200A Homework 3

James Harbour

October 6, 2025

Problem 1

Suppose $p < q < \ell$ are three primes, G is a group, and $|G| = pq\ell$. Prove that G has a normal Sylow ℓ-subgroup.

Lemma 0.0.1. *Suppose $p < q$ are primes and G is a group of order pq. Further assume $q > 3$. Then G has a normal Sylow q-subgroup.*

Proof of Lemma. Sylow's theorems give the restrictions $n_p \in \{1, q\}$ and $n_q \in \{1, p\}$. As $n_q \equiv 1 \pmod{q}$, $q \mid (n_q - 1)$, whence the inequality $p < q$ forces $n_q = 1$. Thus G has a normal Sylow q-subgroup. $\square$

Proof of Problem 1. Note first that $\ell > 3$. Sylow's theorems give the following restrictions

$$\begin{aligned} n_p &\in \{1, q, \ell, q\ell\}, \quad n_p \equiv 1 \pmod{p} \\ n_q &\in \{1, p, \ell, p\ell\}, \quad n_q \equiv 1 \pmod{q} \\ n_\ell &\in \{1, p, q, pq\}, \quad n_\ell \equiv 1 \pmod{\ell} \end{aligned}$$

The congruence $\ell \mid (n_\ell - 1)$ forces $n_\ell \neq p, q$. The congruence $q \mid (n_q - 1)$ forces $n_q \neq p$. This gives the further restrictions

$$\begin{aligned} n_p &\in \{1, q, \ell, q\ell\} \\ n_q &\in \{1, \ell, p\ell\} \\ n_\ell &\in \{1, pq\} \end{aligned}$$

Let $r \in \{p, q, \ell\}$. Suppose that $R_1, R_2 \in \mathrm{Syl}_r(G)$. If $R_1 \cap R_2 > 1$, then $R_1 \cap R_2$ would itself be a Sylow r-subgroup of G whence $R_2 = R_1 \cap R_2 = R_1$. Thus Sylow r-subgroups are either equal or have trivial intersection. Hence by element counting, choices of n_p, n_q, n_ℓ yield the following lower bound

$$pql = |G| \geq 1 + n_p(p-1) + n_q(q-1) + n_\ell(\ell - 1).$$

Suppose, for the sake of contradiction, that $n_p, n_q, n_l \neq 1$. Then $n_p \geq q$, $n_q \geq \ell$, and $n_\ell = pq$, so the above bound gives

$$\begin{aligned} pql &\geq 1 + q(p-1) + \ell(q-1) + pq(\ell - 1) = 1 - q + q\ell - \ell + pq\ell \\ \Longrightarrow 0 &\geq q(\ell - 1) - 1(\ell - 1) = (q-1)(\ell - 1) \end{aligned}$$

which is absurd. Thus, at least one of n_p, n_q, or n_ℓ is equal to 1. If $n_\ell = 1$, then we are done as this implies that the unique Sylow ℓ-subgroup is normal in G. Thus, suppose $n_\ell \neq 1$, whence $n_\ell = pq$. Then $n_p = 1$ or $n_q = 1$.

Suppose, without loss of generality (the other case is entirely analagous), that $n_p = 1$, and let $P \in \mathrm{Syl}_p(G)$, so $P \triangleleft G$. Set $\overline{G} := G/P$, so $|\overline{G}| = q\ell$. By the previous lemma, $\overline{G}$ has a normal Sylow ℓ-subgroup $\widetilde{N} \triangleleft \overline{G}$. By the isomorphism theorems, there exists a normal subgroup $N \triangleleft G$ with $P \subseteq N$ such that $N/P \cong \widetilde{N}$. Then $|N| = |P| \cdot |\widetilde{N}| = p\ell$, so by applying the above lemma again, we obtain a Sylow ℓ-subgroup K of N with $K \triangleleft N$. Note that then $|\mathrm{Syl}_\ell(N)| = 1$
We claim that $K \triangleleft G$. To see this, fix $g \in G$. Note that as $N \triangleleft G$, we have $gKg^{-1} \subseteq gNg^{-1} = N$. However gKg^{-1} is then also a Sylow ℓ-subgroup of N, whence uniquness gives $gKg^{-1} = K$. Thus $K \triangleleft G$ and $|K| = \ell$, so K is a normal Sylow ℓ-subgroup of G.

