, write out explicitly what the automorphism ψ_a does to the elements $\{1, x, x^2, \dots, x^{n-1}\}$ 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 $\sigma \in \operatorname{Aut}(G)$ 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 $\sigma \in \operatorname{Aut}(S_n)$

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

for some distinct integers $a, b_2, b_3, \dots, b_n \in \{1, 2, \dots, n\}$.

(d) Show that $(1\ 2),\ (1\ 3),\ \dots,\ (1\ n)$ 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 $\operatorname{Aut}(S_n) = \operatorname{Inn}(S_n)$ for $n \neq 6$.

19. This exercise shows that $|\operatorname{Aut}(S_6) : \operatorname{Inn}(S_6)| \leq 2$ (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 $\operatorname{Aut}(S_6)$ has a subgroup of index at most 2 which sends transpositions to transpositions.

(b) Prove that $|\operatorname{Aut}(S_6) : \operatorname{Inn}(S_6)| \leq 2$. [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 $Q \le P$ 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 $\alpha \ge 1$ 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 $Q \le gPg^{-1}$, 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.,

$$n_p \equiv 1 \pmod{p}.$$

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.

We first prove the following lemma:

Lemma 19. Let $P \in Syl_p(G)$. If Q is any p-subgroup of G, then $Q \cap N_G(P) = Q \cap P$.

Proof: Let $H = N_G(P) \cap Q$. Since $P \leq N_G(P)$ it is clear that $P \cap Q \leq H$, so we must prove the reverse inclusion. Since by definition $H \leq Q$, this is equivalent to showing $H \leq P$. We do this by demonstrating that PH is a p-subgroup of G containing both P and H; but P is a p-subgroup of G of largest possible order, so we must have $PH = P$, i.e., $H \leq P$.

Since $H \leq N_G(P)$, by Corollary 15 in Section 3.2, PH is a subgroup. By Proposition 13 in the same section

$$|PH| = \frac{|P||H|}{|P \cap H|}.$$

All the numbers in the above quotient are powers of p, so PH is a p-group. Moreover, P is a subgroup of PH so the order of PH is divisible by p^α, the largest power of p which divides $|G|$. These two facts force $|PH| = p^\alpha = |P|$. This in turn implies $P = PH$ and $H \leq P$. This establishes the lemma.

Proof of Sylow's Theorem (1) Proceed by induction on $|G|$. If $|G| = 1$, there is nothing to prove. Assume inductively the existence of Sylow p-subgroups for all groups of order less than $|G|$.

If p divides $|Z(G)|$, then by Cauchy's Theorem for abelian groups (Proposition 21, Section 3.4) $Z(G)$ has a subgroup, N, of order p. Let $\overline{G} = G/N$, so that $|\overline{G}| = p^{\alpha-1}m$. By induction, $\overline{G}$ has a subgroup $\overline{P}$ of order $p^{\alpha-1}$. If we let P be the subgroup of G containing N such that $P/N = \overline{P}$ then $|P| = |P/N| \cdot |N| = p^\alpha$ and P is a Sylow p-subgroup of G. We are reduced to the case when p does not divide $|Z(G)|$.

Let $g_1, g_2, \ldots, g_r$ be representatives of the distinct non-central conjugacy classes of G. The class equation for G is

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|.$$

If $p \mid |G : C_G(g_i)|$ for all i, then since $p \mid |G|$, we would also have $p \mid |Z(G)|$, a contradiction. Thus for some i, p does not divide $|G : C_G(g_i)|$. For this i let $H = C_G(g_i)$ so that

$$|H| = p^\alpha k, \quad \text{where } p \nmid k.$$

Since $g_i \notin Z(G)$, $|H| < |G|$. By induction, H has a Sylow p-subgroup, P, which of course is also a subgroup of G. Since $|P| = p^\alpha$, P is a Sylow p-subgroup of G. This completes the induction and establishes (1).

