Kris Harper
MATH 25700
Homework 5 November 6, 2009

Problem 1 (4.4.1). *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.)*

Proof. Let $x \in G$. Then

$$\sigma\varphi_g\sigma^{-1}(x) = \sigma(\varphi_g(\sigma^{-1}(x))) = \sigma(g\sigma^{-1}(x)g^{-1}) = \sigma(g)\sigma(\sigma^{-1}(x))\sigma(g^{-1}) = \sigma(g)x\sigma(g)^{-1} = \varphi_{\sigma(g)}.$$

Since $\varphi_g, \varphi_{\sigma(g)} \in \mathrm{Inn}(G)$ and $\sigma \in \mathrm{Aut}(G)$, we see that $\sigma\mathrm{Inn}(G)\sigma^{-1} \subseteq \mathrm{Inn}(G)$ for all $\sigma \in \mathrm{Aut}(G)$. Therefore $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. □

Problem 2 (4.4.3). *Prove that under any automorphism of D_8, r has at most 2 possible images and s has has at most 4 possible images. Deduce that $|\mathrm{Aut}(D_8)| \leq 8$.*

Proof. Note that $|sr^i| = 2$ since $(sr^i)(sr^i) = s^2r^{-i}r^i = 1$. Furthermore, $|r^2| = 2$ and $|r^3| = 4$. Since automorphisms preserve order, r must be mapped to either r or r^3. Furthermore, s can't be mapped to r^2 because then the image of sr is the same as the image of rs. Since automorphisms are homomorphisms, this is impossible. Therefore s can be mapped to one of sr^i for the four possible values of i. Since r and s are the two generators of D_8, there are at most $2 \cdot 4 = 8$ possible automorphisms of D_8. □

Problem 3 (4.4.6). *Prove that characteristic subgroups are normal. Give an example of a normal subgroup that is not characteristic.*

Proof. Let H be a characteristic subgroup and let φ_g be conjugation by $g \in G$. We know that φ_g is an automorphism and so $gHg^{-1} = \varphi_g(H) = H$. Since this is true for all $g \in G$, we see that $H \trianglelefteq G$. Consider the Klein 4-group V_4 with generators a, b, c. Then $\langle a \rangle$ is normal, since V_4 is abelian, but an automorphism which maps a to b, b to c and c to a won't fix $\langle a \rangle$. Thus $\langle a \rangle$ is not characteristic. □

Problem 4 (4.4.7). *If H is the unique subgroup of a given order in a group G prove H is characteristic in G.*

Proof. Let $\varphi \in \mathrm{Aut}(G)$ and let $a, b \in H$. Then $\varphi(a)\varphi(b)^{-1} = \varphi(ab^{-1}) \in \varphi(H)$. Therefore $\varphi(H) \leq G$ and so it's order is preserved. Since this is true for any subgroup of G, we know that if H has unique order among subgroups of G, then it is preserved by any automorphism of G. Therefore H char G. □

Problem 5 (4.4.8). *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.

Proof. (a) Suppose H char K and $K \trianglelefteq G$. Then for all $g \in G$, $gKg^{-1} = K$. But this is an automorphism of K and so $gHg^{-1} = H$ since H char K. Therefore $H \trianglelefteq G$.

(b) Let $\varphi \in \mathrm{Aut}(G)$. Then $\varphi(K) = K$ and so $\varphi \in \mathrm{Aut}(K)$. But then $\varphi(H) = H$ since H char K. Therefore H char G. To show that V_4 char S_4 note that V_4 char A_4 by Problem 4 since it is the only subgroup of order 4 in A_4. Likewise, A_4 char S_4 since it the unique subgroup of order 12 in S_4. Thus V_4 char S_4.

