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 $Z(G) \triangleleft G$, 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 $p \mid\mid |G|$ 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.

9.2 Office Hours (Abhijit)

- What do we need to know about the affine group of order p, as discussed in Lecture 8.1?
- Friday's office hours will be the last one unless Frank changes something. If the Twitch stream actually happens, Abhijit isn't sure what day it would be. Frank is currently traveling.
- HW8 2c requires 2d.
- Abhijit will email me more info on the A_5 question that he "beat a tactical retreat from."

9.3 Simple Groups II

11/30:
- Lemma 5: Assume $|G| = 2p^n, 3p^n, 4p^n$. p is a prime, and for mp^n, $m \neq p$. Then G is not simple.

  Proof. We again look at p-Sylows and how many are there. n_p must divide the order of the group and not divide p in these cases. Therefore, $n_p = 1, 2, 3, 4$, so as in Lemma 4, we have a very small set for G to act on. Thus, by Lemma 4, G is not simple. □

- Beefing this up a bit.
- Lemma 6: Assume $|G| = 5p^n$. Then G is not simple.

  Proof. Only interesting case: $n_p = 5$. In this case, we get an action of G on 5 points, namely the transitive action of G on the 5 p-Sylows by conjugation. Thus, we get an injective map $G \to S_5$, so $G \leq 5$ and has order $5p^n$. Additionally, since $n_p = 5 \equiv 1 \pmod p$, we know that $p = 2$. What else can we say? We now look at n_5. We know from Sylow III that $n_5 \equiv 1 \mod 5$ and $n_5 \mid (p^n = 2^n)$, so $2^n \geq 16$ (since $16 \equiv 1 \mod 5$ and 16 divides a power of 2). Thus, $|G|$ divides 16, but $|S_5| = 120$ which is not divisible by 16, a contradiction. □

- See again the procedure of "assume it's simple; derive a contradiction."
- Lemma 7: Assume $|G| = 6p^n$. Then G is not simple.

  Proof. We know that $n_p \mid 6$, so $n_p = 1, 2, 3, 6$. Lemma 4: $n_p = 6$. Sylow III: $n_p \equiv 1 \mod p$. Thus, $p = 5$. G acts on 6 p-Sylows, so we get an injective map from $G \hookrightarrow S_6$. How many powers of 5 can divide $|S_6|$? Only 5^1, so we must have $n = 1$. Thus, $|G| = 6 \cdot 5 = 30 = 5 \cdot 3 \cdot 2$. Applying Lemma 2 (3 distinct primes) finishes us off. □

- Lemma 8: Assume $|G| = 8p, 9p$. Then G is not simple.

  Proof. Look at n_p. $n_p = 1, 2, 4, 8$ in the first case; $n_p = 1, 3, 9$ in the second case. Lemma 4: Rule out $1, 2, 4$ and $1, 3$. Thus, $n_p = 8$ in the first case and $n_p = 9$ in the second case.

  First case: $n_p = 8$ and $n_p \equiv 1 \mod p$. We must have $p = 7$. Thus $|G| = 8 \cdot 7 = 56$. That's all we can get from the p-Sylow; now let's look at the 2-Sylow ($2^3 = 8$). $n_2 = 1, 7$. We apply the pqr too-many-elements style again. Number of elements of order 7 is $n_7(7-1) = 8 \cdot 6 = 48$. We have a group of 56 elements and 48 of them have order 7. So what's left? There are 8 elements left. But we know that the 2-Sylow has order 8, so let $P = G \setminus \{g \in G \mid |g| = 7\}$. Then $|P| = 8$. This implies that there is only one 2-Sylow, so $n_2 = 1$, meaning that the 2-Sylow is normal and giving us a contradiction. □

