Week 9

Simple Groups

9.1 Simple Groups I

11/28:

- **Simple** (group): A group G for which the only normal subgroups of G are G and itself, i.e., $H \triangleleft G$ implies $H = G$ or $H = \{e\}$.
  - Simple does not mean "easy" but means "cannot be broken up into pieces."
  - By analogy, think of atoms as indivisible.
  - If you have G and $H \triangleleft G$, you get H and G/H, and you can think of G as being made up of $H, G/H$. Together, these two groups convey quite a bit of information about G.
  - Warning: $H, G/H$ do *not* determine G; just a lot of information about it.
    - Example: Let $H = \mathbb{Z}/2\mathbb{Z}$ and $G/H = \mathbb{Z}/2\mathbb{Z}$. Then we could have $G = (\mathbb{Z}/2\mathbb{Z})^2$ or $G = \mathbb{Z}/4\mathbb{Z}$.
- Idea: If you want to classify all finite groups, you might start with all finite simple groups, knowing that finite nonsimple groups can in some way be described by its simple quotients and subgroups.
- Problem I (Classification): Classify all finite simple groups.
  - A bit like understanding all prime numbers first in order to understand all composite numbers.
- Problem II (Extension problem): Given A, B, understand all G such that $A \triangleleft G$ and $G/A \cong B$.
  - We can build back up to G with $A \times B$ or other ways.
  - We'll talk about this one less than problem I.
- Examples:
  - Let p be prime. Then $G = \mathbb{Z}/p\mathbb{Z}$ is a simple group.
    - Follows directly form Lagrange's theorem.
    - It's even stronger than simple; the only *subgroups* (let alone normal subgroups) of $\mathbb{Z}/p\mathbb{Z}$ are $\mathbb{Z}/p\mathbb{Z}$ and $\{e\}$.
  - Let $n \geq 5$ and let $G = A_n$. Then A_n is a simple group.
    - More interesting and intricate. Has many subgroups but the only *normal* ones are itself and the trivial one.
    - Note that A_3 is also simple, but cyclic and abelian as well, so it got classified with the above.
- What does it mean to classify simple groups?
  - Start by asking what are the simple groups of some particular order.
  - Start with groups of a certain factorization or those with small order.

  - In this series of lectures, we'll focus on groups of small order. Can we understand for order below 100, 200, or 300?
  - What's important: Less the classification, more the application of techniques we've used. Fancier techniques needed for bigger n.

- Things in math aren't always hard because the technique is hard; they're hard because knowing what technique to use is hard. This is the challenge here.
- The prime factorization of the order says a lot about the group and allows us to make various conclusions.
- Theorem: Let p be prime. Suppose that $|G| = p^n$. Then if G is simple, we have $|G| = p$ and $G \cong \mathbb{Z}/p\mathbb{Z}$.

  Proof. If G is a p-group, then $Z(G) \neq \{e\}$.

  Case 1: $G = Z(G)$, so G is abelian. Therefore, let $g \in G$ have order p and let $H = \langle g \rangle \neq \{e\}$. If G is simple, then $H = G$ and therefore $|G| = p$.

  Case 2: G is not abelian. Take $H = Z(G) \neq G$. We know that $Z(G) \lhd G$, so G is not simple, a contradition. □

- Takeaway: $|G| = 2$ is simple, but $|G| = 4, 8, 16, \dots$ are all not simple.
- The general $p^i q^j$ case is very sophisticated, so we'll start simple.
- Lemma 1: Let $|G| = pq$ where p, q are distinct primes. Then G is not simple.

  Proof. Suppose for the sake of contradiction that G is simple with $|G| = pq$. WLOG, let $p > q$. WTS: One of the Sylow subgroups will be normal. The normal one is the one with greater order (motivation: D_{2n}; it's often useful to consider the p-Sylow subgroups for the largest p). What do we know? From the Sylow theorems, $n_p \cong 1 \mod p$ and $n_p \mid q$ (we know that $|N| = |G|/n_p = pq/n_p$, but since $n_p \equiv 1 \mod p$, $n_p \nmid p$, so it must be that $n_p \mid q$). $p > q$ implies $q \not\equiv 1 \pmod{p}$. Thus, $n_p = 1$. This is a contradiction: If there's only 1 p-Sylow subgroup, then that p-Sylow is normal (because all p-Sylows are conjugate, so one p-Sylow means its in its own conjugacy class). □

- We use a contradiction argument every time.
- Lemma 2: Let $|G| = pqr$. Then G is not simple.

  Proof. Strategy (again): Apply Sylow theorems and get information.

  WLOG, let $p > q > r$. We have that $n_p \equiv 1 \pmod{p}$ and $n_p \mid qr$. $n_p \in \{1, q, r, qr\}$. If $n_p \equiv 1 \pmod{p}$, the p-Sylow is normal in G, a contradiction. $q, r \not\equiv 1 \mod p$, so we eliminate those cases, too. One case left: qr. We thus deduce that $n_p = qr$.