□

Problem 2

Suppose G is a finite group, N is a normal subgroup of G, and $P \in \mathrm{Syl}_p(N)$. Prove that $G = N_G(P)N$.

Proof. Fix $g \in G$ and observe that $gPg^{-1} \subseteq gNg^{-1} = N$. Noting that conjugation does not change the size of the group, it follows that $gPg^{-1} \in \mathrm{Syl}_p(N)$. Then, for $g \in G$, as gPg^{-1} and P are both Sylow p-subgroups of N, by the Sylow theorems they are conjugate in N, i.e. there is some $n \in N$ such that

$$gPg^{-1} = n^{-1}Pn \implies g^{-1}n^{-1}Png = P$$

So $g^{-1}n^{-1} \in N_G(P)$, whence $g^{-1} \in N_G(P)n \subseteq N_G(P)N$. As $g \in G$ was arbitrary, it follows that $G = N_G(P)N$. □

Problem 3

Suppose G is a finite group and H is a subgroup. Suppose for all $x \in H \setminus \{1\}$, $C_G(x) \subseteq H$. Prove that $\gcd(|H|, [G : H]) = 1$.
Hint. Suppose p is a prime which divides $\gcd(|H|, [G : H])$. Suppose $Q \in \mathrm{Syl}_p(H)$. Argue that there exists $P \in \mathrm{Syl}_p(G)$ such that $Q \subseteq P$. Argue that there exists $y \in Z(Q) \setminus \{1\}$. Considering $C_G(y)$, show that $Z(P) \subseteq Q$. Suppose $x \in Z(P) \setminus \{1\}$, consider $C_G(x)$ to obtain that $P \subseteq H$. Argue why this is a contradiction.

Proof. Suppose, for the sake of contradiction, that there is some prime p which divides $\gcd(|H|, [G : H])$. Let $Q \in \mathrm{Syl}_p(H)$. As Q is a p-subgroup of G, there is some $P \in \mathrm{Syl}_p(G)$ such that $Q \subseteq P$. Moreover, Q being a p-group implies that $Z(P) > 1$, so there is some $y \in Z(Q) \setminus \{1\}$. By assumption, $C_G(y) \subseteq H$

Take $x \in Z(P)$. Then $xy = yx$, so $x \in C_G(y) \subseteq H$, whence $Z(P) \subseteq C_G(y) \subseteq H$.
As P is a p-group, we again have $Z(P) > 1$, so let $x \in Z(P) \setminus \{1\}$. Then for $z \in P$, we have that $xz = zx$, whence $z \in C_G(x) \subseteq H$ and thus $P \subseteq H$.

Writing $|G| = p^k a$ with $p \not| a$, by assumption we have that $p \mid [G : H]$. But then $[G : H] \mid [G : P] = a$, whence $p \mid a$, which is a contradiction. □

Problem 4

Suppose G is a finite group, N is a normal subgroup, and p is a prime factor of $|N|$.

(a): Suppose $P \in \mathrm{Syl}_p(G)$ and $Q \in \mathrm{Syl}_p(N)$. Prove that there exists $g \in G$ such that $Q = gPg^{-1} \cap N$.

Proof. As $P \cap N$ is a p-subgroup of N, Sylow's conjugation theorem implies that there is some $g \in N$ such that $gPg^{-1} \cap N = g(P \cap N)g^{-1} \subseteq Q$. Noting now that Q is a p-subgroup of N, there is some $x \in G$ such that $xQx^{-1} \subseteq P$ whence $Q \subseteq x^{-1}Px$. As $Q \subseteq N$, it follows by normality of N that $Q \subseteq x^{-1}Px \cap N = x^{-1}(P \cap N)x$. Now, we observe

$$|P \cap N| = |gPg^{-1} \cap N| \leq |Q| \leq |x^{-1}Px \cap N| = |x^{-1}(P \cap N)x| = |P \cap N|,$$

whence $|Q| = |P \cap N| = |gPg^{-1} \cap N|$, so $Q = gPg^{-1} \cap N$. $\square$

(b): Prove that the following is a well-defined surjective function

$$\Phi : \mathrm{Syl}_p(G) \to \mathrm{Syl}_p(N), \qquad \Phi(P) := P \cap N.$$

Proof. Fix $P \in \mathrm{Syl}_p(G)$. Then $P \cap N$ is a p-subgroup of N so there is some $Q \in \mathrm{Syl}_p(N)$ such that $P \cap N \subseteq Q$. Now by part (a), there is some $g \in G$ such that $gPg^{-1} \cap N = Q$. But $P \cap N \subseteq Q$ and $|Q| = |gPg^{-1} \cap N| = |P \cap N|$, so $P \cap N = Q$. Thus $\Phi(P) = P \cap N \in \mathrm{Syl}_p(N)$, so Φ is well-defined.