- Again, we only have a contradiction because we are assuming G is simple. If we don't assume G is simple, we have a perfectly valid mathematical derivation of the properties of a group of order $8p$.
- Example: Let $G = A_4$. Then $|G| = 12 = 3 \cdot 2^2$, so $n_3 = 1, 2, 4$ and $n_3 \equiv 1 \mod 3$. The 3-Sylow in A_4 is not normal, so $n_p \neq 1$. $n_p \neq 2$ because $2 \not\equiv 1 \mod 3$. Thus, $n_3 = 4$ and therefore the number of elements of order 3 is $n_3(3-1) = 4 \cdot 2 = 8$. Thus, there are 12 elements A_4 minus 8 elements of order 3, so there are 4 elements left. These 4 elements compose the 2-Sylow, meaning that the 2-Sylow is normal. And here (where we're not assuming G is simple), that's fine!
- So far: Continuing to build up and rule out groups of certain (mostly prime) factorizations.
- This will not classify all simple groups, but if we start taking n to be small, we know the factorizations of small numbers tend to have a small number of prime factors. So can we classify all groups of small order? That's our task now.
- Lemma 9: If $|G| = 84, 126, 140, 156, 175, 189, 198, 200$, then G is not simple.

Proof. $84 = 7 \cdot 3 \cdot 2^2$. Sylow III: $n_7 \equiv 1 \mod 7$ and $n_7 \mid 12$, so $n_7 = 1$.

$126 = 7 \cdot 18$. Sylow III: $n_7 \equiv 1 \mod 7$, $n_7 \mid 18$ implies $n_7 = 1$.

$140 = 7 \cdot 20$. Sylow III: $n_7 \equiv 1 \mod 7$, $n_7 \mid 20$ implies $n_7 = 1$.

$189 = 7 \cdot 27$. Sylow III: $n_7 \equiv 1 \mod 7$, $n_7 \mid 27$ implies $n_7 = 1$.

$176 = 11 \cdot 16$. Sylow III: $n_{11} \equiv 1 \mod 11$, $n_{11} \mid 16$ implies $n_{11} = 1$.

$176 = 11 \cdot 18$. Sylow III: $n_{11} \equiv 1 \mod 11$, $n_{11} \mid 18$ implies $n_{11} = 1$.

$175 = 5^2 \cdot 7$. Sylow III: $n_5 \equiv 1 \mod 5$, $n_5 \mid 7$ implies $n_5 = 1$.

$200 = 5^2 \cdot 8$. Sylow III: $n_5 \equiv 1 \mod 5$, $n_5 \mid 8$ implies $n_5 = 1$.

$156 = 13 \cdot 12$. Sylow III: $n_{13} \equiv 1 \mod 13$, $n_{13} \mid 12$ implies $n_{13} = 1$. □

- A bit messy and *ad hoc*, but this covers the simple groups of certain orders we haven't covered so far.
  - If you do a random case for a small number, often it will be a bit like this.
- For a bunch of small numbers, we immediately get without any work from the Sylow theorems a normal p-Sylow.
  - We actually get these conclusions for any groups of these orders??
- This way of thinking lends itself to you generating your own problem; you basically choose a random number and look for a prime with $n_p = 1$.
- Two more exceptional cases.
- Lemma 10: If $|G| = 132$, then G is not simple.

Proof. $132 = 11 \cdot 12$, so $n_{11} = 1, 12$. If 1, we're done. If very large, we get that contradiction. The number of elements of order 11 is $n_{11}(11-1) = 12 \cdot 10 = 120$, so only 12 elements left. We now consider other primes. $11 \cdot 12 = 11 \cdot 3 \cdot 2^2$. $n_3 \equiv 1 \mod 3$, $n_3 \mid 44$. Thus, $n_3 = 1, 2, 4, 11, 22, 44$. If 1, we're done. 2,11,44 can't happen because of the congruence law. If $n_3 = 4$, apply Lemma 4. Thus, $n_3 = 22$, so the number of elements of order 3 is $n_3(3-1) = 22 \cdot 2 = 44$. $120 + 44 > 132$, so we win. □

