553 Review Groups!

24. Does the Symmetric group S_5 have a subgroup of order 10? Justify

Yes. The group D_{2n} acts transitively on $A = \{1, 2, 3, \ldots, n\}$ by visualizing A as the vertices of a regular n-gon in the plane, with r representing a $\frac{2\pi}{n}$ rotation and s representing a reflection about the line passing through the center and a vertex. Moreover, this action is faithful.
Since actions induce a homomorphism $\varphi: D_{2n} \to S_n$, we get that $D_{2n} \hookrightarrow S_n$ since the $\ker \varphi = \{1\}$ (because the action is faithful).
By the First Isomorphism Theorem, $D_{2n} \cong \varphi(D_{2n}) \leq S_n$.
Hence $D_{10} \cong \varphi(D_{10}) \leq S_5$.

---

25. Let G be a subgroup generated by a 5-cycle in S_5. Find the order of $N_{S_5}(G)$.

Solution: By order arguments, $G \in Syl_5(S_5)$. Thus, $|S_5 : N_{S_5}(G)| = n_5$ by Sylow's Theorem.
Now, $n_5 \equiv 1 \bmod 5$, and $n_5 \mid 4 \cdot 3 \cdot 2 = 24$. The only possibilities are $n_5 = 1$ or $n_5 = 6$.
All elements of order 5 are even permutations, so $G \in Syl_5(A_5)$.
Since A_5 is simple, $n_5(A_5) \neq 1$. Hence $n_5(S_5) \neq 1$.
So $n_5(S_5) = 6$.
$\therefore \quad |N_{S_5}(G)| = \frac{|S_5|}{n_5(S_5)} = \frac{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{6} = 20$

26. Show that for any element σ of order 2 in the alternating group A_n, $\exists \tau \in S_n$ s.t. $\tau^2 = \sigma$.

Solution. Consider the unique representation of σ as a product of disjoint cycles. Since disjoint cycles commute, $|\sigma| =$ lcm of the orders of the cycles comprising σ.
Since every n-cycle has order n and $|\sigma| = 2$, it follows that σ is a product of disjoint transpositions.
Since $\sigma \in A_n$, σ is even, and so consists of an even number of disjoint transpositions.
Say, $\sigma = (a_1\ b_1)(a_2\ b_2) \cdots (a_{2k}\ b_{2k})$
It is a quick check to see that $(a\ b)(c\ d) = (a\ c\ b\ d)^2$.
Hence $\sigma = (a_1\ a_2\ b_1\ b_2)^2 \cdots (a_{2k-1}\ a_{2k}\ b_{2k-1}\ b_{2k})^2$
Since each cycle is disjoint from all others, all of these cycles commute, so

$$\sigma = \underbrace{[(a_1\ a_2\ b_1\ b_2) \cdots (a_{2k-1}\ a_{2k}\ b_{2k-1}\ b_{2k})]^2}_{= \tau^2}$$

27. Let G be a finite group, $p > 0$ a prime number. Show that a subgroup $H < G$ contains a Sylow p-subgroup of G if and only if $p \nmid [G:H]$.

Proof. The result is trivially true if $p \nmid |G|$.

Suppose $|G| = p^\alpha m$ where $p \nmid m$.

($\Rightarrow$): Let $P \in \mathrm{Syl}_p(G)$ with $P \leq H$. By Lagrange's Theorem, $|P| \,/\, |H|$. But $|P| = p^\alpha$. Hence $p^\alpha \,/\, |H|$. Say $|H| = p^\alpha k$ with $p \nmid k$. Then $[G:H] = \frac{|G|}{|H|} = \frac{p^\alpha m}{p^\alpha k} = \frac{m}{k}$. Since $p \nmid m$, $p \nmid [G:H]$.

($\Leftarrow$): Suppose $p \nmid [G:H] = \frac{|G|}{|H|} = \frac{p^\alpha m}{|H|}$.

It follows that $|H| = p^\alpha k$ for some k, $p \nmid k$.

Let $P \in \mathrm{Syl}_p(H)$. $|P| = p^\alpha$, a p-subgroup of G.

By Sylow's Theorem, $\exists\ Q \in \mathrm{Syl}_p(G)$ with $P \leq Q$.

Since $P \leq Q$ and $|P| = p^\alpha = |Q|$, $P = Q$. Thus, H contains a Sylow p-subgroup of G.

28. Let G be a finite group, $p > 0$ a prime number, and H a normal subgroup of G. Prove the following:

(a) Any Sylow p-subgroup of H is the intersection $P \cap H$ of a Sylow p-subgroup P of G and subgroup H.

