Problem Set 8
Due Thursday, October 30

Instructions: You are encouraged to work together on these problems, but each student should hand in their own final draft, written in a way that indicates their individual understanding of the solutions. Never submit something for grading that you do not completely understand. You cannot use any resources besides me, your classmates, and our course notes.

I will post the .tex code for these very spooky problems for you to use if you wish to type your homework. If you prefer not to type, please *write neatly.* As a matter of good proof writing style, please use complete sentences and correct grammar. You may use any result stated or proven in class or in a homework problem, provided you reference it appropriately by either stating the result or stating its name (e.g. the definition of ring or Lagrange's Theorem). Please do not refer to theorems by their number in the course notes, as that can change.

Problem 1. Prove that the converse to Lagrange's theorem is false: find a group G and a positive integer d such that d divides the order of G but G does not have any subgroups of order d.

Proof. Consider $G = A_5$, which has order

$$|A_5| = \frac{|S_5|}{2} = \frac{120}{2} = 60.$$

Let $d = 30$, which divides $|A_5|$. If A_5 had a subgroup H with $|H| = 30$, then

$$[A_5 : H] = \frac{60}{30} = 2,$$

so H must be normal in A_5. But we have shown in class that A_5 is simple, so this is a contradiction. We conclude that A_5 has no subgroup of order 30 despite the fact that 30 divides the order of A_5. (Note that there are many possible answers, and this is just one that is easier to justify than some others.) $\square$

Problem 2. Show that there are no simple groups of order 56.

Proof. Let G be a group of order 56. Let $n_7 = |\mathrm{Syl}_7(G)|$. By Sylow theory,

$$n_7 \equiv 1 \pmod{7} \quad \text{and} \quad n_7 \mid 8,$$

so $n_7 \in \{1, 8\}$. Note that if $n_7 = 1$, then the unique subgroup of order 7 would be normal, and G would not be simple. So suppose that $n_7 = 8$.

Given any two Sylow 7-subgroups P and Q, which have order 7, the order of their intersection $P \cap Q$ must divide 7, but it cannot be 7 unless $P = Q$. Thus any two Sylow 7-subgroups have trivial intersection. Moreover, any element in such a subgroup that is not the identity must have order 7. Counting these, we get

$$8(7 - 1) = 48$$

elements of order 7, so that there are at most $56 - 48 = 8$ elements in G that do not have order 7.

Now consider any Sylow 2-subgroup Q of G, which has order 8. By Lagrange, the order of any element in Q must divide 8, so in particular Q has no elements of order 7. But there are only 8 elements in G that may have order other than 7, so they must form the unique subgroup of order 8. In particular, that subgroup must be normal, and G is not simple. $\square$

Problem 3. Show that there are no simple groups of order $2^5 \cdot 7^3$.

Proof. Let $n_2 = |\mathrm{Syl}_2(G)|$ and $n_7 = |\mathrm{Syl}_7(G)|$. If $n_2 = 1$ or $n_7 = 1$, the unique Sylow subgroup corresponding to that prime is normal, and thus G is not simple. So let's assume $n_1 \neq 1$ and $n_7 \neq 1$.

The Main Theorem of Sylow theory gives us

$$n_7 \mid 2^5 \quad \text{and} \quad n_7 \equiv 1 \pmod{7} \quad \Longrightarrow \quad n_7 \in \{1, 8\} \Longrightarrow n_7 = 8.$$

Let's consider the action of G by conjugation on the set of its Sylow 7-subgroups $\mathrm{Syl}_7(G)$. This gives us a group homomorphism (the corresponding permutation representation)

$$\rho \colon G \to \mathrm{Perm}(\mathrm{Syl}_7(G)) = S_8.$$

By the First Isomorphism Theorem,

$$G/\ker(\rho) \cong \mathrm{im}(\rho).$$

Since $\mathrm{im}(\rho)$ is a subgroup of $\mathrm{Perm}(\mathrm{Syl}_7(G))$, then Lagrange's Theorem guarantees that $|\mathrm{im}(\rho)|$ must divide $|\mathrm{Perm}(\mathrm{Syl}_7(G))| = 8!$. Since

$$|\mathrm{im}(\rho)| = |G/\ker(\rho)| = \frac{|G|}{|\ker(\rho)|} = \frac{2^5 \cdot 7^3}{|\ker(\rho)|},$$

we conclude that

$$\frac{2^5 \cdot 7^3}{|\ker(\rho)|} \text{ divides } 8!.$$

Note that while 7 divides $8!$, 7^2 does not, and thus 7^2 must divide $|\ker(\rho)|$. In particular, $\ker(\rho)$ is nontrivial. Moreover, the Main Theorem of Sylow Theory says that the action of G by conjugation on $\mathrm{Syl}_7(G)$ is transitive, so ρ must be nontrivial, and $\ker(\rho) \neq G$. But $\ker(\rho)$ is a normal subgroup of G, and we just proved it is neither $\{e\}$ nor G, so it is a proper nontrivial normal subgroup of G. This shows that G is not simple. $\square$

Problem 4. Let G be a finite group of order pqr with $0 < p \leq q \leq r$ prime numbers[1]. Show that G is not simple.

Proof. Throughout, n_p, n_q, n_r denote $\#\mathrm{Syl}_p(G), \#\mathrm{Syl}_q(G), \#\mathrm{Syl}_r(G)$.

Case (1): $p < q < r$. If any of n_p, n_q, n_r is 1 then G is not simple. Otherwise, Sylow theory gives that $n_p \geq q$, $n_q \geq r$ and $n_r \geq pq$. Since the Sylow p-subgroups, q-subgroups and r-subgroups, respectively, intersect trivially by Lagrange's theorem, this leads to at least $q(p-1)$ elements of order p, $r(q-1)$ elements of order q, and $pq(r-1)$ elements of order r, for a total of at least

$$q(p-1) + r(q-1) + pq(r-1) = pq - q + rq - r + pqr - pq = rq - r - q + pqr$$

---

[1]You should consider four cases:

1. $p < q < r$
2. $p = q < r$
3. $p < q = r$
4. $p = q = r$.

elements. Since $r > q > 2$, we have $rq - r - q > 2r - r - q > 0$, yieldly strictly more elements than $|G|$, which is impossible.

Case (2): $p = q < r$. Sylow Theory gives $n_r \in \{1, p^2\}$. If $n_r = 1$, then the unique Sylow r-subgroup would be a proper, non-trivial normal subgroup and thus G would not simple. So, assume $n_r = p^2$. Since the Sylow r-subgroups have prime order, then intersect pairwise at just $\{e\}$. It follows that G would have $(r - 1)p^2 = |G| - p^2$ elements of order r. Thus, any Sylow p-subgroup would have to coincide with the remaining p^2 elements. That is, there can be just one Sylow p-subgroup, and hence it is normal (and proper and non-trivial).

Case (3): $p < q = r$. Sylow Theory gives that $n_q \mid p$ and $n_q \equiv 1 \pmod{q}$, and hence , since $q > p$, we must have $n_q = 1$. Thus, the Sylow q-subgroup is a non-trivial, proper, normal subgroups of G

Case (4): $p = q = r$. Then G is a p-group and, as we proved in class, G admits a chain of subgroups $\{e\} = G_0 \leq G_1 \leq G_2 \leq G_3$ with each $G_i \trianglelefteq G$ and $|G_i| = p^i$. In particular, G is not simple.

$\square$