Topic: Sylow's Theorems and Their Applications

Study Material

Paper No. - MTM-203

Unit-I

Paper Name- Abstract Algebra

M. Sc. 2nd Semester

Material No. - 1

By

Dr. Ganesh Ghorai
Assistant Professor
Department of Applied Mathematics with
Oceanology and Computer Programming
Vidyasagar University

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.,

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

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: $P_i \in \mathcal{O}_i$, $1 \leq i \leq s$. 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

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

We are now in a position to prove that $r \equiv 1 (\text{mod } p)$. 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)

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

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

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

Thus

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

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., $Q \not\leq gPg^{-1}$ for any $g \in G$). In this situation, $Q \cap P_i < Q$ for all i, so by (1)

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

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 $r \equiv 1 (\text{mod } p)$ (remember, r does not depend on the choice of Q). This contradiction proves $Q \leq gPg^{-1}$ 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, $Q \leq gPg^{-1}$ 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 $n_p = r \equiv 1 (\text{mod } p)$, 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.*

Corollary 20. Let P be a Sylow p-subgroup of G. Then the following are equivalent:

(1) P is the unique Sylow p-subgroup of G, i.e., $n_p = 1$

(2) P is normal in G

(3) P is characteristic in G

(4) All subgroups generated by elements of p-power order are p-groups, i.e., if X is any subset of G such that $|x|$ is a power of p for all $x \in X$, then $\langle X \rangle$ is a p-group.

Proof: If (1) holds, then $gPg^{-1} = P$ for all $g \in G$ since $gPg^{-1} \in Syl_p(G)$, i.e., P is normal in G. Hence (1) implies (2). Conversely, if $P \trianglelefteq G$ and $Q \in Syl_p(G)$, then by Sylow's Theorem there exists $g \in G$ such that $Q = gPg^{-1} = P$. Thus $Syl_p(G) = \{P\}$ and (2) implies (1).

Since characteristic subgroups are normal, (3) implies (2). Conversely, if $P \trianglelefteq G$, we just proved P is the unique subgroup of G of order p^α, hence P char G. Thus (2) and (3) are equivalent.

Finally, assume (1) holds and suppose X is a subset of G such that $|x|$ is a power of p for all $x \in X$. By the conjugacy part of Sylow's Theorem, for each $x \in X$ there is some $g \in G$ such that $x \in gPg^{-1} = P$. Thus $X \subseteq P$, and so $\langle X \rangle \leq P$, and $\langle X \rangle$ is a p-group. Conversely, if (4) holds, let X be the union of all Sylow p-subgroups of G. If P is any Sylow p-subgroup, P is a subgroup of the p-group $\langle X \rangle$. Since P is a p-subgroup of G of maximal order, we must have $P = \langle X \rangle$, so (1) holds.

Examples

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

(1) If p does not divide the order of G, the Sylow p-subgroup of G is the trivial group (and all parts of Sylow's Theorem hold trivially). If $|G| = p^\alpha$, G is the unique Sylow p-subgroup of G.

(2) A finite abelian group has a unique Sylow p-subgroup for each prime p. This subgroup consists of all elements x whose order is a power of p. This is sometimes called the *p-primary component* of the abelian group.

(3) S_3 has three Sylow 2-subgroups: $\langle (1\,2) \rangle$, $\langle (2\,3) \rangle$ and $\langle (1\,3) \rangle$. It has a unique (hence normal) Sylow 3-subgroup: $\langle (1\,2\,3) \rangle = A_3$. Note that $3 \equiv 1 \pmod 2$.

(4) A_4 has a unique Sylow 2-subgroup: $\langle (1\,2)(3\,4), (1\,3)(2\,4) \rangle \cong V_4$. It has four Sylow 3-subgroups: $\langle (1\,2\,3) \rangle$, $\langle (1\,2\,4) \rangle$, $\langle (1\,3\,4) \rangle$ and $\langle (2\,3\,4) \rangle$. Note that $4 \equiv 1 \pmod 3$.

(5) S_4 has $n_2 = 3$ and $n_3 = 4$. Since S_4 contains a subgroup isomorphic to D_8, every Sylow 2-subgroup of S_4 is isomorphic to D_8.

Applications of Sylow's Theorem

We now give some applications of Sylow's Theorem. Most of the examples use Sylow's Theorem to prove that a group of a particular order is not simple. After discussing methods of constructing larger groups from smaller ones (for example, the formation of semidirect products) we shall be able to use these results to classify groups of some specific orders n (as we already did for $n = 15$).