Proof. Let $Q \in \text{Syl}_p(H)$. By Sylow's Theorem, $\exists\ P \in \text{Syl}_p(G)$ s.t. $Q \leq P$. $Q \leq H$ and $Q \leq P$, so $Q \leq P \cap H$.
By Lagrange's Theorem, since $P \cap H \leq P$, $P \cap H$ is a p-group. Moreover, $P \cap H \leq H$, so by Sylow's Theorem, $\exists\ R \in \text{Syl}_p(H)$ s.t. $P \cap H \leq R$. Then $Q \leq P \cap H \leq R$ and $|Q| = |R|$, so $Q = R$, meaning $P \cap H = Q$.

(b) Any Sylow p-subgroup of G/H is the quotient PH/H, where $P \in \text{Syl}_p(G)$.

Proof. We begin by showing that if $R \in \text{Syl}_p(G)$, then $RH/H \in \text{Syl}_p(G/H)$. Since $H \trianglelefteq G$, $RH \leq G$. By the second Isomorphism Theorem, $RH/H \cong R/R \cap H$. Since $|R| = p^\alpha$ for some α, and $R \cap H \leq R$, it follows that RH/H is a p-subgroup of G/H. By the Fourth Isomorphism Theorem, $[G/H : RH/H] = [G : RH]$. $p \nmid [G : RH]$ since $R \leq RH$, and $p \nmid [G : R]$. Thus, RH/H is a Sylow p-subgroup of G/H.
Now, let $Q \in \text{Syl}_p(G/H)$. Since $Q, RH/H \in \text{Syl}_p(G/H)$, by Sylow's Theorem Q and RH/H are conjugate. $\exists\ g \in G$ s.t. $Q = (gH)(RH/H)(g^{-1}H)$. If $K \leq G$ with $K/H = Q$ (guaranteed by Fourth Iso Thm), then $K = gRHg^{-1}$. Let $rh \in RH$. Then $grhg^{-1} = gr(g^{-1}g)hg^{-1}$ which equals $grg^{-1}h'$ for some $h' \in H$ since $H \trianglelefteq G$. Thus, $K = gRg^{-1}H$. But $gRg^{-1} = P$ for some $P \in \text{Syl}_p(G)$. Thus $PH/H = K/H = Q$.

29. Let H be a normal subgroup of a finite group G, and let $N \subset H$ be a normal Sylow subgroup of H. Prove that N is a normal subgroup of G.

Proof. $N \in \mathrm{Syl}_p(H)$ is normal in $H \Leftrightarrow N$ char H.
Thus, it suffices to show that a characteristic subgroup of a normal subgroup is normal.
Let $g \in G$. Now, $gNg^{-1} \leq gHg^{-1} = H$.
Conjugation of H by an element of H is an automorphism of H (since H is normal). Thus $gNg^{-1} = N$ since N char H. Therefore, $N \trianglelefteq G$.

Alternatively, one could note that $N \trianglelefteq H \Leftrightarrow n_p = 1$.
Then $gNg^{-1} \leq gHg^{-1} = H \Rightarrow gNg^{-1} \in \mathrm{Syl}_p(H)$. Since $n_p = 1$, $gNg^{-1} = N$.

30. Let G be a finite group, $p>0$ a prime number, and H a normal p-subgroup of G. Prove the following:

(a) H is contained in each Sylow p-subgroup of G.

Proof. Since H is a p-subgroup of G, by Sylow's Theorem, $\exists\ P \in \mathrm{Syl}_p(G)$ s.t. $H \subseteq P$. Let $P' \in \mathrm{Syl}_p(G)$. By Sylow's Theorem, $\exists\ g \in G$ s.t. $P' = gPg^{-1}$. Since $H \subseteq P$, $gHg^{-1} \subseteq P'$, but since $H \trianglelefteq G$, $gHg^{-1} = H$. So $H \subseteq P'$. Hence H is contained in each Sylow p-subgroup of G.

(b) If K is a normal p-subgroup of G, then HK is a normal p-subgroup of G.

Proof. Since $K \trianglelefteq G$, $HK \leq G$. Moreover, $|HK| = \frac{|H||K|}{|H \cap K|}$. Since $H \cap K \leq K$ a p-group, $H \cap K$ is a p-group. H is also a p-group. Thus, $|HK|$ is a power of p. Thus, HK is a p-subgroup of G.
Let $hk \in HK$. Let $g \in G$.
$ghkg^{-1} = gh(g^{-1}g)kg^{-1} = (ghg^{-1})(gkg^{-1}) = h'k'$ for some $h' \in H$, $k' \in K$ since $H \trianglelefteq G$, $K \trianglelefteq G$. Thus, $ghkg^{-1} \in HK$, so $gHKg^{-1} = HK$; thus $HK \trianglelefteq G$.