- At this point, we've considered a bunch of easy general and special cases. At this point, let's look at the numbers under 200 we can rule out.
  - Calegari writes out all numbers from 1-200.
  - For the prime numbers, there is a simple group of that order.
  - Powers of primes, there is no simple group, so we can cross those off ($4 = 2^2, 8 = 2^3, 9 = 3^2, 16 = 2^4, 25 = 5^2, 27 = 3^3, 32 = 2^5, \ldots$).
  - Products of two primes, there is no simple group ($6 = 2 \cdot 3, 10 = 2 \cdot 5, 15 = 3 \cdot 5, \ldots$).
  - Products of three distinct primes, there is no simple group ($30 = 2 \cdot 3 \cdot 5, 42 = 2 \cdot 3 \cdot 7, \ldots$).
  - Everything that's $2p^n, 3p^n, 4p^n$, there is no simple group ($12 = 3 \cdot 2^2, 18 = 2 \cdot 3^2, \ldots$).
  - Everything that's $5p^n$, there is no simple group ($20 = 5 \cdot 2^2, 40 = 5 \cdot 2^3, \ldots$).
  - Everything that's $6p^n$, there is no simple group (just $150 = 6 \cdot 5^2$). Only got one number with Lemma 7 :(
  - Everything that's $8p, 9p$, there is no simple group ($56 = 8 \cdot 7, 63 = 9 \cdot 7, 88 = 8 \cdot 11, 99 = 9 \cdot 11, \ldots$).
  - Exceptional numbers done by hand: $84, 126, 132, 140, 156, 175, 189, 198, 200$.
- There are no simple groups of order 1 by definition, so the trivial group is not a simple group much the same way 1 is not a prime number.

- At this point, we have to acknowledge that this list left out numbers, so we have to see what's left and then work with it.
- First numbers up: 60 (there does happen to be a simple group of this order here — A_5), 72, 90.
  - Thus, if we have a simple group of order less than 100, it is of prime order or of order 60, 72, or 90 (note that we can still eliminate 72 and 90, but we haven't investigated them yet, so it's fair to include them here; not the most restrictive theorem, but a valid one all the same).
- Next numbers up: 112, 120, 144, 168, 180.
  - Calegari really does have quite a fast mind as he's doing prime factorizations by memory.
- Thus, using the lemmas, we've proven the following: A simple group of order at most 200 either has prime order, or order 60, 72, 90, 112, 120, 144, 168, or 180.

9.4 Simple Groups III

12/2:

- Proposition: Let G be a simple group of order $|G| \leq 200$. Then either $|G|$ is prime (in which case we know there is a unique simple group of said order) or $|G| \in \{72, 112, 60, 90, 120, 144, 180, 168\}$.
  - These numbers are not in increasing order; they are more or less in order of increasing difficulty.
- Case: $|G| = 72 = 3^2 \cdot 2^3$.

  Proof. $n_3 \equiv 1 \mod 3$ and $n_3 \mid 8$, so either $n_3 = 1, 4$. $n_3 = 1$ implies normal 3-Sylow; $n_3 = 4$ implies invoke Lemma 4. Therefore, G is not simple. ☐

- Reminder: If G is simple, then any homomorphism from it to another group must be either trivial or injective.
- Lemma 11: Let G be a simple group with a transitive action on a set of $n \geq 2$ points. Then $G \hookrightarrow A_n$ or $|G| = 2$.

  Proof. The action induces a homomorphism $G \to S_n$ which is nontrivial. Therefore, $G \hookrightarrow S_n$. Now we want to upgrade this map and restrict the range. Now suppose that the image is not in A_n. Then the composite map $G \to S_n \to S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$ is nontrivial. If $g \in A_n$, then $g \mapsto eA_n = A_n$. If $g \notin A_n$, then $g \mapsto gA_n$. This nontrivial map into $\mathbb{Z}/2\mathbb{Z}$ implies, since G is simple, that $G \hookrightarrow \mathbb{Z}/2\mathbb{Z}$, so $|G| = 2$. ☐

- Lemma 12: If $|G| = 112$, then G is not simple.

