210A Discussion Notes

Jung Joo Suh

Fall 2022

Discussion 1 - Groups Related to (Finite) Fields

Spring 2020 Problem 6 (Modified): Let $\mathbb{F}$ be a finite field with $|\mathbb{F}| = n(= p^m)$ (why is $n = p^m$?). Find an explicit formula for $|\mathrm{Gl}_k(\mathbb{F})|$.

Recall that $\mathrm{Gl}_k(\mathbb{F}) = \mathrm{Aut}_{\mathbb{F}-\text{linear}}(\mathbb{F}^k) = \{A \in M_k(\mathbb{F}) \mid \det(A) \neq 0\}$.

Soln. A $k \times k$ matrix $A = \begin{pmatrix} \overrightarrow{a_1} & \overrightarrow{a_2} & \cdots & \overrightarrow{a_k} \end{pmatrix}$ is invertible if and only if the column vectors $\overrightarrow{a_1}, \overrightarrow{a_2}, \ldots, \overrightarrow{a_k}$ are linearly independent. And this is true if and only if $\overrightarrow{a_1} \neq 0$, $\overrightarrow{a_2} \notin \mathrm{Span}(\overrightarrow{a_1}), \ldots, \overrightarrow{a_k} \notin \mathrm{Span}(\overrightarrow{a_1}, \overrightarrow{a_2}, \ldots, \overrightarrow{a_{k-1}})$.

So, there are $n^k - 1$ ways to choose $\overrightarrow{a_1}$, $n^k - n$ ways to choose $\overrightarrow{a_2}$, $n^k - n^2$ ways to choose $\overrightarrow{a_3}$, etc. until at stage k, we have $n^k - n^{k-1}$ ways to choose $\overrightarrow{a_k}$. By the multiplicative principle of counting, there are exactly $(n^k - 1)(n^k - n) \cdots (n^k - n^{k-1})$ many ways to choose such pairs, so $|\mathrm{Gl}_k(\mathbb{F})| = \boxed{(n^k - 1)(n^k - n) \cdots (n^k - n^{k-1})}$. □

For the remainder of the session, we prove the following theorem:

Theorem 1. Let $\mathbb{F}$ be a finite field. Then $\mathbb{F}^\times = (\mathbb{F} - \{0\}, \times)$ is cyclic.

Before we prove the theorem, we prove several lemmas.

Lemma 1. Let G be an abelian group with $|G| = n$. Then, for all $g \in G$, $g^n = e$.

Proof. Let $g \in G$ and consider the map $g \cdot (-) : G \to G, a \mapsto g \cdot a$ the multiplication (left or right, as they are equal) by g. Then, this is clearly a bijection with the inverse given by $g^{-1} \cdot (-)$. So $g \cdot (-)$ shuffles the elements one-to-one, so

$$\prod_{a \in G} a = \prod_{a \in G} ga = g^n \prod_{a \in G} a.$$

Cancelling out the product $\prod_{a \in G} a$, we get $e = g^n$ as desired. □

Remark 1. As a corollary to Lagrange's Theorem (to be covered in later lectures), we can show that the conclusion is true for arbitrary finite groups, not just abelian groups.

Lemma 2. Let G is an abelian group and $g, h \in G$ be with $\mathrm{ord}(g) = m$ and $\mathrm{ord}(h) = n$ such that $\gcd(m, n) = 1$. Then, $\mathrm{ord}(gh) = mn = \mathrm{lcm}(m, n)$.

Proof. First, note $(gh)^{mn} = g^{mn}h^{mn} = e \cdot e = e$. Now, suppose $(gh)^k = g^k h^k = e$, then $g^k = h^{-k}$. We can "raise" both sides to mth power to obtain $e = g^{mk} = h^{-mk}$. So we have $n \mid -mk$ since $n = \text{ord}(h)$. But then, since $\gcd(m, n) = k$, $n \mid k$. By similar reasoning with m and n swapped, we get $m \mid k$. Hence, $\text{lcm}(m, n) = mn \mid k$. □

Remark 2. Without the assumption that $\gcd(m, n) = 1$, $\text{ord}(gh)$ need not be mn or even $\text{lcm}(m, n)$. For example, take any $g \in G$ not equal to the identity so that $\text{ord}(g) = m > 1$, and consider g, g^{-1}. We have $\text{ord}(g) = \text{ord}(g^{-1}) = m$, but $\text{ord}(gg^{-1}) = \text{ord}(e) = 1 < m = \text{lcm}(m, m)$.