(c) Let $G = S_4$, $K = \langle (1\ 2)(3\ 4), (1\ 3)(2\ 4) \rangle$ and $H = \langle (1\ 2)(3\ 4) \rangle$. Then $H \trianglelefteq K$ since $K \cong V_4$ and so K is abelian. Also K char G using part (b). But then H is not normal in G as can be seen by conjugating by $(1\ 2\ 3)$. □

Problem 6 (4.4.15). *Prove that each of the following (multiplicative) groups is cyclic: $(\mathbb{Z}/5\mathbb{Z})^\times$, $(\mathbb{Z}/9\mathbb{Z})^\times$ and $(\mathbb{Z}/18\mathbb{Z})^\times$.*

Proof. We know that $(\mathbb{Z}/5\mathbb{Z})^\times \cong \mathrm{Aut}(\mathbb{Z}/5\mathbb{Z})$. Let $\Psi : (\mathbb{Z}/5\mathbb{Z})^\times \to \mathrm{Aut}(\mathbb{Z}/5\mathbb{Z})$ be an isomorphism such that $\Psi(a) = \psi_a$ where $\psi_a : \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$ is an isomorphism such that $\psi_a(x) = x^a$ for a generator x. Note that since ψ_a is an isomorphism, x^a must be a generator for $\mathbb{Z}/5\mathbb{Z}$ and so $(a, 4) = 1$. Such an a must exist in $(\mathbb{Z}/5\mathbb{Z})^\times$ because Ψ is an isomorphism. Now consider $\psi_b \in \mathrm{Aut}(\mathbb{Z}/5\mathbb{Z})$. We know $\psi_b(x) = x^b = (x^a)^b = (\psi_a(x))^b$. Therefore $\mathrm{Aut}(\mathbb{Z}/5\mathbb{Z})$ is cyclic and so $(\mathbb{Z}/5\mathbb{Z})^\times$ is cyclic as well. A similar argument holds for $(\mathbb{Z}/9\mathbb{Z})^\times$ and $(\mathbb{Z}/18\mathbb{Z})^\times$. $\square$

Problem 7 (4.4.16)**.** *Prove that* $(\mathbb{Z}/24\mathbb{Z})^\times$ *is an elementary abelian group of order* 8*.*

Proof. We know $|(\mathbb{Z}/24\mathbb{Z})^\times| = 8$ since $\varphi(24) = 8$. Furthermore, $\overline{1}^2 = \overline{5}^2 = \overline{7}^2 = \overline{11}^2 = \overline{13}^2 = \overline{17}^2 = \overline{19}^2 = \overline{23}^2 = \overline{1}$. Therefore since $(\mathbb{Z}/24\mathbb{Z})^\times$ has order 2^3 and each element applied to itself 2 times is the identity, it must be an elementary abelian group. $\square$

Problem 8 (4.4.20)**.** *For any finite group P let $d(P)$ be the minimum number of generators of P (so, for example, $d(P) = 1$ if an 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).
(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 $J(P) \trianglelefteq G$.

Proof. (a) Let φ be an automorphism of P. We know that for each abelian subgroup $A \le P$, φ must map A to some abelian subgroup $\varphi(A)$ of the same order. Furthermore, suppose $d(A) = k$ and $d(\varphi(A)) = k'$. Then it must be the case that $k = k'$. If one were less than the other then we could use φ or φ^{-1} and to find a smaller set of generators for A or $\varphi(A)$. Therefore for each abelian subgroup $A \le P$ we have $d(A) = d(\varphi(A))$. But this directly implies that $m(P) = m(\varphi(P))$. If $x \in J(P)$, then x is a product of elements of $A \le P$ where $d(A) = m(P)$. Then $\varphi(x)$ can be written as a product of images under φ of elements of these sets, and therefore $\varphi(x) \in \langle \varphi(A) \mid \varphi(A) \text{ is abelian and } d(\varphi(A)) = m(P)\rangle$. But we've just shown this set is precisely $J(P)$. Therefore $J(P)$ char P.

