Problem Set 8
solutions

Problem 1. Show that there are no simple groups of order $56 = 8 \cdot 7$.

Proof. Let G be a group of order 56. Let $n_7 = |\operatorname{Syl}_7(G)|$. 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. □

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

Proof. Let $n_2 = |\operatorname{Syl}_2(G)|$ and $n_7 = |\operatorname{Syl}_7(G)|$. 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

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

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

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

By the First Isomorphism Theorem,

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

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

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

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 $\operatorname{Syl}_7(G)$ 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. □

Problem 3. Let G be a finite group of order pqr with $0 < p < q < r$ prime numbers. Show that G is not simple.

Proof. Let

$$n_p = |\operatorname{Syl}_p(G)|, \quad n_q = |\operatorname{Syl}_q(G)|, \quad n_r = |\operatorname{Syl}_r(G)|.$$

If any of n_p, n_q, or n_r is 1, then the unique Sylow subgroup corresponding to that prime is normal, and G is not simple.

So suppose that $n_p, n_q, n_r \neq 1$. By the Main Theorem of Sylow Theory,

$$n_p \mid qr,$$

and since $1 < q < r < qr$ are the only divisors of qr, we conclude that $n_p \geqslant q$. Moreover, $n_q \equiv 1 \pmod{q}$, and since $n_q \neq 1$, we conclude that $n_q \geqslant q + 1$. But we also have

$$n_q \mid pr,$$

and $1 < p < r < pr$ are the only divisors of pr. Since $p < q$, we conclude that $n_q \geqslant r$. Finally,

$$n_r \equiv 1 \pmod{r}, n_r \neq 1 \implies n_r \geqslant r + 1,$$

while

$$n_r \mid pq \implies n_r \in \{p, q, pq\}.$$

But $p, q < r$, so $n_r = pq$.

By Lagrange's Theorem, for any distinct $a, b \in \{p, q, r\}$, any Sylow a-subgroup and any Sylow b-subgroup intersect trivially. Moreover, since a is prime, any two Sylow a-subgroups, which have order a, must intersect trivially. Thus each Sylow a-subgroup contains $a-1$ nonidentity elements that are not in any other subgroup.

Counting all these distinct elements gives us

$$\begin{aligned} 1 + (p-1)n_p + (q-1)n_q + (r-1)n_r &\geqslant 1 + (p-1)q + (q-1)r + (r-1)pq \\ &= 1 + pqr + rq - r - q. \end{aligned}$$

Since $r > q > 2$, then

$$rq - r - q > 2r - r - q > 0,$$

and thus we have found strictly more elements than $|G|$, which is impossible. □

Problem 4. Prove that S_4 has precisely three distinct subgroups of order 8, all of which are isomorphic to D_4.

Proof. First, note that $|S_4| = 4! = 2^3 \cdot 3$. Thus any subgroup of S_4 of order 8 is a Sylow 2-subgroup; let n_2 be the number of Sylow 2-subgroups. By Sylow Theory,

$$n_2 \equiv 1 \pmod{2} \quad \text{and} \quad n_2 \mid 3.$$

Thus $n_2 \in \{1, 3\}$.

Any transposition or 4-cycle generates a subgroup of S_4 of order 2 or 4, which are powers of 2, so by the Main Theorem of Sylow Theory they must each be subgroups of some Sylow 2-subgroup. But we counted in class that there are six 2-cycles and six 4-cycles, and $6 + 6 > 8$, so they cannot all be in the same Sylow 2-subgroup. Thus $n_2 = 3$, meaning that there are precisely 3 distinct subgroups of order 8.

By the Main Theorem of Sylow Theory, all of the Sylow 2-subgroups are conjugate. Given one such group H and $g \in S_4$, the function $H \to gHg^{-1}$ given by $h \mapsto ghg^{-1}$ is a group isomorphism, so any two Sylow 2-subgroups are isomorphic. Hence, we just need to show that S_4 contains a subgroup isomorphic to D_8.