31. Prove that the automorphism group of $(\mathbb{Z}/3)^4$ is $80 \times 78 \times 72 \times 54$.

Proof. In general, $\mathrm{Aut}[(\mathbb{Z}/p)^n] \cong GL(n, \mathbb{F}_p)$. (*)
Let $A \in GL(n, \mathbb{F}_p)$. Looking at the first column of A, we have p choices for each entry. However, the first column cannot be the zero vector. Hence, there are $p^n - 1$ choices for column 1. Column 2 can be anything but a linear combination of column 1. Since linear combinations of a single column are scalar multiples of said column, there are p possible choices for a scalar, so there are $p^n - p$ choices for column 2. Column 3 cannot be a linear combo of columns 1 & 2, so there are p choices for scalar of column 1 and p choices for scalar of column 2, meaning there are $p^n - p^2$ choices for column 3. Continuing this way, there are $(p^n-1)(p^n-p)(p^n-p^2)\cdots(p^n-p^{n-1})$ elements of $GL(n, \mathbb{F}_p)$, and hence, also of $\mathrm{Aut}[(\mathbb{Z}/p)^n]$.

Thus, $|(\mathbb{Z}/3)^4| = |GL(4,3)| = (3^4-1)(3^4-3)(3^4-3^2)(3^4-3^3)$

$= 81 \cdot (81-3) \cdot (81-9) \cdot (81-27)$

$= 81 \cdot 78 \cdot 72 \cdot 54$

(*) $(\mathbb{Z}/p)^n$ is isomorphic to $\mathbb{F}_p^n$, an n-dimensional vector space over the field $\mathbb{F}_p$. An automorphism $\varphi: \mathbb{F}_p^n \to \mathbb{F}_p^n$ is a bijective linear transformation, i.e., a nonsingular $n \times n$ matrix with entries in $\mathbb{F}_p$. Hence, it is isomorphic to $GL(n, \mathbb{F}_p)$.

32. Prove, for fixed n, that the following conditions are equivalent:
(a) Every abelian group of order n is cyclic.
(b) n is square free (i.e., not divisible by any square integer >1).

Proof. (a) $\Rightarrow$ (b): By the Fundamental Theorem of Finitely Generated Abelian groups, $G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$ where $n_{i+1} | n_i$ for $1 \le i \le s-1$. Since $\mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s}$, it follows that $(n_i, n_j) = 1 \ \forall i \neq j$. Thus, $n = n_1 \cdots n_s$ is square free.
(Alternatively, assume $n = d^2 m$. Then $\mathbb{Z}_{dm} \times \mathbb{Z}_d$ is an Abelian group of order n which is not cyclic).

(b) $\Rightarrow$ (a): Let $n = p_1 \cdots p_s$ be a unique factorization of n into primes. Since n is square free, $p_i \neq p_j \ \forall i \neq j$. We induct of s. This is trivial for $s = 1$ by Cauchy's Theorem. Suppose that for all $k \le s-1$, $\mathbb{Z}_{p_1 \cdots p_k} \cong \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_k}$.
Now, consider $\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_s} = (\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_{s-1}}) \times \mathbb{Z}_{p_s}$
$\cong \mathbb{Z}_{p_1 \cdots p_{s-1}} \times \mathbb{Z}_{p_s}$ by induction hypothesis.
Since $(p_1 \cdots p_{s-1}, p_s) = 1$, $\cong \mathbb{Z}_n$.
Therefore, (a) holds.

33. Prove that there is no simple group of order 4125.

Proof. Suppose $|G| = 4125 = 11 \cdot 5^3 \cdot 3$ with G simple. Since G is simple, $n_5 \neq 1$. Since $n_5 \equiv 1 \bmod 5$ and $n_5 \mid 11 \cdot 3$, it follows that $n_5 = 11$. By Sylow's Theorem, $[G : N_G(P)] = n_5$ where $P \in \mathrm{Syl}_5(G)$. Let A be the set of left cosets of $N_G(P)$. By the calculation above and Lagrange's Theorem, $|A| = 11$. Let G act by left multiplication on A. This action is transitive and induces a homomorphism $\varphi : G \to S_{11}$. Since $\ker \varphi \trianglelefteq G$, and G is simple, it follows that $\ker \varphi = \{1\}$. (Transitivity ensures $\ker \varphi \neq G$.)
Thus, by the First Isomorphism Theorem, G is isomorphic to a subgroup of S_{11}. By Lagrange's Theorem, $|G| \mid |S_{11}|$. Hence, $11 \cdot 5^3 \cdot 3 \mid 11!$ But the highest power of 5 dividing $11!$ is 5^2. This is a contradiction. Hence, G is not simple.