Since Sylow's Theorem ensures the existence of p-subgroups of a finite group, it is worthwhile to study groups of prime power order more closely. This will be done in Chapter 6 and many more applications of Sylow's Theorem will be discussed there.

For groups of small order, the congruence condition of Sylow's Theorem alone is often sufficient to force the existence of a *normal* subgroup. The first step in any numerical application of Sylow's Theorem is to factor the group order into prime powers. The largest prime divisors of the group order tend to give the fewest possible values for n_p (for example, the congruence condition on n_2 gives no restriction whatsoever), which limits the structure of the group G. In the following examples we shall see situations where Sylow's Theorem alone does not force the existence of a normal subgroup, however some additional argument (often involving studying the elements of order p for a number of different primes p) proves the existence of a normal Sylow subgroup.

Example: (Groups of order pq, p and q primes with $p < q$)

Suppose $|G| = pq$ for primes p and q with $p < q$. Let $P \in Syl_p(G)$ and let $Q \in Syl_q(G)$. We show that Q is normal in G and if P is also normal in G, then G is cyclic.

Now the three conditions: $n_q = 1 + kq$ for some $k \geq 0$, n_q divides p and $p < q$, together force $k = 0$. Since $n_q = 1$, $Q \trianglelefteq G$.

Since n_p divides the prime q, the only possibilities are $n_p = 1$ or q. In particular, if $p \nmid q - 1$, (that is, if $q \not\equiv 1 (\text{mod } p)$), then n_p cannot equal q, so $P \trianglelefteq G$.

Let $P = \langle x \rangle$ and $Q = \langle y \rangle$. If $P \trianglelefteq G$, then since $G/C_G(P)$ is isomorphic to a subgroup of $\text{Aut}(Z_p)$ and the latter group has order $p - 1$, Lagrange's Theorem together with the observation that neither p nor q can divide $p - 1$ implies that $G = C_G(P)$. In this case $x \in P \leq Z(G)$ so x and y commute. (Alternatively, this follows immediately from Exercise 42 of Section 3.1.) This means $|xy| = pq$ (cf. the exercises in Section 2.3), hence in this case G is cyclic: $G \cong Z_{pq}$.

If $p \mid q - 1$, we shall see in Chapter 5 that there is a unique non-abelian group of order pq (in which, necessarily, $n_p = q$). We can prove the existence of this group now. Let Q be a Sylow q-subgroup of the symmetric group of degree q, S_q. By Exercise 34 in Section 3, $|N_{S_q}(Q)| = q(q - 1)$. By assumption, $p \mid q - 1$ so by Cauchy's Theorem $N_{S_q}(Q)$ has a subgroup, P, of order p. By Corollary 15 in Section 3.2, PQ is a group of order pq. Since $C_{S_q}(Q) = Q$ (Example 2, Section 3), PQ is a non-abelian group. The essential ingredient in the uniqueness proof of PQ is Theorem 17 on the cyclicity of $\text{Aut}(Z_q)$.

Example: (Groups of order 30)

Let G be a group of order 30. We show that G has a normal subgroup isomorphic to Z_{15}. We shall use this information to classify groups of order 30 in the next chapter. Note that any subgroup of order 15 is necessarily normal (since it is of index 2) and cyclic (by the preceding result) so it is only necessary to show there exists a subgroup of order 15. The quickest way of doing this is to quote Exercise 13 in Section 2. We give an alternate argument which illustrates how Sylow's Theorem can be used in conjunction with a counting of elements of prime order to produce a normal subgroup.

Let $P \in Syl_5(G)$ and let $Q \in Syl_3(G)$. If either P or Q is normal in G, by Corollary 15, Chapter 3, PQ is a group of order 15. Note also that if either P or Q is normal, then both P and Q are characteristic subgroups of PQ, and since $PQ \trianglelefteq G$, *both* P and Q are normal in G (Exercise 8(a), Section 4). Assume therefore that neither Sylow subgroup is normal. The only possibilities by Part 3 of Sylow's Theorem are $n_5 = 6$ and $n_3 = 10$. Each element of order 5 lies in a Sylow 5-subgroup, each Sylow 5-subgroup contains 4 nonidentity elements and, by Lagrange's Theorem, distinct Sylow 5-subgroups intersect in the identity. Thus the number of elements of order 5 in G is the number of nonidentity elements in one Sylow 5-subgroup times the number of Sylow 5-subgroups. This would be $4 \cdot 6 = 24$ elements of order 5. By similar reasoning, the number of elements of order 3 would be $2 \cdot 10 = 20$. This is absurd since a group of order 30 cannot contain $24 + 20 = 44$ distinct elements. One of P or Q (hence both) must be normal in G.