Let X be the set of left cosets of the subgroup $S = \{1, s\}$ of D_4. Note that

$$|X| = [D_4 : S] = \frac{8}{2} = 4.$$

Let G act on X by left multiplication. Note that since $|X| = 4$, $\operatorname{Perm}(X) \cong S_4$. This action induces a homomorphism $\phi\colon G \to S_4$. Moreover, we proved in class that

$$\ker(\rho) = \bigcap_{g \in D_4} gSg^{-1}.$$

This is the largest normal subgroup of G contained in S. But S is not normal, so $\ker(\rho) \neq S$, leaving $\ker(\rho) = \{e\}$ as the only possibility. Thus ϕ is injective and the image of ϕ is a subgroup of S_4 isomorphic to D_8. □

Problem 5. Let C_n denote the cyclic group of order $n \geqslant 2$, and consider the group

$$(\mathbb{Z}/n)^\times = \{[j]_n \mid \gcd(j, n) = 1\}$$

with the binary operation given by the usual multiplication. Prove that

$$\operatorname{Aut}(C_n) \cong (\mathbb{Z}/n)^\times.$$

Proof. Let $C_n = \langle x \mid x^n = e \rangle$. By the Universal Mapping Property for cyclic groups, each group homomorphism $C_n \to C_n$ is uniquely determined by the image of x. The possible images for x are the n elements in C_n, which are $x^i \in C_n$ for $0 \leqslant i < n$. Let $\rho_i\colon C_n \to C_n$ be the unique homomorphism determined by $\rho_i(x) = x^i$. We have for now shown that

$$\operatorname{Aut}(C_n) = \{\rho_i \mid 0 \leqslant i < n\}.$$

Note that $\operatorname{im}(\rho_i) = \langle x^i \rangle$, and we proved in class that $\langle x^i \rangle = C_n$ if and only if $\gcd(i, n) = 1$. Note moreover that if ρ_i is surjective, then it must also be injective, given that it is a function between two finite sets of the same order. Thus

$$\rho_i \in \operatorname{Aut}(C_n) \quad \text{if and only if} \quad [i]_n \in (\mathbb{Z}/n)^\times.$$

Now consider $\varphi\colon \operatorname{Aut}(C_n) \to (\mathrm{Z}/n)^\times$ given by

$$\varphi(\rho_i) = [i]_n.$$

Note that

$$(\rho_i \circ \rho_j)(x) = x^{ij} = \rho_{ij \pmod m}(x).$$

The uniqueness part of the UMP for cyclic groups implies that

$$\rho_i \circ \rho_j = \rho_{ij \pmod m}.$$

Hence,

$$\varphi(\rho_i \circ \rho_j) = \varphi\left(\rho_{ij \pmod m}\right) = [ij]_n = [i]_n[j]_n = \varphi(\rho_i)\varphi(\rho_j).$$

Thus φ is a group homomorphism.

Given $[j]_n \in (\mathbb{Z}/n)^\times$, by the UMP for cyclic groups there exists a unique homomorphism

$$\psi([j]_n) \colon C_n \to C_n$$

that takes $x \mapsto x^j$. This gives us a map $\psi\colon (\mathbb{Z}/n)^\times \to \operatorname{Aut}(C_n)$. We need to show that ψ is well-defined both in terms of independence of representative in $(\mathbb{Z}/n)^\times$ but also in terms of the the image landing in the automorphism group of C_n.[1] Indeed,

$$i \equiv i' \pmod n \implies x^i = x^{i'} \in C_n \implies \psi([i]_n) = \psi([i']_n).$$

Thus the definition of ψ does not depend on the choice of representative i for the class $[i]_n$. Moreover, the image of $\psi([i]_n)$ is the subgroup $\langle x^i \rangle$ of C_n, and since $\gcd(i, n) = 1$, we know that $\langle x^i \rangle = C_n$. This shows that $\psi([i]_n)$ is surjective, and hence bijective because its domain and codomain have the same number of elements. This shows that ψ is a well-defined function whose codomain is indeed $\operatorname{Aut}(C_n)$.

Finally,

$$\psi(\varphi(\rho_i)) = \psi([i]_n) = \psi_i \quad \varphi(\psi([i]_n) = \varphi(\rho_i) = [i]_n.$$

Therefore, φ is a group isomorphism, as desired. □

[1]Note that in principle $\psi([j]_n)$ could simply be a homomorphism $C_n \to C_n$, rather than an isomorphism.