(b) For Q_8 the subgroups are $\langle i\rangle$, $\langle j\rangle$, $\langle k\rangle$, $\langle -1\rangle$ and $\langle 1\rangle$. For D_8 the subgroups are $\langle s, r^2\rangle$ and $\langle rs, r^2\rangle$. For D_{16} the subgroups are $\langle sr^2, r^4\rangle$, $\langle s, r^4\rangle$, $\langle sr^3, r^4\rangle$ and $\langle sr^5, r^4\rangle$. For QD_{16} the subgroups are $\langle a^4, x\rangle$ and $\langle a^4, a^2x\rangle$.

(c) Every subgroup of Q_8 is used to generate $J(Q_8)$. In particular, the cyclic group generated by every element is a generator for $J(Q_8)$. Thus $J(Q_8) = Q_8$. In $J(D_8)$, note that s and rs are both generators by part (b). But then $(rs)s = r$ is in $J(D_8)$ and so both generators of D_8 are in $J(D_8)$. Therefore the groups are equal. The case for $J(D_{16})$ is similar since s, sr^5 and r^4 are all generators of $J(D_{16})$. The group $J(QD_{16})$ is generated by a^4, x, and a^2x. Multiplying a^2x and x, it's easy to get a^4, so we have $J(QD_{16}) = \langle x, a^2\rangle$. Then these elements have order 2 and 4 respectively, so they can be mapped to s and r in D_8. In particular $x(a^2)^i = (a^2)^{-i}x$. This shows that $J(QD_{16}) \cong D_8$ in QD_{16}.

(d) Since $Q \le P$ it's certainly the case that $J(Q) \subseteq J(P)$. Let $x \in J(P)$. Then $x \in Q$ and x is the product of elements from abelian subgroups A of P such that $d(A) = m(P)$. But note that since $J(P) \le Q$, each of these subgroups A is a subgroup of Q as well. Therefore $x \in J(Q)$ and so $J(P) \subseteq J(P)$. We've shown both inclusions so $J(P) = J(Q)$. If $P \leq G$ and $J(P) \leq Q$ where $Q \trianglelefteq G$, then $J(P) = J(Q)$. From part (a) we know that $J(Q)$ char Q, and from Problem 5 we know this means $J(Q) \trianglelefteq G$. But then $J(P) \trianglelefteq G$. □

Problem 9 (4.5.1). *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.*

Proof. Note that $|G| = p^\alpha m$ with $p \nmid m$ and by Lagrange's Theorem, $|H| = p^\beta k$ where $0 \leq \beta \leq \alpha$, $p \nmid k$ and $k \leq m$. Since $P \leq H$ we know $p^\alpha \mid |H|$ and thus $\beta = \alpha$. Therefore $|H| = p^\alpha k$ where $p \nmid k$. Hence $P \in Syl_p(H)$.

As an example, A_4 has the unique Sylow 2-subgroup $\langle (12)(34), (13(24) \rangle$ with order 2^2, but $|S_4| = 2^3 \cdot 3$ and so this is not a Sylow 2-subgroup in S_4. □

Problem 10 (4.5.13). *Prove that a group of order 56 has a normal Sylow p-subgroup for some prime p dividing its order.*

Proof. Note that $56 = 2^3 \cdot 7$ and the Sylow divisibility and congruence rules dictate that either $n_2 = 1$ or $n_2 = 3$ and either $n_7 = 1$ or $n_7 = 8$. Suppose that $n_2 \neq 1$ and $n_7 \neq 1$. Then there are 8 subgroups of G of order 7 and since distinct Sylow p-subgroups intersect only at the identity, there are $8 \cdot 6 = 48$ elements of G with order 7. Similarly, there 3 subgroups of order 8 which means at least $7 + 1 = 8$ distinct elements of order 2, 4 or 8. But $48 + 8 + 1 = 57 > 56$ which is a contradiction. Therefore either $n_2 = 1$ or $n_7 = 1$ which implies the Sylow p-subgroup corresponding to this prime is normal in G. □