Lemma 3. Let G be an abelian group with $|G| = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ where $p_1, p_2, \ldots, p_k$ are distinct primes. Set, for each $i = 1, 2, \ldots, k$,

$$m_i = \max \{a_i \mid \exists g \in G \text{ such that } \text{ord}(g) = p_i^{a_i} v_i \text{ where } p_i \nmid v_i\}$$

In other words, each m_i is the maximum power of p_i that appears in the prime factorization of order of $g \in G$. Then, there exists an element $h \in G$ of order $p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$.

Proof. For each i, choose g_i with order $p_i^{m_i} v_i$ with $p_i \nmid v_i$. Then, set $h_i = g^{v_i}$, which has order p^{m_i}. Now, by Lemma 2, the element $h := h_1 h_2 \cdots h_k$ has order $p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$, as desired. □

Corollary 1. For all $g \in G$, $\text{ord}(g) \mid p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$.

Proof. Let $g \in G$. Then, $\text{ord}(g) \mid |G| = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ by Lemma 1, so $\text{ord}(g) = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$ for some $f_1, f_2, \ldots, f_k \geq 0$. By definition of m_i's it follows $f_i \leq m_i$, which implies that $\text{ord}(g)$ divides $p_2^{m_1} p_2^{m_2} \cdots p_k^{m_k}$. □

We're finally ready to present the proof of Theorem 1

Proof of Theorem 1. Let $|\mathbb{F}^\times| = n - 1 = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. We can set m_i as before.

Claim. For all i, $m_i = e_i$.

Proof of the Claim. Suppose for some i, $m_i < e_i$. Set $L = p_1^{m_1} p^{m_2} \cdots p^{m_k}$ which, by assumption, must be strictly smaller than $n - 1 = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Then, by Lemma 3, $\alpha^L = 1$ for all $\alpha \in \mathbb{F}^\times$. But then, we have $x^L - 1$ having at least $n - 1 > L$ many distinct roots, which is impossible for a field. □

The claim implies that we can find an element $\alpha \in \mathbb{F}^\times$ of order $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} = n - 1 = |\mathbb{F}^\times|$ by Lemma 3 again. Hence, $\mathbb{F}^\times$ is cyclic. □

Remark 3. Later in 210B, we will learn the Structure Theorem for Finitely Generated Abelian Groups, which will allow us to prove the theorem much more easily.

Discussion 2 - Zorn's Lemma and Finitely Generated Groups

Definition 1. Given a set $\mathcal{P}$, a partial order $\preceq$ on $\mathcal{P}$ is a binary relation satisfying the following properties:

(i) (Reflexivity) For all $x \in \mathcal{P}$, $x \preceq x$

(ii) (Anti-symmetry) For all $x, y \in \mathcal{P}$, $x \preceq y$ and $y \preceq x$ implies $x = y$

(iii) (Transitivity) For all $x, y, z \in \mathcal{P}$, $x \preceq y$ and $y \preceq z$ implies $x \preceq z$.

A set $\mathcal{P}$ together with partial order $\preceq$ $(\mathcal{P}, \preceq)$ is called a *Partially Ordered Set*, or *poset* for short. As usual, the partial order is often suppressed.

A subset $\varnothing \neq \mathcal{C} \subset \mathcal{P}$ is a chain if the relation $\preceq$ restricted to $\mathcal{C}$ is in addition, linear (total) order. That means for all $x, y \in \mathcal{C}$, $x \preceq y$ or $y \preceq x$.

An element $M \in \mathcal{P}$ is maximal if there doesn't exist any $x \in \mathcal{P}$ with $x \succ M$. In other words, M is *not* strictly less than any other element.

Now, we state Zorn's Lemma, which will be used throughout this 210ABC course sequence.

Lemma 4 (Zorn's Lemma)**.** Let $\mathcal{P}$ be a non-empty poset. If every chain $\mathcal{C} \subset \mathcal{P}$ has an upper bound in $\mathcal{P}$, then, $\mathcal{P}$ has a maximal element.

We state this lemma as fact without proof:

Lemma 5 (Hartog's Lemma)**.** Let A be any set. Then, there exists an ordinal α that does not inject into A ($\alpha \not\hookrightarrow A$). I.e. there does not exists an injection $f : \alpha \hookrightarrow A$.

Proof of Zorn's Lemma. Suppose for the sake of contradiction that $\mathcal{P}$ does not have a maximal element. First, applying Hartog's Lemma, choose an ordinal $\alpha \not\hookrightarrow \mathcal{P}$. We apply transfinite recursion on α to construct a strictly increasing α-sequence $\{a_\beta\}_{\beta<\alpha}$.