This sort of counting technique is frequently useful (cf. also Section 6.2) and works particularly well when the Sylow p-subgroups have order p (as in this example), since then the intersection of two distinct Sylow p-subgroups must be the identity. If the order of the Sylow p-subgroup is p^α with $\alpha \geq 2$, greater care is required in counting elements, since in this case distinct Sylow p-subgroups may have many more elements in common, i.e., the intersection may be nontrivial.

Example: (Groups of order 12)

Let G be a group of order 12. We show that either G has a normal Sylow 3-subgroup or $G \cong A_4$ (in the latter case G has a normal Sylow 2-subgroup). We shall use this information to classify groups of order 12 in the next chapter.

Suppose $n_3 \neq 1$ and let $P \in Syl_3(G)$. Since $n_3 \mid 4$ and $n_3 \equiv 1 \pmod 3$, it follows that $n_3 = 4$. Since distinct Sylow 3-subgroups intersect in the identity and each contains two elements of order 3, G contains $2 \cdot 4 = 8$ elements of order 3. Since $|G : N_G(P)| = n_3 = 4$, $N_G(P) = P$. Now G acts by conjugation on its four Sylow 3-subgroups, so this action affords a permutation representation

$$\varphi : G \to S_4$$

(note that we could also act by left multiplication on the left cosets of P and use Theorem 3). The kernel K of this action is the subgroup of G which normalizes all Sylow 3-subgroups of G. In particular, $K \leq N_G(P) = P$. Since P is not normal in G by assumption, $K = 1$, i.e., φ is injective and

$$G \cong \varphi(G) \leq S_4.$$

Since G contains 8 elements of order 3 and there are precisely 8 elements of order 3 in S_4, all contained in A_4, it follows that $\varphi(G)$ intersects A_4 in a subgroup of order at least 8. Since both groups have order 12 it follows that $\varphi(G) = A_4$, so that $G \cong A_4$.

Note that A_4 does indeed have 4 Sylow 3-subgroups (see Example 4 following Corollary 20), so that such a group G does exist. Also, let V be a Sylow 2-subgroup of A_4. Since $|V| = 4$, it contains all of the remaining elements of A_4. In particular, there cannot be another Sylow 2-subgroup. Thus $n_2(A_4) = 1$, i.e., $V \trianglelefteq A_4$ (which one can also see directly because V is the identity together with the three elements of S_4 which are products of two disjoint transpositions, that is, V is a union of conjugacy classes).

Example: (Groups of order p^2q, p and q distinct primes)

Let G be a group of order p^2q. We show that G has a normal Sylow subgroup (for either p or q). We shall use this information to classify some groups of this order in the next chapter (cf. Exercises 8 to 12 of Section 5.5). Let $P \in Syl_p(G)$ and let $Q \in Syl_q(G)$.

Consider first when $p > q$. Since $n_p \mid q$ and $n_p = 1 + kp$, we must have $n_p = 1$. Thus $P \trianglelefteq G$.

Consider now the case $p < q$. If $n_q = 1$, Q is normal in G. Assume therefore that $n_q > 1$, i.e., $n_q = 1 + tq$, for some $t > 0$. Now n_q divides p^2 so $n_q = p$ or p^2. Since $q > p$ we cannot have $n_q = p$, hence $n_q = p^2$. Thus

$$tq = p^2 - 1 = (p - 1)(p + 1).$$

Since q is prime, either $q \mid p-1$ or $q \mid p+1$. The former is impossible since $q > p$ so the latter holds. Since $q > p$ but $q \mid p+1$, we must have $q = p+1$. This forces $p = 2$, $q = 3$ and $|G| = 12$. The result now follows from the preceding example.

Groups of Order 60

We illustrate how Sylow's Theorems can be used to unravel the structure of groups of a given order even if some groups of that order may be simple. Note the technique of changing from one prime to another and the inductive process where we use results on groups of order < 60 to study groups of order 60.

Proposition 21. If $|G| = 60$ and G has more than one Sylow 5-subgroup, then G is simple.

Proof: Suppose by way of contradiction that $|G| = 60$ and $n_5 > 1$ but that there exists H a normal subgroup of G with $H \neq 1$ or G. By Sylow's Theorem the only possibility for n_5 is 6. Let $P \in Syl_5(G)$, so that $|N_G(P)| = 10$ since its index is n_5.

If $5 \mid |H|$ then H contains a Sylow 5-subgroup of G and since H is normal, it contains all 6 conjugates of this subgroup. In particular, $|H| \geq 1 + 6 \cdot 4 = 25$, and the only possibility is $|H| = 30$. This leads to a contradiction since a previous example proved that any group of order 30 has a normal (hence unique) Sylow 5-subgroup. This argument shows 5 does not divide $|H|$ for any proper normal subgroup H of G.