Problem 11 (4.5.14). *Prove that a group of order 312 has a normal Sylow p-subgroup for some prime p dividing its order.*

Proof. Note that $312 = 2^3 \cdot 3 \cdot 13$. But from the Sylow divisibility rules $n_{13} = 1 + 13k$ for some k and $n_{13} \mid 24$. This forces $k = 0$ so $n_{13} = 1$ which directly implies G has a Sylow 13-subgroup which is normal in G. □

Problem 12 (4.5.16). *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.*

Proof. First, consider all the elements of order p. There are at least n_p of these, and for each Sylow p-subgroup P there are $(p-1)$ automorphisms of P, that is $(p-1)$ elements of P with order p. Therefore, there are $n_p(p-1)$ elements in G with order p. The same can be said for q and r as well. Since the two sets of elements of order q and order r are disjoint except for the identity, we have

$$n_q(q-1) + n_r(r-1) \leq pqr - 1.$$

Now we can use Sylow divisibility conditions on n_q and n_r. Since $n_q \mid pr$, we have one of $n_q = 1$, $n_q = p$, $n_q = r$ or $n_q = pr$. We also know that $n_q \equiv 1 \pmod q$ so if $n_q \neq 1$, $n_q > q$ and we must have $n_q \geq r$. Likewise, either $n_r = 1$, $n_r = p$, $n_r = q$ or $n_r = pq$. Using the fact that $n_r \equiv 1 \pmod r$, if $n_r \neq 1$ then $n_r > r$ and so $n_r = pq$. Now, assume to the contrary that $n_q \neq 1$ and $n_r \neq 1$. Then we use the fact that p, q and r are primes and q is between p and r. We have

$$\begin{aligned}
n_q(q-1) + n_r(r-1) &\geq r(q-1) + pq(r-1) \\
&= r(q-1) + pqr - pq \\
&= pqr - pq + p(q-1) + (r-p)(q-1) \\
&\geq pqr - pq + p(q-1) + 2(q-1) \\
&> pqr - pq + p(q-1) + p \\
&= pqr - pq + pq \\
&= pqr.
\end{aligned}$$

This contradicts our original statement about n_q and n_r and thus $n_q = 1$ or $n_r = 1$. Therefore either a Sylow q-subgroup or Sylow r-subgroup is one of unique order and is therefore normal in G. □

Problem 13 (4.5.22). *Prove that if $|G| = 132$ then G is not simple.*

Proof. Note that $132 = 2^2 \cdot 3 \cdot 11$. Using the Sylow divisibility rules we know $n_{11} = 1$ or $n_{11} = 12$, $n_3 = 1$, $n_3 = 4$ or $n_3 = 22$ and $n_2 = 1$, $n_2 = 3$, $n_2 = 11$ or $n_2 = 33$. Suppose that $n_{11} \neq 1$. Then $n_{11} = 12$ and since distinct Sylow p-subgroups intersect only in the identity, there are $12 \cdot 10 = 120$ elements of G with order 11. Now suppose that $n_3 \neq 1$. If $n_3 = 22$ then there are $22 \cdot 2 = 44$ elements of order 3. This is a contradiction since $120 + 44 = 164 > 132$. Therefore $n_3 = 4$ which adds $4 \cdot 2 = 8$ elements of order 3. Now suppose that $n_2 \neq 1$ and that $n_2 = 3$. Then there are 3 subgroups of order 4 which adds $3 + 1 = 4$ elements of order 2 or order 4. But now G has at least $120 + 8 + 4 + 1 = 133 > 132$ distinct elements which is a contradiction. A similar contradiction arises if $n_2 = 11$ or $n_2 = 33$. Therefore at least one of n_{11}, n_3 or n_2 must be 1 which implies the existence of a normal Sylow p-subgroup of G. Thus G is not simple. □

Problem 14. *If G is a nonabelian simple group of order < 100, prove that $G \cong A_5$.*

Proof. We proceed by eliminating all possible orders but 60. First eliminate all the prime and prime squared orders. Now eliminate orders of the form pq for primes p and q with $p < q$. Eliminate orders of the form p^2q for $p \neq q$. Also eliminate the order 30 and 56 by Problem 10. This leaves the following possible orders:

8, 16, 24, 27, 32, 36, 40, 42, 48, 54, 60, 64, 66, 70, 72, 78, 80, 81, 84, 88, 90, 96.