0 case: Choose any $a_0 \in \mathcal{P}$ (this is where we use non-emptiness).
Successor $\beta = \gamma + 1$ case: Assume a_λ has been constructed for all $\lambda < \beta$, including $\lambda = \gamma$. Now, since $\mathcal{P}$ has no maximal element, $a_\gamma \in \mathcal{P}$ is not maximal. So we can choose $a_\beta \succ a_\gamma$ (we use the Axiom of Choice here).
Limit case $\beta = \sup_{\gamma<\beta} \gamma$: Again, assume a_γ has been constructed for all $\gamma < \beta$. By the inductive hypothesis, the sequence $\{a_\delta\}_{\delta<\gamma}$ up to γ can be assumed to be a strictly increasing sequence; hence, $\{a_\gamma\}_{\gamma<\beta}$ is a strictly increasing sequence. In particular, this is a chain in $\mathcal{P}$, so we can choose a_{beta} an upper bound of the sequence (we again used Axiom of Choice here). Note a_β is strictly larger than a_γ for all $\gamma < \beta$ (why?).

Now, the sequence $\{a_\beta\}_{\beta<\alpha}$ constructed must be an injective map from $\alpha \to \mathcal{P}$ since it is also strictly increasing. But this contradicts the choice of α. □

Recall given a set $S \subset G$,

$$\langle S \rangle := \bigcup_{\substack{H \leq G \\ S \subset H}} H = \{s_1^{\varepsilon_1} s^{\varepsilon_2} \cdots s_n^{\varepsilon_n} \mid s_i \in S, \varepsilon_i = \pm 1\}$$

We call $\langle S \rangle$ the subgroup generated by S (the second equality there is left as an exercise to the reader).

Definition 2. We say a group G is finitely generated if there exists a finite subset $S \subset G$ so that $\langle S \rangle = G$.

Theorem 2. Every non-trivial finitely generated group G has a maximal (proper) subgroup.

Proof. Let $\mathcal{P} = \{H \mid H \lneq G\}$ the set of all proper subgroups of G (ordered by inclusion). What we're looking for is exactly a maximal element of $\mathcal{P}$ - to that end, we apply Zorn's lemma.

Since $\{e\} \in \mathcal{P}$ (this is where we use G is nontrivial), $\mathcal{P}$ is non-empty. Now, suppose we have a chain $\mathcal{C} \subset \mathcal{P}$ of proper subgroups. Set $K = \cup\mathcal{C} = \cup_{H\in\mathcal{C}} H$.

Claim. K is an upper bound of $\mathcal{C}$ in $\mathcal{P}$.

Proof of the Claim. Clearly, if $K \in \mathcal{P}$, K is an upper bound of $\mathcal{C}$, so this is what we check. Let $g, h \in K$ be two elements. Then, $g \in H_1$ and $h \in H_2$ for some $H_1, H_2, \in \mathcal{C}$. Assume WLOG $H_1 \leq H_2$ (this is where we use that $\mathcal{C}$ is a chain). Then, $gh^{-1} \in H_2 \subset K$. So K is a subgroup.

Next, we check K is proper. Suppose $K = G$. Since G is finitely generated, there exists $g_1, g_2, \ldots, g_n$ which generate G, and we know $g_1, g_2, \ldots, g_n \in K$. So for each i, $g_i \in H_i$ for some $H_i \in \mathcal{C}$. Take $H = \max(H_1, H_2, \ldots, H_n) \in \mathcal{C}$ (again, this is where we use that $\mathcal{C}$ is a chain). Then, $g_1, g_2, \ldots, g_n \in H \in \mathcal{C}$. But then, this contradicts that $H \in \mathcal{C}$ as H is not a *proper* subgroup. □

By the claim, we can now apply Zorn's Lemma to $\mathcal{P}$. It follows that $\mathcal{P}$ has a maximal element as desired. □

Fall 2015 Problem 8: Let $\mathbb{F}$ be a field. Show that the group $\mathrm{Sl}_2(\mathbb{F})$ is generated by the matrices $\begin{pmatrix} 1 & e \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ e & 1 \end{pmatrix}$ for elements $e \in \mathbb{F}$.

Spring 2012 Problem 5: Let G be a finite group, K a normal subgroup and P a p-Sylow subgroup of G. Prove that $P \cap K$ is a p-Sylow subgroup of K.