Now suppose $Q \in \mathrm{Syl}_p(N)$. Then by the Sylow theorems, as Q is a p-subgroup of G, there is some $P \in \mathrm{Syl}_p(G)$ such that $Q \subseteq P$. Then $Q \subseteq P \cap N = \Phi(P) \in \mathrm{Syl}_p(N)$, whence by size considerations it follows that $Q = P \cap N$. Thus Φ is a surjective function. $\square$

(c): For $P \in \mathrm{Syl}_p(G)$, prove that $N_G(P) \subseteq N_G(\Phi(P))$ and

$$|\Phi^{-1}(\Phi(P))| = [N_G(\Phi(P)) : N_G(P)].$$

Proof. Suppose that $gPg^{-1} = P$. Then

$$g\Phi(P)g^{-1} = g(P \cap N)g^{-1} = gPg^{-1} \cap N = P \cap N = \Phi(P),$$

whence $N_G(P) \subseteq N_G(\Phi(P))$.

Fix $P \in \mathrm{Syl}_p(G)$.
Define a map $F : N_G(\Phi(P))/N_G(P) \to \Phi^{-1}(\Phi(P))$ by $F(gN_G(P)) := gPg^{-1}$. We claim that this a well-defined bijection.

If $g \in N_G(\Phi(P))$, then $gPg^{-1} \cap N = g(P \cap N)g^{-1} = P \cap N$, so $gPg^{-1} \in \Phi^{-1}(\Phi(P))$. Moreover, suppose that $g, h \in N_G(\Phi(P))$ and there is some $x \in N_G(P)$ such that $g = hx$. Then by definition of $N_G(P)$,

$$gPg^{-1} = hxPx^{-1}h^{-1} = hPh^{-1}.$$

Thus F is a well-defined function on $N_G(\Phi(P))/N_G(P)$.

To see that F is injective, suppose that $g, h \in N_G(\Phi(P))$ are such that $F(gN_G(P)) = F(hN_G(P))$. Then

$$gPg^{-1} = hPh^{-1} \implies h^{-1}gPg^{-1}h = P \implies h^{-1}g \in N_G(P)$$

whence $gN_G(P) = hN_G(P)$.

To see that F is surjective, suppose that $\widetilde{P} \in \Phi^{-1}(\Phi(P))$. Then by definition $\widetilde{P} \cap N = P \cap N$. Applying Sylow's conjugation theorem, there is some $g \in G$ such that $\widetilde{P} = gPg^{-1}$. Then we observe that

$$g(P \cap N)g^{-1} = gPg^{-1} \cap N = \widetilde{P} \cap N = P \cap N,$$

so $g \in N_G(\Phi(P))$, whence $F(gN_G(P)) = gPg^{-1} = \widetilde{P}$.

Thus F is a bijection, so $[N_G(\Phi(P)) : N_G(P)] = |\Phi^{-1}(\Phi(P))|$. $\square$

(d): Prove that $|\mathrm{Syl}_p(N)|$ divides $|\mathrm{Syl}_p(G)|$.

Proof. For $g \in G$ and $P \in \mathrm{Syl}_p(G)$, observe that

$$\Phi(gPg^{-1}) = gPg^{-1} \cap N = g(P \cap N)g^{-1} = g\Phi(P)g^{-1}.$$

Note that if $K \subseteq G$ is a subgroup and $x \in G$, then $N_G(xKx^{-1}) = xN_G(K)x^{-1}$. Fix $P, P_0 \in \mathrm{Syl}_p(G)$ and choose $x \in G$ such that $xPx^{-1} = P_0$. Then we compute,

$$\begin{aligned}
[N_G(\Phi(P_0)) : N_G(P_0)] &= [N_G(\Phi(xPx^{-1})) : N_G(xPx^{-1})] \\
&= [N_G(x\Phi(P)x^{-1}) : xN_G(P)x^{-1}] \\
&= [xN_G(\Phi(P))x^{-1} : xN_G(P)x^{-1}] \\
&= \frac{|xN_G(\Phi(P))x^{-1}|}{|xN_G(P)x^{-1}|} = \frac{|N_G(\Phi(P))|}{|N_G(P)|} = [N_G(\Phi(P)) : N_G(P)].
\end{aligned}$$