  Proof. $112 = 7 \cdot 2^4$. We can deduce that $n_7 \equiv 1 \mod 7$ and $n_7 \mid 16$, so $n_7 = 1, 8$. If $n_7 = 1$, we win, so let's consider $n_7 = 8$. 8 is pretty big, but not too big. It's in this annoying intermediate range. We deduce from this that there are $n_7(7-1) = 8 \cdot 6 = 48$ elements of order 7, which doesn't help much. Here, it's better to look at $n_2 = 1, 7$. If $n_2 = 1$, we win, so consider $n_2 = 7$. Then by Lemma 11, $G \hookrightarrow A_7$. $|G| = 112$ and $|A_7| = 2520$. But $|G| \nmid |A_7|$, contradicting Lagrange's Theorem. ☐

- Next up: 60, 90, 120, which we will consider all at once because they're all a bit similar. One preliminary lemma first, though.
- Lemma 13: Let $n \geq 5$ and $H \leq A_n$ of index $d > 1$. Then $d \geq n$ and if $d = n$, then $H \cong A_{n-1}$. In other words, there are no small-index subgroups and the smallest one is isomorphic to A_{n-1}.

Proof. A_n acts transitively on the cosets A_n/H (by left multiplication??), inducing a nontrivial map from $A_n \to S_d = S_{\{\text{cosets}\}}$. Since A_n is simple for $n \geq 5$, we get that $A_n \hookrightarrow A_d = A_{\{\text{cosets}\}}$ (by Lemma 11). The injection implies that $d \geq n$. Now assume that $d = n$. Then we have an isomorphism from A_n to $A_{\{\text{cosets}\}}$. What is $H \leq A_n$? How does H act on $A_{\{\text{cosets}\}}$? Well H stabilizes the coset H, so $H \hookrightarrow \text{Stab}(H)$. But the stabilizer of a point in the symmetric group is isomorphic to the symmetric group of one smaller size, and the same holds true in the alternating group, so $\text{Stab}(H) \cong A_{n-1}$. $[A_n : H] = n$ by hypothesis, so $|H| = (n!/2)/n = (n-1)!/2$. But since this is also $|A_{n-1}|$, we have an injection from H into a group of the same order, meaning that we have a bijection. In particular, $H \cong A_{n-1}$, as desired. □

- Comments on Lemma 13: ...
- Lemma 14: If G is simple and $|G| \in \{60, 90, 120\}$, then $G \cong A_5$. In particular, we rule out 90,120 and know that 60 must be the last number standing.

Proof. $60 = 5 \cdot 12$, $90 = 5 \cdot 18$, $120 = 5 \cdot 24$. $n_5 \equiv 1 \mod 5$ and $n_5 \mid 12, 18, 24$ implies $n_5 = 1, 6$ (we can confirm that 11,16,21 are not factors). If $n_5 = 1$, we're done, so assume $n_5 = 6$. G acts on the 6 5-Sylow subgroups transitively, giving us $G \hookrightarrow A_6$ by Lemma 13. $[A_6 : G] = 6, 4, 3$ for 60,90,120. But by Lemma 13, $d \geq 6$, so contradiction for 90,120, and the latter part of the Lemma proves that $G \cong A_5$. □

- We have our first genuine simple group of nonprime order at this point, and we know that that group is unique and equal to A_5.
- Lemma 15: There is no simple group of order 144.

Proof. Many of the arguments we've used thus far will play in, but in new and unexpected ways. We have $144 = 2^4 3^2$. $n_3 \equiv 1 \mod 3$ and $n_3 \mid 16$, so $n_3 = 1, 4, 16$. If $n_3 = 1$, we're done (normal 3-Sylow). If $n_3 = 4$, we apply Lemma 4. Thus, $n_3 = 16$. Number of elements of order 3: Issue — we no longer know that the intersections of the p-Sylows are trivial since $p^2 = 9$; we could have a subgroup of order 3 as the intersection.

Case 1: $P \neq Q$ are 3-Sylows, WTS: $P \cap Q = \{e\}$. Number of elements of order 3 or 9 is $n_3 \cdot 8 = 16 \cdot 8 = 128$. This leaves $144 - 128 = 16$ elements. But since G has a 2-Sylow P_2 of order 16, so $G = P_2 \cup \{|g| = 3, 9\}$. Thus, $n_2 = 1$, so we have a normal subgroup, which is a contradiction.

