

Frank Moore
Algebra 901 Notes
Professor: Tom Marley

Let G be a group, H a subgroup, and let G act on G/H via $g \cdot xH := (gx)H$ where juxtaposition is the group operation. Note that $g \in G_{xH} \Leftrightarrow gxH = xH \Leftrightarrow x^{-1}gx \in H \Leftrightarrow g \in xHx^{-1}$. So we have that the stabilizer, G_{xH} is xHx^{-1} .

Remember that every group action induces a group homomorphism from the group to the permutations of the set, so we have:

$$\phi : G \rightarrow \text{Perm}(G/H).$$

The kernel of ϕ is $\ker \phi = \bigcap_{x \in G} xHx^{-1}$. This action is faithful $\Leftrightarrow \bigcap_{x \in G} xHx^{-1} = \{1\}$.

Remarks:

1. So if H is normal, the action is faithful $\Leftrightarrow H = \{1\}$, since $\ker(\phi) = H$ for H normal. In particular ϕ is injective because ϕ becomes $G \hookrightarrow \text{Perm}(G)$. Therefore G is isomorphic to a subgroup of permutations of G (Recall if $|X| = n$ then $\text{Perm}(X) \cong S_n$). Hence, if $|G| = n$, then G is isomorphic to a subgroup of S_n .
2. Since $\bigcap_{x \in G} xHx^{-1} = \ker \phi$, we see that $\bigcap_{x \in G} xHx^{-1} \triangleleft G$.

Exercise: Show that $\bigcap_{x \in G} xHx^{-1}$ is the largest normal subgroup contained in H .

Proposition: Let p be the smallest prime dividing $|G|$. Suppose \exists a subgroup H with $[G : H] = p$. Then H must be normal.

Proof: So we have the Cayley map:

$$\phi : G \rightarrow \text{Perm}(G/H) \cong S_p$$

Let $K = \ker \phi \subseteq H$. So we then have the induced map

$$\begin{aligned} \bar{\phi} : G/K &\hookrightarrow S_p \text{ is injective} \\ gK &\mapsto \phi(g) \end{aligned}$$

So, since $G/K \cong$ to some subgroup of S_n , $|G/K|$ divides $|S_p|$ by Lagrange's theorem. Hence $|G/K|$ divides $p!$. Therefore,

$$[G : K] = [G : H][H : K]$$

where we have $[G : H]$ by assumption. Thus, $[H : K]$ divides $(p-1)!$, but it also divides $|G|$. But p was the smallest prime dividing $|G|$ by assumption, so we have that $[H : K] = 1$. Thus, $H = K \triangleleft G$.

Corollary: If $[G : H] = 2$ then $H \triangleleft G$.

Back to Conjugation Example of Group Actions: Let G act on itself via $g \cdot x = gxg^{-1}$. So, the orbit $Gx = \{gxg^{-1} | g \in G\}$. These orbits are called **conjugacy classes** here. Notice that since the

orbits partition the group, our conjugacy classes partition G .

Also notice that

$$\begin{aligned} g \in G_x &\Leftrightarrow gxg^{-1} = x \\ &\Leftrightarrow gx = xg \\ &\Leftrightarrow g \in C_G(x) = \{g \in G \mid gx = xg\} \end{aligned}$$

(where $C_G(x)$ is the centralizer of x in G). Recall from previous lecture that $|Gx| = [G : G_x] = [G : C_G(x)]$ in this case.

Hence we have

$$\begin{aligned} |Gx| = 1 &\Leftrightarrow G = C_G(x) \\ &\Leftrightarrow x \in Z(G) = \{g \in G \mid ga = ag \quad \forall a \in G \end{aligned}$$

(where $Z(G)$ denotes the center of the group.)