Now consider orders of the form $p^\alpha m$ where $m < p$. Since $n_p = 1 + kp$, but $n_p \mid m$, the only possibility for k is $k = 0$. Therefore $n_p = 1$ and these groups are not simple. Using this and Problem 12 we're left with the following possibilities:

24, 36, 40, 48, 60, 72, 80, 84, 90, 96.

In a group of order 40 we find that $n_5 = 1$ and in a group of 84 we find that $n_7 = 1$ by Sylow divisibility conditions. Also in a group of order 80 we have $n_5 = 1$ or $n_5 = 16$ and $n_2 = 1$ or $n_2 = 5$. If this group is to be simple, we need $n_5 = 16$, which gives 64 elements of order 5, and $n_2 = 5$, which gives $16 + 1 = 17$ elements of order other than 5. But this is now 81 distinct elements, a contradiction. This leaves us with the following possible orders:

24, 36, 48, 60, 72, 90, 96.

In a group G of order 24, we find $n_2 = 1$ or 3. Assuming that G is simple, $n_2 = 3$. Now let G act on the Sylow 2-subgroups of G by conjugation. Then this defines a homomorphism $\varphi : G \to S_3$. But since $|G| = 24 > 3! = |S_3|$ we see that φ has a nontrivial kernel and this kernel gives a nontrivial normal subgroup of G. Therefore G is not simple. The same argument holds for a group of order 48 or 96 since in those cases $n_2 = 1$ or $n_2 = 3$ as well. In the case of orders 36 or 72 we find that $n_3 = 1$ or $n_3 = 4$ and a similar argument holds since $|S_4| = 24 < 36 < 72$.

This only leaves the possible orders as 60 or 90. Suppose $|G| = 90$. Then $n_5 = 1$ or $n_5 = 6$ and if G is to be simple, we need $n_5 = 6$. This gives 24 elements of order 5. Furthermore, $n_3 = 1$ or $n_3 = 10$. Suppose $P, Q \in Syl_3(G)$ such that $P \cap Q = R$ with $|R| = 3$. Note here that we're assuming $P \neq Q$, but that P and Q are not disjoint. Lagrange's Theorem ensures $|R| = 3$. Since $|P| = 9 = 3^2$, P is abelian and so $R \trianglelefteq P$. Thus, $P \leq N = N_G(R)$ and the same is true for Q. Thus we know that $|N| = 18$, $|N| = 45$ or $|N| = 90$. In the third case, we must have $R \trianglelefteq G$ and in the second case $|G : N| = 2$ so $N \trianglelefteq G$. In the final case $|G : N| = 5$ and since $90 \nmid 5!$, G cannot be simple. Thus we must have $P \cap Q = 1$ for all Sylow 3-subgroups. This gives $8 \cdot 10 = 80$ elements of order 3 or 9. But then there are $24 + 80$ nonidentity elements of G which is a contradiction. This shows that G is not simple which leaves the only simple nonabelian order less than 100 as 60. □

Problem 15 (4.5.30). *How many elements of order 7 must there be in a simple group of order 168.*

Proof. Let G be such a group. Note that $168 = 2^3 \cdot 3 \cdot 7$. The Sylow divisibility rules dictate that $n_7 = 1$ or $n_7 = 8$. But since G is simple, $n_7 \neq 1$ and so there are 8 subgroups or order 7. Each of pair of these intersects only in the identity and so there are $8 \cdot 6 = 48$ elements of order 7. $\square$