We have thus shown that the index in question is independent of the choice of Sylow p-subgroup $P \in \mathrm{Syl}_p(G)$. Fix $P \in \mathrm{Syl}_p(G)$. Write $\mathrm{Syl}_p(N) := \{Q_1, \ldots, Q_s\}$ and choose $P_1, \ldots, P_s \in \mathrm{Syl}_p(G)$ such that $Q_j = \Phi(P_j)$ for all $1 \le j \le s$. Then

$$\mathrm{Syl}_p(G) = \bigsqcup_{j=1}^{s} \Phi^{-1}(Q_j) = \bigsqcup_{j=1}^{s} \Phi^{-1}(\Phi(P_j)).$$

Now we compute,

$$\begin{aligned}
|\mathrm{Syl}_p(G)| = \left| \bigsqcup_{j=1}^{s} \Phi^{-1}(\Phi(P_j)) \right| &= \sum_{j=1}^{s} |\Phi^{-1}(\Phi(P_j))| \\
&= \sum_{j=1}^{s} [N_G(\Phi(P_j)) : N_G(P_j)] = s \cdot [N_G(\Phi(P)) : N_G(P)],
\end{aligned}$$

which shows that $|\mathrm{Syl}_p(N)| = s$ divides $|\mathrm{Syl}_p(G)|$ as desired. □

Problem 5

Suppose p is an odd prime and G is a group of order $p(p+1)$ which does not have a normal subgroup of order p. Prove that p is a Mersenne prime; that is, $p = 2^n - 1$ for some positive integer n.

Proof. As G does not have a normal subgroup of order p, it follows that $n_p(G) = p + 1$. Let $\mathrm{Syl}_p(G) = \{P_1, \ldots, P_{p+1}\}$. Then as each P_i is cyclic of order p, they intersect trivially, whence

$$S := \bigcup_{i=1}^{p+1} P_i \setminus \{1\}$$

has size $(p+1)(p-1) = p^2 - 1$. Let $H := G \setminus S$, whence $|H| = p+1$. In the lecture notes we have shown that $g \in G \setminus H \implies o(g) = p$. We have also shown that H is a subgroup where $H \setminus \{1\} = Cl(h)$ for any $h \in H \setminus \{1\}$.

Let q be a prime dividing $p+1$. As p is an odd prime, $q \neq p$. By Cauchy's theorem there is some $x \in G$ such that $o(x) = q$. Hence, $o(x) \neq p$, so $x \notin G \setminus H$. Equivalently, this implies that $x \in H$. As $x \neq 1$, $x \in H \setminus \{1\}$, whence $H \setminus \{1\} = Cl(x)$. Thus every element of $H \setminus \{1\}$ has order $o(x) = q$, whence H is a q-group.

As H is a finite q-group, there is some $m \geq 1$ such that $|H| = q^m$. But $|H| = p+1$, so $p+1 = q^m$. Suppose first that $m = 1$. Then $q = p+1$ is prime and p is prime, whence $p = 2$ which contradicts that p is an odd prime. Thus $m \geq 2$, so we may write

$$p = q^m - 1 = (q-1)(q^{m-1} + q^{m-2} + \cdots + q + 1)$$

whence p being prime forces $q - 1 = 1 \implies q = 2$. In conclusion, $p = 2^m - 1$ is a Mersenne prime. □

Problem 6

Suppose p and q are prime numbers and G is a group of order $p^2 q$. Prove that G is not simple.