If $|H| = 6$ or 12, H has a normal, hence characteristic, Sylow subgroup, which is therefore also normal in G. Replacing H by this subgroup if necessary, we may assume $|H| = 2$, 3 or 4. Let $\overline{G} = G/H$, so $|\overline{G}| = 30$, 20 or 15. In each case, $\overline{G}$ has a normal subgroup $\overline{P}$ of order 5 by previous results. If we let H_1 be the complete preimage of $\overline{P}$ in G, then $H_1 \trianglelefteq G$, $H_1 \neq G$ and $5 \mid |H_1|$. This contradicts the preceding paragraph and so completes the proof.

Corollary 22. A_5 is simple.

Proof: The subgroups $\langle (1\,2\,3\,4\,5) \rangle$ and $\langle (1\,3\,2\,4\,5) \rangle$ are distinct Sylow 5-subgroups of A_5 so the result follows immediately from the proposition.

The next proposition shows that there is a unique simple group of order 60.

Proposition 23. If G is a simple group of order 60, then $G \cong A_5$.

Proof: Let G be a simple group of order 60, so $n_2 = 3$, 5 or 15. Let $P \in Syl_2(G)$ and let $N = N_G(P)$, so $|G : N| = n_2$.

First observe that G has no proper subgroup H of index less that 5, as follows: if H were a subgroup of G of index 4, 3 or 2, then, by Theorem 3, G would have a normal subgroup K contained in H with G/K isomorphic to a subgroup of S_4, S_3 or S_2. Since $K \neq G$, simplicity forces $K = 1$. This is impossible since 60 ($= |G|$) does not divide 4!. This argument shows, in particular, that $n_2 \neq 3$.

If $n_2 = 5$, then N has index 5 in G so the action of G by left multiplication on the set of left cosets of N gives a permutation representation of G into S_5. Since (as above) the kernel of this representation is a proper normal subgroup and G is simple, the kernel is 1 and G is isomorphic to a subgroup of S_5. Identify G with this isomorphic copy so that we may assume $G \leq S_5$. If G is not contained in A_5, then $S_5 = GA_5$ and, by the Second Isomorphism Theorem, $A_5 \cap G$ is of index 2 in G. Since G has no (normal) subgroup of index 2, this is a contradiction. This argument proves $G \leq A_5$. Since $|G| = |A_5|$, the isomorphic copy of G in S_5 coincides with A_5, as desired.

Finally, assume $n_2 = 15$. If for every pair of distinct Sylow 2-subgroups P and Q of G, $P \cap Q = 1$, then the number of nonidentity elements in Sylow 2-subgroups of G would be $(4-1) \cdot 15 = 45$. But $n_5 = 6$ so the number of elements of order 5 in G is $(5-1) \cdot 6 = 24$, accounting for 69 elements. This contradiction proves that there exist distinct Sylow 2-subgroups P and Q with $|P \cap Q| = 2$. Let $M = N_G(P \cap Q)$. Since P and Q are abelian (being groups of order 4), P and Q are subgroups of M and since G is simple, $M \neq G$. Thus 4 divides $|M|$ and $|M| > 4$ (otherwise, $P = M = Q$). The only possibility is $|M| = 12$, i.e., M has index 5 in G (recall M cannot have index 3 or 1). But now the argument of the preceding paragraph applied to M in place of N gives $G \cong A_5$. This leads to a contradiction in this case because $n_2(A_5) = 5$ (cf. the exercises). The proof is complete.