34. Show that P is abelian whenever $\mathrm{Aut}(P)$ is cyclic.

Proof. $P/Z(P) \cong \mathrm{Inn}(P) \leq \mathrm{Aut}(P)$. Since $\mathrm{Aut}(P)$ is cyclic and subgroups of cyclic groups are cyclic (*), $P/Z(P)$ is cyclic. Hence, P is abelian. (**)

(*) Let $G = \langle a \rangle$ and $H \leq G$. If $H = \{e\}$, then $H = \langle e \rangle$. Assume $H \neq \{e\}$. Since G is cyclic and $H \leq G$, all elements of H are powers of a. Let $c = a^n$ be an element of H with n minimal. We will show that $H = \langle c \rangle$. Let $b \in H \leq G$. Then $b = a^m$. It follows that $n < m$ (assuming $b \neq c$). Thus, $\exists\ q, r \in \mathbb{N}$ s.t. $m = qn + r$ where $r < n$.
$b = a^m = a^{qn+r} = (a^n)^q a^r = c^q a^r$. Then $a^r = bc^{-q} \in H$. Since $r < n$ and $a^r \in H$, by minimality of n, $r = 0$. Thus, $b = a^m = (a^n)^q = c^q$. Thus, $H = \langle c \rangle$.

(**). Suppose $G/Z(G)$ is cyclic. Let $xZ(G)$ generate $G/Z(G)$. If $y \in G$, then $yZ(G) = x^a Z(G)$ for some $a \in \mathbb{Z}$. Thus $y = x^a z$ for some $z \in Z(G)$.
Let $g, h \in G$. Then $g = x^a z_1$, $h = x^b z_2$ for $a, b \in \mathbb{Z}$, $z_1, z_2 \in Z(G)$.
$gh = (x^a z_1)(x^b z_2) = z_1 x^a x^b z_2 = z_2 x^{a+b} z_1 = z_2 x^b \cdot x^a z_1$
$= x^b z_2 \cdot x^a z_1 = hg$.

35. Let G be a finite group of order pqr, where $p > q > r$ are prime.

(a) If G fails to have a normal subgroup of order p, determine the number of elements in G of order p.

Solution. $n_p \equiv 1 \bmod p$ and $n_p \mid qr$. The only divisors of qr are $1, q, r$, and qr. Since $1 < r < q < p$, it follows that $n_p = 1$ or qr. But since G has no normal subgroup of order p, $n_p \neq 1$. Thus, $n_p = qr$. Since all groups of order p are cyclic, all distinct groups of order p intersect trivially. Thus, each one has $p-1$ elements of order p. Therefore, there are $qr(p-1)$ elements of order p.

(b) If G fails to have a normal subgroup of order q, prove that G has at least q^2 elements of order q.

Solution. As above, $n_q \equiv 1 \bmod q$, $n_q \mid pr$, and $n_q \neq 1$. Since $1 < r < q$, it follows that $n_q \neq r$, so $n_q = p$ or pr. Since $pr > p$, we will assume $n_q = p$. As above, there are $p(q-1) = pq - p$ elements of order q. Since $q < p$, $q + k = p$ for some $k \in \mathbb{N}$. Then there are $(q+k)q - (q+k)$ elements of order q. i.e., $q^2 + kq - (q+k)$ elements of order q. If $k > 1$, then $kq \geq q + k$, so the result is proved. If $k = 1$, then $q + 1 = p$, so $q = 2$ and $p = 3$. This is not possible as $r < q$ is a prime. Thus, G has at least q^2 elements of order q.

35 (c) Prove that G has a nontrivial normal subgroup.

Proof. We may assume $n_p \neq 1$ and $n_q \neq 1$ or we are done. Then G has $qr(p-1)$ elements of order p and at least q^2 elements of order q. G has 1 identity element.
Now, consider $pqr - qr(p-1) - q^2 - 1$
$= pqr - pqr + qr - q^2 - 1 = qr - q^2 - 1$
By similar arguments to (a) and (b), if $n_r \neq 1$, then G has at least $q(r-1) = qr - q$ elements of order r.
Hence, $qr - q^2 - 1 - qr + q = q - q^2 - 1$ other elements.
But $q^2 > q$, so this means G has negative elements remaining. This is a contradiction. Hence, $n_p = 1$ or $n_q = 1$ or $n_r = 1$, giving G a nontrivial normal subgroup.