Problem 16 (4.5.31)**.** *For $p = 2$, 3 and 5 find $n_p(A_5)$ and $n_p(S_5)$.*

Proof. From the Sylow divisibility rules on A_5 we know $n_5 = 1$ or $n_5 = 6$, $n_3 = 1$, $n_3 = 4$ or $n_3 = 10$ and $n_2 = 1$, $n_2 = 3$, $n_2 = 5$ or $n_2 = 15$. Note that since A_5 is simple, we can conclude $n_5 = 6$. Also, since $\binom{5}{3} = 10$, there are at least 10 distinct 3-cycles in A_5 each which generate a subgroup of order 3. Therefore $n_3 = 10$. Finally, there are $\binom{5}{4} = 5$ copies of V_4 formed by taking double transpositions on four of the five elements. So $n_5 \geq 5$. But note that each of the elements in these copies of V_4 is distinct since they're formed by taking one element and replacing it with a different element of $\{1, 2, 3, 4, 5\}$. But now we have $4 \cdot 6 + 2 \cdot 10 + 3 \cdot 5 + 1 = 60$ distinct elements. Thus $n_2 = 5$.

From the Sylow divisibility rules on S_5 we know $n_5 = 1$ or $n_5 = 6$, $n_3 = 1$, $n_3 = 4$, $n_3 = 10$ or $n_3 = 40$ and $n_2 = 1$, $n_2 = 3$, $n_2 = 5$ or $n_2 = 15$. Since $A_5 \leq S_5$ we know $n_5 = 6$, $n_3 \geq 5$ and $n_2 \geq 5$. Now note that in addition to the Klein 4-groups in A_5 we also have at least one group of order 4 generated by a four cycle in S_5. Therefore $n_2 = 15$. Finally, note that a group of order 3 must be cyclic, and thus generated by an element of order 3. Since this is necessarily a 3 cycle, all 10 subgroups of order 3 are in A_5 and so $n_3 = 10$. $\square$

Problem 17 (4.5.32)**.** *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*).*

Proof. Note that since $P \trianglelefteq H$ we also know P char H. Then by Problem 5 we know $P \trianglelefteq K$. If $P \in Syl_p(G)$ and $H = N_G(P)$ then $P \trianglelefteq H$ and $H \trianglelefteq N_G(H)$. Therefore $P \trianglelefteq N_G(H)$. But H is the largest subgroup of G which contains P as a normal subgroup and therefore $N_G(H) = H$. $\square$

Problem 18 (4.5.33)**.** *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.*

Proof. Assume that $P \cap H$ is not a Sylow p-subgroup. Then some subgroup $K \leq P \cap H$ has order p^α where α is maximal for H. But then $K \leq gPg^- = P$ since P is normal. But then $K \leq H \cap P$, which is a contradiction. To show uniqueness let $h \in H$ and consider $h(P \cap H)h^{-1} = \{hkh^{-1} \mid k \in P \cap H\} = \{hkh^{-1} \mid k \in P\} \cap \{hkh^{-1} \mid k \in H\} = hPh^{-1} \cap hHh^{-1} = P \cap H$ since $P \trianglelefteq G$. Therefore $P \cap H \trianglelefteq H$ and so $P \cap H$ is the unique Sylow p-subgroup of H. $\square$

Problem 19 (4.5.34)**.** *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).*

Proof. Suppose that $P \cap N$ is not a Sylow p-subgroup of N. Then there exists some $K \leq N$ such that $|K| = p^\alpha$ and α is maximal for N. Then K is a p-subgroup so $K \leq gPg^{-1}$ and $g^{-1}Kg \leq P$. But N is normal so $g^{-1}Kg \leq g^{-1}Ng = N$. Thus $g^{-1}Kg \leq P \cap N$ and since conjugation is an automorphism $|g^{-1}Kg| = p^\alpha$. But this is a contradiction and so $P \cap N$ is a Sylow p subgroup of N.