So we may refine our previous counting formula a little more to give better insight into the problem by removing all those orbits of the elements that are in the center of the group.

$$\begin{aligned} |G| &= \sum_x [G : C_G(x)] \\ &= |Z(G)| + \sum_x [G : C_G(x)] \end{aligned}$$

where x runs over all distinct conjugacy classes in the first sum and all distinct conjugacy classes having 2 or more elements in the second sum. The above is known as the class formula.

Definition: Let p be a prime. A group of order p^n for some $n \geq 1$ is called a p -group.

Proposition: If G is a p -group, then $Z(G) \neq \{1\}$.

Proof: If $Z(G) = \{1\}$, then $|G| = p^n = 1 + \sum_i p^{\alpha_i}$ where $\alpha_i \geq 1$ because all orders of subgroups of G divide the order of G and $C_G(x)$ is a subgroup for all $x \in G$, so $[G : C_G(x)] = p^\alpha$ some $\alpha \geq 1$. If we mod out by p , we get that zero is equivalent to 1 mod p , a contradiction.

Exercise: If $G/Z(G)$ is cyclic, then G is abelian.

Corollary: If $|G| = p^2$, p a prime, then G is abelian.

Proof: If $Z(G) \neq G$ then $|Z(G)| = p$ by Lagrange's, but that makes $|G/Z(G)| = p$. Therefore $G/Z(G)$ is cyclic, which in turn implies G is abelian, a contradiction.

Lemma: Let G be a finite abelian group and p a prime dividing $|G|$. Then G has an element of order p .

Proof: Induct on $|G|$. If $|G| = p$, then G is cyclic. Suppose $|G| > p$. Let $x \in G, x \neq 1$. We shall break this problem up into two cases:

1. If $p \mid o(x) = n$, then $o(x^{n/p}) = p$ and we are done.

2. If $p \nmid o(x) = n$, then $|G/\langle x \rangle| = \frac{|G|}{n} < |G|$. Also, p divides $|G/\langle x \rangle|$ since $p \nmid n$. By our inductive hypothesis, $|G/\langle x \rangle|$ has an element $\bar{y} = y\langle x \rangle$ of order p . Therefore we have $o(\bar{y})|o(y) = m$. So, $o(y^{m/p}) = p$.

Some notes on normal subgroups:

1. Subgroups of G/H are of the form L/H where $H \subseteq L \subseteq G$.
2. $L/H \triangleleft G/H \Leftrightarrow L \triangleleft G$
3. If L/H is normal, then $(G/L)/(L/H) \cong G/H$.

Sylow's First Theorem: Let G be a finite group and suppose p^α divides $|G|$ for some $\alpha \geq 0$. Then G has a subgroup of order p^α . So this subgroup is then a p -group.

Proof: If $|G| = p^\alpha$, we are done, and assume that $|G| > p^\alpha$. We can create the following cases:

1. Suppose p divides $|Z(G)|$. The center is abelian, so by the previous lemma we know $\exists x \in Z(G) \mid o(x) = p$. Let $H = \langle x \rangle$. H is then normal in G since $x \in Z(G)$. Then G/H is a group, and $|G/H| = \frac{|G|}{p} < |G|$. Therefore $p^{\alpha-1}$ divides $|G/H|$ because p^α divided $|G|$ and $|H| = p$. Hence, by induction, G/H has a subgroup of order $p^{\alpha-1}$. So let L be a subgroup of G containing H such that $|L/H| = p^{\alpha-1}$. Therefore, $|L/H| = |L|/|H|$ which implies $|L| = |H| \cdot p^{\alpha-1} = p^\alpha$.
2. Suppose $p \nmid |Z(G)|$. Then by the class formula:

$$|G| = |Z(G)| + \sum_x [G : C_G(x)]$$

we must have that $p \nmid [G : C_G(x)] \forall x \notin Z(G)$ by easily reducing mod p and looking at the residues. Therefore, p^α does divide $|C_G(x)| < |G|$ (why?), and by induction, $C_G(x)$ has a subgroup of order p^α , so G does as well.