  New technique: Because of these congruences, the number of p-Sylows cannot be really small (congruence obstructions). But we also know that it can't be too big. If there are that many elements of order p, we will crowd out the elements of other orders. We know that $n_q \equiv 1 \mod q$, and $n_q \mid pr$. $n_q = 1$ gives a contradiction. $n_q \not\equiv r$ because $n > r$. Thus, $n_q \in \{p, pr\}$. Doing the same thing for n_r, we get three possibilities: p, q, pr. Next step: Count elements. How many elements of order p are in G?

  Proposition: If $p \mid |G|$ exactly, then any two distinct p-Sylows have only trivial intersection. The number of $g \in G$ of order p is equal to $n_p(p-1)$.

  Because p exactly divides p, each p-Sylow is a subgroup of order p, but their intersection is a subgroup and thus has to divide the order (Lagrange's theorem). Thus, the order of the intersection is either 1 or p. Thus, all elements of order p lie in trivially intersecting p-Sylows. We count $p - 1$ elements of order p for each p-Sylow (p minus the identity).

Thus, since $p \,||\, |G|$ in this case, we know that the number of $g \in G$ with $|g| = p$ is $n_p(p-1) = qr(p-1)$. The number of $g \in G$ with $|g| = q$ is $n_q(q-1) \geq p(q-1)$. The number of $g \in G$ with $|g| = r$ is $n_r(r-1) \geq q(r-1)$. Counting the number of elements and the identity, we get

$$qr(p-1) + p(q-1) + q(r-1) + 1 = qrp + pq - p - q + 1 = pqr + (p-1)(q-1) > pqr = |G|$$

a contradiction. □

- This has to fail eventually, though — we know A_5 is simple for instance, and it has prime factorization $2^2 \cdot 3 \cdot 5$, so pqr^2 can be simple.
- Thus, we now turn to other types of factorizations.
- Thus, consider variations of the two primes case.
- First, new technique.
- Lemma 3: Let $G \subset S_4$ is simple. Then $|G| = 2, 3$.

  Proof. If we have a homomorphism from a simple group to any other group, it is either trivial or injective (our group doesn't break up; it either injects fully or disappears completely). We know that $\ker \phi \triangleleft G$, so if G is simple, either $\ker \phi = \{e\}$ (injective) or $\ker \phi = G$ (trivial).

  We know that $A_4 \triangleleft S_4 \twoheadrightarrow S_4/A_4 \cong \mathbb{Z}/2\mathbb{Z}$. Now let $G \triangleleft S_4$. We can apply a homomorphism to get a map from $G \to S_4/A_4$. It follows by the above claim that the homomorphism is either trivial or injective.

  Let Γ be a group with $A \triangleleft \Gamma$. Let $\Gamma/A = B$. If $G \hookrightarrow \Gamma$ is simple, then either $G \hookrightarrow A$ or $G \hookrightarrow \Gamma/A = B$. Proof: We have $G \to \Gamma \to \Gamma/A = B$. Case 1: G injects into B, so we get the latter claim. Case 2: the map is trivial, so everything in G maps to the identity in $B = \Gamma/A$. Then $G \leq A$. So if we know how to divide our group up, we can make something of the pieces.

  Returning to our example, we have $A_r \triangleleft S_4$, $S_4/A_4 = \mathbb{Z}/2\mathbb{Z}$, so $G \hookrightarrow A_4$, $G \hookrightarrow \mathbb{Z}/2\mathbb{Z}$. In the latter case, it has order 2. We have $K \triangleleft A_4$ and $A_4/K \equiv \mathbb{Z}/3\mathbb{Z}$. So either $G \leq K$ or $G \leq \mathbb{Z}/3\mathbb{Z}$. The first one implies since $K = (\mathbb{Z}/2\mathbb{Z})^2$ that $G \triangleleft \mathbb{Z}/2\mathbb{Z}$. □

- Groups of order 2,3 are trivially simple, so it's kind of meaningless, but doesn't matter; the lemma still holds.
- We narrowed in on the case of S_4 in order to prove our next theorem.
- Lemma 4 (No small actions): Let G be a simple group, and suppose $G \circlearrowright X$ transitively, where $|X| = 2, 3, 4$. Then $|G| = 2, 3$.

  Proof. Given a transitive action, we get a homomorphism $G \to S_X$. Transitivity and $|X| \geq 2$ implies the homomorphism is nontrivial. But since G is simple, $G \hookrightarrow S_X$. But since $|X| \leq 4$, this means that $G \hookrightarrow S_4$. We now use Lemma 3. This means that $|G| = 2, 3$.

  See lemma 6 for the kind of group action we are talking about?? □

- Corollary: If $p \mid |G|$, p is prime, G is simple, $|G| \neq 2, 3, p$, then $n_p \neq 1, 2, 3, 4$.
- Next time: At the same time these videos release, there will be a blog post with the statements of these lemmas and maybe some words on them.