Proof. Note $P \cap K \leq P$ is also group of prime power. By the second isomorphism theorem,

$$P/P \cap K \cong PK/K$$

So $\frac{|P|}{|P\cap K|} = \frac{|PK|}{|K|}$, so rearranging, we get $\frac{|K|}{|P\cap K|} = \frac{|PK|}{|P|}$. Now, note $P \leq PK \leq G$ since K is normal (so PK is a subgroup of G) and $p \nmid \frac{|G|}{|P|}$. Hence, $p \nmid \frac{|PK|}{|P|} = \frac{|K|}{|P\cap K|}$. So we have $P \cap K$ a subgroup of K of p-power such that $p \nmid [K : P \cap K]$, so $P \cap K$ is a p-Sylow subgroup of K. □

Discussion 3 - Group Actions: Part 1

Definition 3 (Group Action Dynamical Version)**.** Let G be a group and X a set. Then, a *group action* of G on X, denoted $G \curvearrowright X$, is a binary function $\cdot : G\times X \to X, (g, x) \mapsto g\cdot x$ satisfying the following:

(i) $e \cdot x = x$ for all $x \in X$

(ii) for all $g, h \in G$, and $x \in X$, $(gh) \cdot x = g \cdot (h \cdot x)$.

Definition 4 (Group Action Alternative Version)**.** Let G be a group and X a set. A *group action* of G on X is just a homomorphism $\phi : G \to S_X$, where S_X is the symmetric group on X.

Remark 4. We can translate one definition from another as follows. Given a $\cdot : G \times X \to X$, we define $\phi(g) \in S_X$ to be $x \mapsto g \cdot x$ (check $\phi(g)$ belongs to S_X). This is a homomorphism by the condition (ii). On the other hand, if we're given a homomorphism $\phi : G \to S_X$, we can define $g \cdot x = \phi(g)(x)$. From the fact that ϕ is a homomorphism, (ii) immediately follows. Since $\phi(e) = \mathrm{id}_X$, (i) follows as well.

Moreover, the assignment $\cdot \mapsto \phi$ and $\phi \mapsto \cdot$ described as above gives one-to-one correspondence between the two definitions which are inverses of one another.

Remark 5. Orbits partition X, so if X is finite, then $|X| = \sum |\mathrm{orbit}(X)|$ where the sum ranges over all possible orbits. Now, $\mathrm{orbit}(X) \cong G/\mathrm{Stab}(X)$ as G-sets. So if G is a p-group, then $p \mid \mathrm{orbit}(X)$ if and only if $\mathrm{Stab}(X) \lneq G$. In particular, $|X| \equiv |X^G| \bmod(p)$.

Spring 2014 Problem 5: Let G be a finite group acting transitively on a finite set X. Let $x \in X$ and let P be a Sylow p-subgroup of the stabilizer of x in G. Show that $N_G(P)$ acts transitively on X^P.

Proof. Let $y \in X^P$. Since $G \curvearrowright X$ is transitive, $\exists g \in G$ such that $y = g \cdot x$. We want to look for such a $g \in N_G(P)$. Set $S = \{g \in G \mid y = g \cdot x\}$. Then, we want $S \cap N_G(P) \neq \varnothing$.

Lemma 6. For any finite subgroup $H \leq G$, we have $H \curvearrowright G/H$ via $h \cdot (gH) = hgH$. Then, $g \in N_G(H)$ if and only if gH is a fixed point.

Proof. Let $g \in G$. Now,

$$\begin{aligned} gH \text{ is a fixed point } &\Leftrightarrow hgH = gH \text{ for all } h \in H \\ &\Leftrightarrow g^{-1}hgH = H \text{ for all } h \in H \\ &\Leftrightarrow g^{-1}hg \in H \text{ for all } h \in H \\ &\Leftrightarrow g^{-1}Hg \leq H \end{aligned}$$

But note since H is finite, and $|g^{-1}Hg| = |H|$, $g^{-1}Hg = H$. But this is equivalent to $g \in N_G(H)$. □

So we want $g \in S$ such that gP is the fixed point of the action $P \cap G/P$. Set $S/P = \{gP \mid g \in S\}$ (which equals $\pi(S)$ where $\pi : G \to G/P, g \mapsto gP$). Note for any $g \in S$, $S = g \cdot \mathrm{Stab}(x)$. So, $S/P \cong g \cdot \mathrm{Stab}(x)/P$ as G-sets. So $|S/P| = |\mathrm{Stab}(x)/P|$. But note $p \nmid |S/P| = |\mathrm{Stab}(x)|$ since P is a Sylow p-subgroup of $\mathrm{Stab}(x)$, so $|S/P|$ must have a fixed point. In particular, there exists $g \in S$ so that gP is a fixed point, equivalently, $g \in N_G(P)$. □

Fall 2014 Problem 6: Let G be a finite group and let p be the smallest prime number dividing the order of G. Assume G has a normal subgroup H of order p. Show that H is contained in the center of G.