Let $|G| = p^a m$ and $|N| = p^b k$ Use the formula $|PN/N| = |PN|/|N| = |P||N|/(|P \cap N||N|) = |P|/|P \cap N| = p^a/p^b = p^{a-b}$. But also $|G/N| = |G|/|N| = (m/k)p^{a-b}$ and we're done. $\square$

Problem 20 (4.5.37)**.** *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).

Proof. (a) Let $P \in Syl_p(G)$. We know that since R is a p-subgroup of G, there exists $g \in G$ such that $R \leq gPg^{-1}$. But this is the same as saying $gRg^{-1} \leq P$. Since $R \trianglelefteq G$ we know $R \leq P$ for each $P \in Syl_p(G)$.

(b) Let $g \in G$. Then $gRSg^{-1} = \{gqg^{-1} \mid q \in RS\} = \{grsg^{-1} \mid r \in R, s \in S\} = \{grg^{-1}gsg^{-1} \mid r \in R, s \in S\} = gRg^{-1}gSg^{-1} = RS$ since R and S are normal in G. To see that RS is a p-subgroup let $r \in R$ and $s \in S$. Then $|r| = p^a$ and $|s| = p^b$. But then $|rs| = p^{a+b}$ and we're done. □

Problem 21 (4.5.39)**.** *Show that the subgroup of strictly upper triangular matrices in $GL_n(\mathbb{F}_p)$ is a Sylow p-subgroup of this finite group.*

Proof. We know $|GL_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p) \dots (p^n - p^{n-1})$. Then the smallest power in the expansion will be the product of all the second powers in the binomials, that is $p^{0+1+\dots+n-1} = p^{n(n-1)/2}$. Since this power of p is common to every term in the expansion, but no higher power is, a Sylow p-subgroup of $GL_n(\mathbb{F}_p)$ must have order $p^{n(n-1)/2}$. But then note that in any matrix, there are precisely $n(n-1)/2$ elements above the diagonal. Since there are p choices for each element, this gives the result. □

Problem 22 (4.5.40)**.** *Prove that the number of Sylow p-subgroups of $GL_2(\mathbb{F}_p)$ is $p + 1$.*

Proof. Note that $|GL_2(\mathbb{F}_p)| = (p^2 - 1)(p^2 - p) = p(p+1)(p-1)^2$. Therefore $n_p = 1$, $n_p = p+1$ or $n_p > p+1$. But note that

$$\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$$

has order p and is thus a Sylow p-subgroup of $GL_2(\mathbb{F}_p)$. But in addition

$$\left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle$$

has order p as well. Since these two groups are distinct, we must have $n_p > 1$. Let A be the set of strictly upper triangular matrices (i.e., the first group mentioned above). Then note that any (nonzero) upper triangular matrix will conjugate this group. Since there are p choices for the off diagonal element and $p - 1$ nonzero choices for each diagonal element, we see that $|N_{Gl_2}(A)| = p(p-1)^2$. From Sylow's theorem, this directly shows that $n_p \leq p + 1$ from which we conclude that $n_p = p + 1$. □

Problem 23 (4.5.44)**.** *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 $N_G(P) = C_G(P)$.*

Proof. Suppose that $|G| = p^\alpha m$. We know $N_G(P)/C_G(P)$ is isomorphic to a subgroup of $\mathrm{Aut}(P)$. Also note that $|\mathrm{Aut}(P)| = \varphi(\alpha) = p^{\alpha-1}(p-1)$. Since P is cyclic, $P \leq C_G(P)$ and thus $|N_G(P)/C_G(P)|$ contains no powers of P, as P is a Sylow p-subgroup. Therefore $|N_G(P)/C_G(P)| \mid p - 1$ and since p is the smallest prime dividing the order of G, every divisor of this number is greater than $p - 1$. Therefore $N_G(P)/C_G(P) = 1$ and $N_G(P) = C_G(P)$. □