36. Find all abelian groups of order 60. Find the number of elements of order 6 in each group.

Solution. By the Fundamental Theorem of Finitely Generated Abelian groups, the abelian groups of order 60 are $G_1 = \mathbb{Z}_{60}$, $G_2 = \mathbb{Z}_{30} \times \mathbb{Z}_2$. No other groups are possible since $60 = 5 \cdot 3 \cdot 2^2$ and $\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$ iff $(p, q) = 1$.

In $G_1 = \mathbb{Z}_{60}$, there is a unique subgroup of order 6 having $\varphi(6) = \varphi(2)\varphi(3) = (1)(2) = 2$ elements of order 6.

In G_2, since G_2 is abelian, elements of order 6 are composed of $a \times b$ where $\text{lcm}(|a|, |b|) = 6$.
Thus, elements of order 6 are of the form
$a \times b$ where $|a| = 6$ & $|b| = 1$, $|a| = 6$ & $|b| = 2$,
$|a| = 3$ & $|b| = 2$.
In $\mathbb{Z}_{30}$, there are $\varphi(6) = 2$ elements of order 6 and $\varphi(3) = 2$ elements of order 3. Since $\mathbb{Z}_2$ has precisely 1 element of order 1 and 1 element of order 2, there are $2 \cdot 1 + 2 \cdot 1 + 2 \cdot 1 = 2 + 2 + 2 = 6$ elements of order 6 in $G_2 = \mathbb{Z}_{30} \times \mathbb{Z}_2$.

37. Show that any group G of order 80 is solvable.

Solution. First, we notice that every finite p-group is solvable. Let P be a p-group. i.e., $|P| = p^n$. We induct on n. For $n=1$, $|P| = p$, so $1 \trianglelefteq P$ is a solvable series since P is Abelian (so $P/\langle 1 \rangle$ is Abelian). Suppose this is true for $n-1$. Now, let $|P| = p^n$. Since P is a p-group, $\exists\, Q \leq P$ with $|Q| = p^{n-1}$. $[P:Q] = \frac{|P|}{|Q|} = \frac{p^n}{p^{n-1}} = p$, the smallest prime dividing $|P|$. Thus, $Q \trianglelefteq P$. By induction hypothesis, Q is solvable. Moreover, $P/Q \cong \mathbb{Z}_p$ is solvable. Thus, P is solvable.
We also note that abelian groups are solvable.
Here, we used the fact that if $H \trianglelefteq G$, H and G/H solvable, then G is solvable.

Let $|G| = 80 = 5 \cdot 2^4$.
If $n_2 = 1$, and $P \in \mathrm{Syl}_2(G)$, then $|P| = 2^4$ and $P \trianglelefteq G$.
$|G/P| = \frac{5 \cdot 2^4}{2^4} = 5$, so $G/P \cong \mathbb{Z}_5$ which is solvable.
P is a 2-group and is solvable. Thus, G is solvable.

If $n_5 = 1$, and $Q \in \mathrm{Syl}_5(G)$, then $|Q| = 5$ and $Q \trianglelefteq G$.
$|G/Q| = \frac{5 \cdot 2^4}{5} = 2^4$, so G/Q is a 2-group which is solvable.
Q is a 5-group which is solvable, Thus, G is solvable.

If $n_5 \neq 1$, $n_5 = 16$. Thus, G has $16 \cdot 4 = 64$ elements of order 5.
$|G| - 64 = 80 - 64 = 16 = |P|$ for $P \in \mathrm{Syl}_2(G)$. Thus, $n_2 = 1$.
This means we always have $n_2 = 1$ or $n_5 = 1$, implying that G is always solvable.

38. Let G be a finite ~~solvable~~ group and suppose $Aut(G)$ is solvable. Show that G is solvable.

Proof. $Z(G) \trianglelefteq G$. Now, $G/Z(G) \cong Inn(G) \leq Aut(G)$. Since subgroups of solvable groups are solvable, $Inn(G)$ and hence $G/Z(G)$ is solvable. Now, $Z(G)$ is an Abelian group and all Abelian groups are solvable (since $1 \trianglelefteq H$ is a solvable series for H, Abelian). If a normal subgroup and the quotient by that normal subgroup are solvable, then the group itself is solvable. So since $Z(G)$ and $G/Z(G)$ are solvable, G is solvable.