Proof. Let $G \curvearrowright H$ by the conjugation: $g \cdot h = ghg^{-1}$. This is a valid action since H is conjugation invariant (since it is normal in G). Note $h \in Z(G)$ if and only if $ghg^{-1} = h$ for all $g \in G$, i.e. h is a fixed point.

Note $\text{Orbit}(e) = \{e\} \lneq H$, and since the orbits partition H, for all $h \in H$, $\text{Orbit}(h) \lneq H$. Now, again, by the orbit-stabilizer theorem, $\text{Orbit}(h) = G/\text{Stab}(h)$, so $|\text{Orbit}(h)| \mid |G|$. But note since $|\text{Orbit}(h)| < p$ and p is the smallest prime dividing $|G|$, no prime divisor of $|G|$ can divide $|\text{Orbit}(h)|$. Hence, the only possibility is $|\text{Orbit}(h)| = 1$, i.e. h is a fixed point. □

Lemma 7 (Burnside's Lemma)**.** Let G be a finite group and X a finite set, and suppose $G \curvearrowright X$. Set, for each $g \in G$, $\text{Fix}(g) = \{x \in X \mid g \cdot x = x\}$. Then,

$$\#\text{Orbits} = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|$$

Proof. First, note

$$\#\text{Orbits} = \sum_{\substack{A \subset X \\ A \text{ orbit}}} 1 = \sum_{\substack{A \subset X \\ A \text{ orbit}}} \sum_{x \in A} \frac{1}{|A|}$$

Since orbits partition X, summing over all the said partitions, then over all element in the said partition is the same as just summing over all element of X. Also, in preparation, set for each $g \in G$ and $x \in X$, $\chi(g, x) = 1$ if $g \cdot x = x$ and 0 otherwise. Combining these, we get:

$$\begin{aligned}
\sum_{\substack{A \subset X \\ A \text{ orbit}}} \sum_{x \in A} \frac{1}{|A|} &= \sum_{x \in X} \frac{1}{|\text{Orbit}(x)|} \\
&= \sum_{x \in X} \frac{|\text{Stab}(x)|}{|G|} \\
&= \frac{1}{|G|} \sum_{x \in X} \sum_{g \in G} \chi(g, x) \\
&= \frac{1}{|G|} \sum_{g \in G} \sum_{x \in X} \chi(g, x) \\
&= \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|
\end{aligned}$$

□

Spring 2016 Problem 9: Show that if G is a finite group acting transitively on a set X with at least two elements, then there exists $g \in G$ which fixes no point of X.

Proof. Here, since G acts transitively, X has exactly one orbit, so $\#\text{Orbit} = 1$. So by the Burnside's lemma, $1 = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|$, or equivalently, $|G| = \sum_{g \in G} |\text{Fix}(g)| = |\text{Fix}(e)| + \sum_{\substack{g \in G \\ g \neq e}} |\text{Fix}(g)|$. But we know $\text{Fix}(e) = X$, and $|X| \geq 2$, so $|G| \geq 2 + \sum_{g \neq e} |\text{Fix}(g)|$. Now, assume for the sake of contradiction, that every $g \in G$ fixes at least one point, i.e. for all $g \in G$, $|\text{Fix}(g)| \geq 1$; then, we get $|G| \geq 2 + \sum_{g \neq e} 1 = 2 + |G| - 1 = |G| + 1$, a contradiction. □

Remark 6. It was suggested during the discussion that since $X \cong G/\text{Stab}(x)$ as G-sets, it's enough to choose $g \notin \text{Stab}(x)$. This is wrong for the following reason:

We know $h\text{Stab}(x)$ is fixed by g if and only if $gh\text{Stab}(x) = h\text{Stab}(x)$ if and only if $h^{-1}gh \in \text{Stab}(x)$ if and only if $g \in h\text{Stab}(x)h^{-1}$. So g has no fixed point if and only if for all $h \in G$, $g \notin h\text{Stab}(x)h^{-1}$. Note this requires more than just selecting $g \notin \text{Stab}(x)$ (unless $\text{Stab}(x)$ is normal, which is not necessarily true!).