Case 2: There exist 3-Sylows P, Q such that $C = P \cap Q$ has $|C| = 3$. We can still gain some advantage since it's 3^2, not 3^n. Remark: If $|P| = 9$, then P is abelian. Recall that p-groups of order p^2 are abelian. What other constructions do we have for subgroups besides Sylows? Consider $N = N_G(C)$, where $C = P \cap Q$. $C \leq P$ and $C \leq Q$. But since P is abelian, then $P \subset N_G(C)$. Lagrange: $9 \mid N \mid 144$, so $N = 18, 36, 72, 144$. So we need 4 contradictions to finish this off. If $|N| = 144$, then $N = G$. But since $C \triangleleft N$, this means that $C \triangleleft G$, i.e., G has a normal subgroup and is not simple, a contradiction. If $N = 72, 36$, then $[G : N] = 2, 4$. Thus, G acts transitively on a set of size 2,4, so Lemma 4 eliminates these. Only possibility: $|N| = 18$. We know that $Q \subset N$ and $P \subset N$. By applying the Sylow theorems to N, we get that $n_3 \equiv 1 \mod 3$, $n_3 \mid 2$, so $n_3 = 1$, but N contains 2 distinct p-Sylows, a contradiction. □

- The case of 180 is quite similar.
- Lemma 16: There is no simple group of order 180.

Proof. $180 = 5 \cdot 3^2 \cdot 2^2$. $n_5 \equiv 1 \mod 5$, so $n_5 = 1, 6, 36$. $n_5 \neq 1$. If $n_5 = 6$, then $G \hookrightarrow A_6$ and we get index 2, which is a contradiction by Lemma 13 (same contradiction as with 90,120). If $n_5 = 36$, then we get a number of elements of order 5 equal to $n_5(5-1) = 144$, leaving $180 - 144 = 36$ elements left to contain the 2-Sylows and 3-Sylows. But we get the same annoyance about whether or not they overlap.

$n_3 \mid 20$ and $n_3 \equiv 1 \mod 3$ yields $n_3 = 1, 4, 20$. $n_3 = 1$ is normal, 4 invokes lemma 4, so $n_3 = 20$.

Case 1: $P \cap Q = \{e\}$. Then the number of elements of order 3 or 9 is $n_3(9-1) = 160$. Contradiction (too many elements).

Case 2: $P \cap Q = C$, $|C| = 3$. Take $N = N_G(C)$. So once again, we have $9 \mid |N| \mid 180$ and $|N| > 9$. Thus, $|N| = 18, 36, 45, 90, 180$. $|N| = 180$ gives us $C \triangleleft G$ again. $|N| = 90, 45$ yields $[G:N] = 2, 4$ again. This leaves us with 18,36. We can't have 2 3-Sylows, so $|N| = 36$. Thus, $[G:N] = 5$. This induces $G \hookrightarrow A_5$, but G is too big; $G \not\leq A_5$, a contradiction. □