Before proving (2) and (3) we make some calculations. By (1) there exists a Sylow p-subgroup, P, of G. Let

$$\{P_1, P_2, \ldots, P_r\} = \mathcal{S}$$

be the set of all conjugates of P (i.e., $\mathcal{S} = \{gPg^{-1} \mid g \in G\}$) and let Q be *any* p-subgroup of G. By definition of $\mathcal{S}$, G, hence also Q, acts by conjugation on $\mathcal{S}$. Write $\mathcal{S}$ as a disjoint union of orbits under this action by Q:

$$\mathcal{S} = \mathcal{O}_1 \cup \mathcal{O}_2 \cup \cdots \cup \mathcal{O}_s$$

where $r = |\mathcal{O}_1| + \cdots + |\mathcal{O}_s|$. Keep in mind that r does not depend on Q but the number of Q-orbits s does (note that by definition, G has only one orbit on $\mathcal{S}$ but a subgroup Q of G may have more than one orbit). Renumber the elements of $\mathcal{S}$ if necessary so that the first s elements of $\mathcal{S}$ are representatives of the Q-orbits: $P_i \in \mathcal{O}_i$, $1 \le i \le s$. It follows from Proposition 2 that $|\mathcal{O}_i| = |Q : N_Q(P_i)|$. By definition, $N_Q(P_i) = N_G(P_i) \cap Q$ and by Lemma 19, $N_G(P_i) \cap Q = P_i \cap Q$. Combining these two facts gives

$$|\mathcal{O}_i| = |Q : P_i \cap Q|, \qquad 1 \le i \le s. \tag{4.1}$$

We are now in a position to prove that $r \equiv 1 \pmod p$. Since Q was arbitrary we may take $Q = P_1$ above, so that (1) gives

$$|\mathcal{O}_1| = 1.$$

Now, for all $i > 1$, $P_1 \neq P_i$, so $P_1 \cap P_i < P_1$. By (1)

$$|\mathcal{O}_i| = |P_1 : P_1 \cap P_i| > 1, \qquad 2 \le i \le s.$$

Since P_1 is a p-group, $|P_1 : P_1 \cap P_i|$ must be a power of p, so that

$$p \bigm| |\mathcal{O}_i|, \qquad 2 \le i \le s.$$

Thus

$$r = |\mathcal{O}_1| + (|\mathcal{O}_2| + \ldots + |\mathcal{O}_s|) \equiv 1 \pmod p.$$

We now prove parts (2) and (3). Let Q be any p-subgroup of G. Suppose Q is not contained in P_i for any $i \in \{1, 2, \ldots, r\}$ (i.e., $Q \not\le gPg^{-1}$ for any $g \in G$). In this situation, $Q \cap P_i < Q$ for all i, so by (1) ?

$$|\mathcal{O}_i| = |Q : Q \cap P_i| > 1, \qquad 1 \le i \le s.$$

Thus $p \bigm| |\mathcal{O}_i|$ for all i, so p divides $|\mathcal{O}_1| + \ldots + |\mathcal{O}_s| = r$. This contradicts the fact that $r \equiv 1 \pmod p$ (remember, r does not depend on the choice of Q). This contradiction proves $Q \le gPg^{-1}$ for some $g \in G$.

To see that all Sylow p-subgroups of G are conjugate, let Q be any Sylow p-subgroup of G. By the preceding argument, $Q \le gPg^{-1}$ for some $g \in G$. Since $|gPg^{-1}| = |Q| = p^\alpha$, we must have $gPg^{-1} = Q$. This establishes part (2) of the theorem. In particular, $\mathcal{S} = Syl_p(G)$ since *every* Sylow p-subgroup of G is conjugate to P, and so $n_p = r \equiv 1 \pmod p$, which is the first part of (3).

Finally, since all Sylow p-subgroups are conjugate, Proposition 6 shows that

$$n_p = |G : N_G(P)| \quad \text{for any } P \in Syl_p(G),$$

completing the proof of Sylow's Theorem.

Note that the conjugacy part of Sylow's Theorem together with Corollary 14 shows that *any two Sylow p-subgroups of a group (for the same prime p) are isomorphic.*