Problem 24 (4.5.50)**.** *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 $N_P(U) = P$.)*

Proof. We see that if U is conjugate to W in $N_G(P)$ then U is certainly conjugate to W in G. To prove the other direction let $g \in G$ such that $gUg^{-1} = W$. Note that we may assume $g \notin N_G(P)$ since otherwise, we'd be done. Furthermore, since conjugation is an automorphism, $gPg^{-1} = Q$ for some Sylow p-subgroup Q. Also note that $N_Q(gUg^{-1}) = N_Q(W) = Q$ since normality is preserved by automorphisms. Consider $N_G(W)$. This is a subgroup of G and we now know, $N_G(W)$ contains both P and Q. Furthermore, these are Sylow p-subgroups of $N_G(W)$ which means there exists $h \in N_G(W)$ such that $P = hQh^{-1}$. But then $P = (gh)P(gh)^{-1}$ which means $gh \in N_G(P)$. We've chosen $h \in N_G(W)$ so $hWh^{-1} = W$ but then $(gh)U(gh)^{-1} = W$. This concludes the proof. □

Problem 25. *Prove if p is prime and G is any group of order $2p$, then G must have a subgroup of order p, which is normal in G.*

Proof. Since $p \mid |G|$, G has an element of order p. But then $|G : \langle p\rangle| = 2$ and thus $\langle p\rangle \trianglelefteq G$. □

Problem 26. *Suppose G has order pq, where p and q are distinct primes. If G has a normal subgroup of order p and a normal subgroup of order q, prove G is cyclic.*

Proof. Let $P \trianglelefteq G$ and $Q \trianglelefteq G$ with $|P| = p$ and $|Q| = q$. Note that P and Q are cyclic subgroups of G, so let $P = \langle x\rangle$ and $Q = \langle y\rangle$. Now since P and Q are both normal in G, we know PQ is a subgroup and for any two powers of x and y we have $x^i y^j = y^j x^i$. Since all powers of x and y commute, we have $(xy)^{pq} = x^{pq}y^{pq} = 1$. Suppose there exists some integer $a < pq$ such that $(xy)^a = 1$. Then $x^a y^a = 1$. Note that since $(xy)^{pq} = 1$, we must have $a \mid pq$. Therefore $a = p$ or $a = q$. But since p and q are distinct, at least one of x^a or y^a will not be the identity. Therefore $|xy| = pq$ and G is cyclic. □

Problem 27. *Suppose p and q are distinct primes and q divides $(p1)$. Show there exists a non-abelian group of order pq and any two such non-abelian groups are isomorphic.*

Proof. Consider $Z_p = \langle x\rangle$ and $Z_q = \langle y\rangle$. We wish to define a relation $yxy^{-1} = x^c$ which will force our group to have order 21. To do this, note that if we apply the conjugation $yxy^{-1} = x^c$ q times we arrive at $y^q x y^{-q} = x^{c^q}$. Since $|y| = q$, we want to find c such that $c^q \equiv 1 \pmod p$. We know that $qk = p-1$ for some k and $\mathrm{Aut}(Z_p) \cong (\mathbb{Z}/p\mathbb{Z})^\times$. This shows the automorphism of Z_p which takes a generator x to x^k will have order q. So now define $yxy^{-1} = x^k$ for a generator y of Z_q. Let $G = \langle x, y \mid x^p = y^q = 1, yxy^{-1} = x^k\rangle$. This group has order pq by construction.

Furthermore, we know that we must have the rule $yxy^{-1} = x^c$ for some c. There may be more than one choice for c. Namely, any c for which $p \mid c^q - 1$ will work. But for any two of these groups the order of these automorphisms in Z_p is always q. We can use the fact that $\mathrm{Aut}(Z_p)$ is cyclic to conclude that the two groups must be isomorphic. □