Proof. Sylow's theorems give the following initial restrictions on n_p,n_q.

$$\begin{aligned} n_p &\in \{1, q\}, \quad n_p \equiv 1 \pmod{p} \\ n_q &\in \{1, p, p^2\}, \quad n_q \equiv 1 \pmod{q} \end{aligned}$$

If $n_q = 1$, then we are done, so assume $n_q \neq 1$. If $p = q$, then Sylow's theorems force $n_q = n_p = 1$, so it must hold that $p \neq q$. Suppose first that $n_q = p$. Then as $q \mid (p-1)$, it follows that $q < p$. Thus the restriction $p \mid (n_p - 1)$ forces $n_p = 1$, whence G has a normal Sylow p-subgroup.

Now suppose that $n_q = p^2$. Note that nonequal Sylow q-subgroups must intersect trivially, so we may count the set

$$S := \bigsqcup_{Q \in \mathrm{Syl}_q(G)} Q \setminus \{1\} \implies |S| = n_q(q-1) = p^2 q - p^2.$$

Every element in S has order q. The remaining room inside of G, namely $G \setminus S$, has size p^2. Let $P \in \mathrm{Syl}_p(G)$. We claim that $P \subseteq G \setminus S$. Suppose $g \in P$. Then by Lagrange, $o(g) \in \{1, p, p^2\}$, whence $o(g) \neq q$ so $g \notin S$. Thus $P \subseteq G \setminus S$, whence $|P| = p^2 = |G \setminus S|$ implies that $P = G \setminus S$. Hence $n_p = 1$, so G has a normal Sylow p-subgroup. □

Problem 7

A subgroup K of G is called a *characteristic subgroup* if for all $\theta \in \mathrm{Aut}(G)$, $\theta(K) = K$. Notice that every characteristic subgroup is normal.
(a): Suppose N is a normal subgroup of G and K is a characteristic subgroup of N. Prove that K is a normal subgroup of G.

Proof. Let $g \in G$. Consider the inner automorphism $\sigma_g \in Aut(G)$ given by $\sigma_g(x) = gxg^{-1}$. As $N \lhd G$, we have that $\sigma_g(N) = gNg^{-1} = N$, whence $\sigma_g|_N \in \mathrm{Aut}(N)$. As K is characteristic in N, it follows that $K = \sigma_g|_N(K) = gKg^{-1}$, so K is a normal subgroup of G. □

(b): We say a group H is *characteristically simple* if the only characteristic subgroups of H are $\{1\}$ and H. Suppose N is a minimal normal subgroup of G; that is, if $M \leq N$ and $M \trianglelefteq G$, then either $M = \{1\}$ or $M = N$. Then N is characteristically simple.

Proof. Suppose, for the sake of contradiction, that N is not characteristically simple. Then there is some subgroup $K \subseteq N$ with $K \neq 1, N$ such that K is characteristic in N. As N is normal in G, part (a) implies that $K \lhd G$, contradicting the minimality of N. □

Problem 8

Suppose G is a finite group.
(a): Prove that a normal Sylow p-subgroup is a characteristic subgroup.

Proof. Let N be a normal Sylow p-subgroup of G, so $|\operatorname{Syl}_p(G)| = 1$. Fix $\theta \in \operatorname{Aut}(G)$. Then $|\theta(N)| = |N|$, whence $\theta(N)$ is also a Sylow p-subgroup of G. Now, as $|\operatorname{Syl}_p(G)| = 1$, it follows that $\theta(N) = N$. $\square$

(b): Suppose H is a normal subgroup of G and $\gcd(|H|, [G : H]) = 1$. Prove that H is a characteristic subgroup.

Proof. Suppose, for the sake of contradiction, that there is some $\theta \in \operatorname{Aut}(G)$ such that $\theta(H) \neq H$. As G is a finite group, it follows that $\theta(H) \cap H < H$.

On one hand, observe that

$$\left|\frac{\theta(H)H}{H}\right| \cdot [G : \theta(H)H] = [G : H],$$

so $\left|\frac{\theta(H)H}{H}\right|$ divides $[G : H]$.
On the other hand, by the diamond isomorphism theorem we have

$$\left|\frac{\theta(H)H}{H}\right| = \frac{|\theta(H)|}{|\theta(H) \cap H|} = \frac{|H|}{|\theta(H) \cap H|},$$

which divides $|H|$. Thus by assumption we have that $|\theta(H)H/H| = 1$, whence $H = \theta(H)H$. This implies that $\theta(H) \subseteq H$, but θ is an automorphism so it preserves size, whence $\theta(H) = H$ which is a contradiction. $\square$