Here's how to fix the argument: we can have G act on $\text{Stab}(x)$ by conjugation, with the stabilizer of $\text{Stab}(x)$ under this action equaling to $N_G(\text{Stab}(x)) \geq \text{Stab}(x)$. So this descends to an action $G/N_G(\text{Stab}(x))$ on $\text{Stab}(x)$. So $\cup_{h\in G} h\text{Stab}(x)h^{-1}$ is a union of at most $|G/N_G(\text{Stab}(x))| \leq |G/\text{Stab}(x)|$ many sets of size $|\text{Stab}(x)|$. But note the sets $h\text{Stab}(x)h^{-1}$ all share the element $e \in G$, so in fact, the union must have at most 1 less than $|\text{Stab}(x)||G/\text{Stab}(x)| = |G|$ many elements (the only exception is if $|G/N_G(\text{Stab}(x)| = |G/\text{Stab}(x)| = 1$, i.e. $|X| = 1$). So we can choose $g \notin \cup_{h\in G} h\text{Stab}(x)h^{-1}$.

Discussion 4 - Group Actions: Part 2 and Sylow Groups

Fall 2018 Problem 1: Let $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ be the quaternion group of order 8.

(1) Show that every non-trivial subgroup contains -1.

(2) Show that Q_8 does not embed in the symmetric group S_7 (as a subgroup).

Proof. For (1), suppose $H \leq Q_8$ which contains $g \neq 1$. If $g = -1$, then we're done. Otherwise, note $i^2 = j^2 = k^2 = -1$, so $g^2 = -1 \in H$.

For (2), suppose we have an embedding $\phi : Q_8 \hookrightarrow S_7$. Then, note the homomorphism ϕ corresponds to an action $\cdot$ given by $g \cdot m = \phi(m)$. Note $\text{Orbit}(m) \cong Q_8/\text{Stab}(m)$ by as Q_8-sets by orbit-stabilizer theorem. Since the orbit is at most size 7, $\text{Stab}(m)$ is a nontrivial subgroup. By part (1), it must contain -1. So for all $m \in \{1, 2, \ldots, 7\}$, $-1 \in \text{Stab}(m)$. But this means that for all m, $\phi(-1)(m) = (-1) \cdot m = m$, so $\phi(-1) = \phi(1) = \text{id}$, which contradicts that ϕ was an embedding. □

Fall 2018 Problem 2: Let G be a finitely generated group having a subgroup of finite index $n > 1$. Show that G has finitely many subgroups of index n and has a proper characteristic subgroup (*i.e.* preserved by all automorphisms) of finite index.

Proof. First, we prove that there are finitely many subgroups of index $\leq n$. Choose a subgroup $H \leq G$ of index n, and consider the action $G \curvearrowright G/H$. This induces a homomorphism $\phi : G \to S_{G/H} \cong S_n$. So let's analyze the number of homomorphisms from $G \to S_n$.

Lemma 8. Given a finitely generated group G and a finite group K, there are only finitely many homomorphisms from G to K.

Proof. Choose $g_1, g_2, \ldots, g_m$ which generates G. Then, note a homomorphism $\phi : G \to K$ is uniquely determined by where it sends $g_1, g_2, \ldots, g_m$. Expressed more formally, the map $\text{Hom}_{\text{Grp}}(G, K) \hookrightarrow K^m, \phi \mapsto (\phi(g_1), \phi(g_2), \ldots, \phi(g_m))$ is injective (note we are not saying the map is surjective - we do not claim that any choice of m-tuples of K induces a homomorphism $\phi : G \to K$). Since the latter set is finite, so is the former, but that's exactly what we were trying to prove. □

It follows there are only finitely many homomorphisms from $G \to S_n$. Now, given the homomorphism $G \to S_{G/H} \cong S_n$ induces by H, we can translate back to the group action $G \to [n]$ and thus, we get $H = \text{Stab}_\phi(1)$ (say in the bijection $G/H \to [n]$, we sent H to 1). So, we have a surjection $\text{Hom}_{\text{Grp}}(G, S_n) \twoheadrightarrow \{H \mid H \leq G, [G : H] \leq n\}$ given by $\phi \mapsto \text{Stab}_\phi(1)$. Since the former is finite, so should be the latter as well. In particular, we showed that there are only finitely many subgroups of index $\leq n$ (and hence $= n$) as desired.