EXERCISES

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

1. Prove that if $P \in Syl_p(G)$ and H is a subgroup of G containing P then $P \in Syl_p(H)$. Give an example to show that, in general, a Sylow p-subgroup of a subgroup of G need not be a Sylow p-subgroup of G.
2. Prove that if H is a subgroup of G and $Q \in Syl_p(H)$ then $gQg^{-1} \in Syl_p(gHg^{-1})$ for all $g \in G$.
3. Use Sylow's Theorem to prove Cauchy's Theorem. (Note that we only used Cauchy's Theorem for abelian groups — Proposition 3.21 — in the proof of Sylow's Theorem so this line of reasoning is not circular.)
4. Exhibit all Sylow 2-subgroups and Sylow 3-subgroups of D_{12} and $S_3 \times S_3$.
5. Show that a Sylow p-subgroup of D_{2n} is cyclic and normal for every odd prime p.
6. Exhibit all Sylow 3-subgroups of A_4 and all Sylow 3-subgroups of S_4.
7. Exhibit all Sylow 2-subgroups of S_4 and find elements of S_4 which conjugate one of these into each of the others.
8. Exhibit two distinct Sylow 2-subgroups of S_5 and an element of S_5 that conjugates one into the other.
9. Exhibit all Sylow 3-subgroups of $SL_2(\mathbb{F}_3)$ (cf. Exercise 9, Section 2.1).
10. Prove that the subgroup of $SL_2(\mathbb{F}_3)$ generated by $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is the unique Sylow 2-subgroup of $SL_2(\mathbb{F}_3)$ (cf. Exercise 10, Section 2.4).
11. Show that the center of $SL_2(\mathbb{F}_3)$ is the group of order 2 consisting of $\pm I$, where I is the identity matrix. Prove that $SL_2(\mathbb{F}_3)/Z(SL_2(\mathbb{F}_3)) \cong A_4$. [Use facts about groups of order 12.]
12. Let $2n = 2^a k$ where k is odd. Prove that the number of Sylow 2-subgroups of D_{2n} is k. [Prove that if $P \in Syl_2(D_{2n})$ then $N_{D_{2n}}(P) = P$.]

13. Prove that a group of order 56 has a normal Sylow p-subgroup for some prime p dividing its order.

14. Prove that a group of order 312 has a normal Sylow p-subgroup for some prime p dividing its order.

15. Prove that a group of order 351 has a normal Sylow p-subgroup for some prime p dividing its order.

16. Let $|G| = pqr$, where p, q and r are primes with $p < q < r$. Prove that G has a normal Sylow subgroup for either p, q or r.

17. Prove that if $|G| = 105$ then G has a normal Sylow 5-subgroup and a normal Sylow 7-subgroup.

18. Prove that a group of order 200 has a normal Sylow 5-subgroup.

19. Prove that if $|G| = 6545$ then G is not simple.

20. Prove that if $|G| = 1365$ then G is not simple.

21. Prove that if $|G| = 2907$ then G is not simple.

22. Prove that if $|G| = 132$ then G is not simple.

23. Prove that if $|G| = 462$ then G is not simple.

24. Prove that if G is a group of order 231 then $Z(G)$ contains a Sylow 11-subgroup of G and a Sylow 7-subgroup is normal in G.

25. Prove that if G is a group of order 385 then $Z(G)$ contains a Sylow 7-subgroup of G and a Sylow 11-subgroup is normal in G.

26. Let G be a group of order 105. Prove that if a Sylow 3-subgroup of G is normal then G is abelian.

27. Let G be a group of order 315 which has a normal Sylow 3-subgroup. Prove that $Z(G)$ contains a Sylow 3-subgroup of G and deduce that G is abelian.

28. Let G be a group of order 1575. Prove that if a Sylow 3-subgroup of G is normal then a Sylow 5-subgroup and a Sylow 7-subgroup are normal. In this situation prove that G is abelian.

29. If G is a non-abelian simple group of order < 100, prove that $G \cong A_5$. [Eliminate all orders but 60.]

30. How many elements of order 7 must there be in a simple group of order 168?

31. For $p = 2, 3$ and 5 find $n_p(A_5)$ and $n_p(S_5)$. [Note that $A_4 \leq A_5$.]

32. Let P be a Sylow p-subgroup of H and let H be a subgroup of K. If $P \trianglelefteq H$ and $H \trianglelefteq K$, prove that P is normal in K. Deduce that if $P \in Syl_p(G)$ and $H = N_G(P)$, then $N_G(H) = H$ (in words: *normalizers of Sylow p-subgroups are self-normalizing*).

33. Let P be a normal Sylow p-subgroup of G and let H be any subgroup of G. Prove that $P \cap H$ is the unique Sylow p-subgroup of H.

34. Let $P \in Syl_p(G)$ and assume $N \trianglelefteq G$. Use the conjugacy part of Sylow's Theorem to prove that $P \cap N$ is a Sylow p-subgroup of N. Deduce that PN/N is a Sylow p-subgroup of G/N (note that this may also be done by the Second Isomorphism Theorem — cf. Exercise 9, Section 3.3).

35. Let $P \in Syl_p(G)$ and let $H \leq G$. Prove that $gPg^{-1} \cap H$ is a Sylow p-subgroup of H for some $g \in G$. Give an explicit example showing that $hPh^{-1} \cap H$ is not necessarily a Sylow p-subgroup of H for any $h \in H$ (in particular, we cannot always take $g = 1$ in the first part of this problem, as we could when H was normal in G).