- Summary of what we've proven so far.
- Theorem: Let G be a simple group of order at most 200. Then either...
  1. $|G| = $ prime;
  2. $G \cong A_5$;
  3. $|G| = 168$ and $G \cong \mathrm{GL}_3(\mathbb{F}^2) \cong \mathrm{PSL}_2(\mathbb{F}_7)$.
- This is the limit of what we'll do; Calegari doesn't think it's worth the hour it'd take to do a full analysis of 168.
- A word on 168, though.
  - $168 = 2^3 \cdot 3 \cdot 7$.
  - Deduce that $n_7 = 8$. $n_2 = 1, 3, 7, 21$ so $n_2 = 7, 21$. $n_3 = 1, 2, 4, 7, 8, 14, 28, 56$ so $n_3 = 7, 28$ by Lemma 4 and the $1 \mod 3$ rule. But none of the remaining numbers are super easy to work with; we need normalizers and such.
  - Start with n_7 to learn that $G \hookrightarrow A_8$. We also know that $n_7 = [G:N]$, so $|N| = 21$. Let P be a 7-Sylow. Up to conjugation, we may as well take $P = \langle(1,2,3,4,5,6,7)\rangle \subset A_6$. Additionally, $N \subset N_{A_8}(\langle(1,2,3,4,5,6,7)\rangle)$ which has order 21.
  - More and more elaborate facts lead you to write down parts of the group in terms of elements of A_8.
  - The contradictions and computations we eventually get do get messy eventually.
  - The reason for this is because there *does* exist a simple group of order 168: We know that $\mathrm{SL}_2(\mathbb{F}_7)$ has an action on 8 points. The quotient $G = \mathrm{PSL}_2(\mathbb{F}_7)$ is a simple group of order 168.
  - There's another group $|\mathrm{GL}_3(\mathbb{F}^2)| = (2^3-1)(2^3-2)(2^3-2^2) = 168$. These two groups are isomorphic (this is completely opaque from the description, but it is true; there is an exotic isomorphism; it's like the story between the cube group and S_4?? This is a recurring theme in finite group theory).
  - Indeed, these two groups are the only one of 168.
- On the blog, Calegari will continue from 200 all the way up to 300.
- Particularly bad cases include more and more powers of 2 and 3.
- Theorem (Burnside's pq theorem): If $|G| = p^n q^m$, then G is not simple.
  - In other words, once you remove the cyclic group, any simple group has at least 3 prime factors dividing its factorization.
  - This theorem is beyond the scope of this course, but it could come up in an intro grad course on representations of groups.
- In our course, we've really been studying actions of G on finite sets, i.e., maps to symmetric groups.

  - Another natural thing we can do is consider the actions on vector spaces (specifically the basis of a vector space). This corresponds to a map from $G \to \mathrm{GL}_n(V)$. This is a rich theory and allows us to write out all the possible representations. Proving Burnside's pq theorem involves all of this plus algebraic number theory.

- Burnside's pq theorem came to prominence around 1900, so about 120 years back.
- Theorem (Feit-Thompson): If G is a simple group and $|G|$ is odd, then $|G| =$ prime.
  - From the 1960s.
  - This is the start of modern group theory.
  - It follows by the Sylow theorems that our group has an element of order 2. From here, we can start to think about the classification of all finite simple groups.
- Thus, not only do simple groups have to have at least 3 prime factors, they also have to have even order.
- The classification of finite simple groups was achieved 20-30 years after Feit-Thompson.
  - Thus, we now really understand all finite simple order.
  - This means that we can describe them by various lists that we know how to construct.
  - Examples: Cyclic groups of prime order, A_n ($n \geq 5$), $\mathrm{PSL}_n(\mathbb{F}_p)$ ($n \geq 3$ or $n = 2$ and $p \geq 5$).
  - Calegari goes over several more groups of Lie type. There are also 26 sporadic group types that don't really fit in any other category. One class called the Mathieu group. Simplest weird group: M_{11} of order $11 \cdot 10 \cdot 9 \cdot 8 = 7920$. There's also M_{12}, M_{23}, M_{24}. There are 26 of these leading up to a group M called the **monster group** (of order $\approx 8 \times 10^{53}$).
  - We have to be careful in saying that the monster group is scary just because it's so big; indeed, S_{52} is bigger. But the latter is understandable by its action on a relatively small set. S_{52} acts on a vector space of dimension 52. If you try to let M act on a vector space, the dimension is 196883.
  - Something better than this type of description is infinite groups. The most interesting infinite groups arise when you have topological considerations as well (e.g., continuity). This is why S_∞ is not the most interesting. We have orthogonal and unitary groups (these arise in physics often as infinite symmetry groups). Pure topology and spaces and symmetries are potential applications, too. We don't consider these in this course because these topics are so intertwined.
- Next quarter is ring theory, and last quarter is Galois theory.
- In group theory, you want to understand all finite groups. In ring theory, you don't want to classify rings; rather, you want to consider a bunch of simple rings that come up all the time, and you want to understand those very well.

9.5 Twitch Stream

12/3:

- 18a of the review sheet is true.
  - Orbit-Stabilizer Theorem: $|C| \cdot |\langle g \rangle| = |G|$. C is the centralizer. So we need to compute the size of the conjugacy class of the n-cycle. There are $n!/n$ of these. So $C = n$.
  - The centralizer is not the normalizer; the latter will be bigger.