Next, we show that there is a characteristic normal subgroup of finite index. Set

$$N = \bigcap_{\sigma \in \text{Aut}(G)} \sigma(H)$$

This group is clearly invariant under all automorphisms, so it remains to check that it is finite index. Observe that for all $\sigma \in \text{Aut}(G)$, $\sigma(H)$ also has index n. So by the previous part, the above intersection is actually a finite intersection, say, $H_1, H_2, \ldots, H_k$. Now, we know for any two groups H_1, H_2, $[G : H_1 \cap H_2] = [G : H_1] \cdot [H_1 : H_1 \cap H_2] \leq [G : H_1] \cdot [G : H_2]$. We can apply that to k many subgroups to get: $[G : N] \leq [G : H_1][G : H_2] \cdots [G : H_k] \leq n^k$, which is finite. □

For the remainder of the session, we begin solving qual problems that involve Sylow groups. We will state 1st-3rd Sylow theorems without proof.

Theorem 3 (1st Sylow Theorem)**.** Every finite group G has a p-Sylow subgroup for all prime divisors p of $|G|$.

Theorem 4 (2nd Sylow Theorem)**.** Any two p-Sylow subgroups are conjugates.

Theorem 5 (3rd Sylow Theorem)**.** Let n_p be the number of p-Sylow groups. Then, for any given Sylow p-group P,

$$n_p = [G : N_G(P)] \equiv 1 \bmod (p)$$

Fall 2017 Problem 1: Let G be a finite group, p a prime number, and S a Sylow p-subgroup of G. Let $N = \{g \in G \mid gSg^{-1} = S\}$. Let X and Y be two subsets of $Z(S)$ (the center of S) such that there exists $g \in G$ with $gXg^{-1} = Y$.

Show that there exists $n \in N$ such that $nxn^{-1} = gxg^{-1}$ for all $x \in X$.

Proof. Note for each $x \in X$, $nxn^{-1} = gxg^{-1}$ if and only if $g^{-1}nxn^{-1}g = g^{-1}nx(ng^{-1})^{-1}$. So n satisfies the above condition if and only if $g^{-1}n \in C_G(X)$ if and only if $n \in gC_G(X)$. So it suffices to show $N \cap gC_G(X) = N_G(S) \cap gC_G(X) \neq \varnothing$.

Recall that $n \in N_G(S)$ if and only if nS is a fixed point of the action $S \cap G/S$, so we want to find $n \in gC_G(X)$ so that nS is a fixed point. Consider the action $S \curvearrowright gC_G(X)/S$ where again, $gC_G(X)/S = \pi(gC_G(X))$ for $\pi : G \to G/S$. First, we check that this is a valid action: for any $s \in S$ and $gh \in gC_G(X)$, we want to show $sgh \in gC_G(X)$. Let $x \in X$, and set $y = gxg^{-1} \in Y$. Then

$$\begin{aligned} sghx(sgh)^{-1} &= sghxh^{-1}g^{-1}s^{-1} \\ &= sgxg^{-1}s^{-1} \\ &= sys^{-1} \\ &= y && \text{(this is true since } Y \subset Z(S)\text{)} \\ &= gxg^{-1} \end{aligned}$$

So it follows $sgh \in gC_G(X)$ as the conjugation by sgh results in conjugation by g for all $x \in X$.

Since $S \leq C_G(X)$ (because $X \subset Z(S)$), $|gC_G(X)/S| = |C_G(X)/S| \mid |G/S|$. In particular, $p \nmid |gC_G(X)/S|$ so it must have a fixed point nS. This is our desired $n \in N \cap C_G(S)$. □

Discussion 5 - Sylow Groups: Part 2

Fall 2020 Problem 1: Let $p < q < r$ be primes and G a group of order pqr. Prove that G is not simple and, in fact, has a normal Sylow r-subgroup.

Proof. Let us first prove that G is not simple. We'll do this by showing G has a normal p, q, or r Sylow subgroup. By the second Sylow theorem, a Sylow subgroup is normal if and only if it is the unique Sylow subgroup. So let n_p, n_q, n_r be the number of each Sylow subgroups - we want to show $n_p = 1$ or $n_q = 1$ or $n_r = 1$. Suppose not, i.e. $n_p, n_q, n_r > 1$.

By the Third Sylow's theorem, $n_r \mid pqr$ and $n_r \equiv 1 \bmod (r)$. So $n_r \mid pq$, so $n_r = 1, p, q$, or pq. Since $n_r > 1$, the only possibility is $n_r = pq$. With similarly analyses, we can conclude $n_p \mid qr$, $n_q \mid pr$ with $n_p \equiv \bmod (p)$ and $n_q \equiv \bmod (q)$, so $n_p \geq q$ and $n_q \geq r$.

Let $P_1, P_2, \ldots, P_q$ be q distinct Sylow q-subgroups, $Q_1, Q_2, \ldots, Q_r$ be r many distinct Sylow r-subgroups, and $R_1, R_2, \ldots, R_{pq}$ be pq many distinct Sylow r-subgroups.

Claim. Consider the collection of subgroups $\{P_i\}_{i=1}^{q} \cup \{Q_i\}_{i=1}^{r} \cup \{R_i\}_{i=1}^{pq}$. Any two distinct subgroups there have trivial intersection $\{e\}$.

Proof of the Claim. Let $A, B \in \{P, Q, R\}$. If $A \neq B$, then $|A_i \cap B_j| \mid \gcd(|A|, |B|) = 1$. If $A = B$, then for any $i \neq j$, $A_i \cap A_j \subsetneq A_i, A_j$, so it is a proper subgroup of a group of prime order; by Lagrange's theorem, it must be trivial. □

So, the union

$$\bigcup_{i=1}^{q} P_i \bigcup \bigcup_{i=1}^{r} Q_i \bigcup \bigcup_{i=1}^{pq} R_i = \bigsqcup_{i=1}^{q} (P_i - \{e\}) \bigsqcup \bigsqcup_{i=1}^{r} (Q_i - \{e\}) \bigsqcup \bigsqcup_{i=1}^{pq} (R_i - \{e\}) \bigsqcup \{e\}$$

So, the union of those subgroups have size at $(p-1)q + (q-1)r + (r-1)pq + 1 = pqr - pq + pq - q + qr - r = pqr + qr - q - r + 1 > pqr = |G|$. So we have a subset of G of size $> |G|$, a contradiction.

We conclude that $n_p = 1$, or $n_q = 1$, or $n_r = 1$. If we're given $n_r = 1$, then we've already proven that $R \trianglelefteq G$. So suppose $n_p = 1$ or $n_q = 1$, and in fact, without loss of generality, $n_p = 1$ ($n_q = 1$ case is dealt similarly). We have $P \trianglelefteq G$, so consider the quotient G/P of size qr. Choose an r-Sylow subgroup $\widetilde{K} \leq G/P$. This is a normal subgroup (why?). Take $K = \pi^{-1}(\widetilde{K}) \trianglelefteq G$ where $\pi : G \to G/P$ is the quotient map. Then, K is a normal subgroup of size pr, so it must also have a Sylow r-subgroup $R \trianglelefteq K \trianglelefteq G$ ($R \trianglelefteq K$ part is left as an exercise, similar to $\widetilde{K} \trianglelefteq G/P$ part). Normality isn't transitive, but in this case, $R \trianglelefteq G$, as we show in the following:

Claim. $R \trianglelefteq G$.

Proof of the Claim. Let $g \in G$. Then, $gRg^{-1} \leq gKg^{-1}$. Since $K \trianglelefteq G$, $gKg^{-1} = K$, so gRg^{-1} is another r-Sylow subgroup of K. But since $R \trianglelefteq K$, R is the unique Sylow r-subgroup, so in fact, $R = gRg^{-1}$. □

□

Spring 2018 Problem 9: Show that there is no simple group of order 616.

Proof. Factor $616 = 2^3 \times 7 \times 11$. Once again, assume we have a group G of order 616 which is simple, so that $n_2, n_7, n_{11} > 1$. We have $n_{11} \mid 2^3 \times 7$ and $n_{11} \equiv 1 \bmod (11)$, so $n_{11} = 56$. We have $n_7 \mid 2^3 \times 11$ and $n_7 \equiv 1 \bmod (7)$, so $n_7 = 8$ or 22 (in particular, $n_7 \geq 8$). We have $n_2 \geq 2$.

□

Fall 2017 Problem 2: Let G be a finite group of order a power of a prime number p. Let $\Phi(G)$ be the subgroup of G generated by elements of the form g^p for $g \in G$ and $ghg^{-1}h^{-1}$ for $g, h \in G$.

Show that $\Phi(G)$ is the intersection of the maximal proper subgroups of G.

Discussion 6 - Solvability

Spring 2019 Problem 1: Let G be a finite solvable group, and $1 \neq N \subset G$ be a minimal normal subgroup. Prove that there exists a prime p such that N is either cyclic of order p or a direct product of cyclic groups of order p.

Fall 2021 Problem 9: The *outer automorphism group* of a group H is the quotient of the group of automorphisms of H by the subgroup of inner automorphisms. It is known that the outer automorphism group of every finite simple group is solvable. Using that, show that if G is a finite group with a normal subgroup N such that both N and G/N are nonabelian simple groups, then G is isomorphic to the product group $N \times (G/N)$.

Discussion 7 - Presentation of Groups, how to Solve Hard Group Theory Problems

Theorem 6. ddddd