Group Theory

Lecture 9, Sunday December 18, 2022
Ari Feiglin

If C is a cube, which is a graph, recall that $\mathrm{Aut}(C)$ is the set of automorphisms of the cube. We can think of the cube as either a set of 8 vertices, or 6 faces, or 12 edges. Notice that if we determine the placement of two vertices in a automorphism, that determines the rest of them. So we have 8 places to place the first vertex, and this vertex has three neighbors so we have 3 places to put the next vertex, so all in all we have 24 automorphisms. If we think in terms of faces, we have 6 places to put the first face, and we can rotate it (or rather the other faces) 4 times, which gives 24 automorphisms. And lastly if we think in terms of edges, we can flip an edge, giving 24 automorphisms. And as it turns out $\mathrm{Aut}(C) \cong S_4$.

9.1 More Group Actions

Notice that by a previous proposition:

$$\left[G : G_x\right] = |G \cdot x|$$

Which means that

$$|G| = |G \cdot x| \cdot |G_x|$$

and therefore the orders of both the orbit and stabilizer of x divide the order of G.
Notice that we can define the following group actions of G on itself:

- $g \cdot x = gx$, we used this in our proof of Cayley's theorem.
- $g \cdot x = xg^{-1}$.
- $g \cdot x = gxg^{-1}$. This specific group action has some interesting properties, so we will show that it is indeed a group action: $e \cdot x = exe^{-1} = x$ and $g \cdot (h \cdot x) = g \cdot (hxh^{-1}) = ghxh^{-1}g^{-1} = ghx(gh)^{-1} = (gh) \cdot x$.

Notice that under the third group action, the orbit of an element $x \in G$ is $G \cdot x = \left\{gxg^{-1} \;\middle|\; g \in G\right\} = [x]$ the equivalence class of all conjugates of x. And its stabilizer we denote $C_G(x) = G_x = \left\{g \in G \;\middle|\; gxg^{-1} = x\right\} = \{g \in G \mid gx = xg\}$ is the set of all elements $g \in G$ which commute with x. Thus

$$|[x]| = \left[G : C_G(x)\right]$$

Definition 9.1.1:

We define for every $x \in G$ the center of x, $C_G(x)$, to be the stabilizer of x under the conjugate group action of G.

Now for example take $\begin{pmatrix}1 & 2 & 3\end{pmatrix} \in S_4$, its conjugacy class is the set of all 3-cycles $\begin{pmatrix}i & j & k\end{pmatrix}$ of which there are $\frac{4\cdot 3\cdot 2}{3}$ (we have 4 choices for i, 3 for j, 2 for k, and we can rotate our choices and get the same cycle three times), which is 8. And so $\left[G : C_G(x)\right] = 8$ and so $|C_G(x)| = \frac{|G|}{8} = \frac{4!}{8} = 3$ and since $\left\langle\begin{pmatrix}1 & 2 & 3\end{pmatrix}\right\rangle = 3$ this means that $C_G(x) = \begin{pmatrix}1 & 2 & 3\end{pmatrix}$.
If G acts on X and $x, y \in X$ are in the same orbit, which means that there is a g_0 such that $y = g_0 \cdot x$. Notice then that

$$\begin{aligned} G_y = \{g \in G \mid g \cdot y = y\} &= \{g \in G \mid g \cdot (g_0 \cdot x) = g_0 \cdot x\} = \{g \in G \mid gg_0 \cdot x = g_0 \cdot x\} \\ &= \left\{g \in G \;\middle|\; g_0^{-1}gg^{-1} \cdot x = x\right\} = \left\{g \in G \;\middle|\; g_0^{-1}gg_0 \in G_x\right\} = \left\{g \in G \;\middle|\; g \in g_0 G_x g_0^{-1}\right\} \end{aligned}$$

And thus

$$G_y = g_0 G_x g_0^{-1}$$

Recall that if $H \leq G$ then $gHg^{-1} \leq G$, so we can define an action of G on its set of subgroups via conjugation, that is

$$g \cdot H = gHg^{-1}$$

In this case the orbit of H is the set of all conjugate subgroups of H, there's not much more we can discuss here. We will define $N_G(H)$ to be the stabilizer of H:

$$N_G(H) = \left\{g \in G \;\middle|\; gHg^{-1} = H\right\} = \{g \in G \mid gH = Hg\}$$

Definition 9.1.2:

For $H \leq G$ we define the **normalizer** of H, $N_G(H)$ to be its stabilizer under the conjugate group action over the set of subgroups of G.

Proposition 9.1.3:

$N_G(H)$ is the largest subgroup of G where H is normal in $N_G(H)$.

Proof:

Since $N_G(H)$ is a stabilizer, it is a subgroup, and it is trivial to see that $H \leq N_G(H)$ since $hH = Hh$ for every $h \in H$. And if $H \trianglelefteq K$ then if $k \in K$, it must be that $kH = Hk$ by the definition of normalcy and therefore $k \in N_G(H)$ so $K \leq N_G(H)$.

■

This means that H is normal in G if and only if $N_G(H) = G$. Also notice that if G is abelian both conjugate group actions (over G and the set of subgroups of G) are trivial.
And by definition, the number of subgroups of G which are conjugate to H is equal to the index of $N_G(H)$. And since $\left[G : H\right] = \left[G : N_G(H)\right] \cdot \left[N_G(H) : H\right]$, the order of the conjugacy class of H divides $\left[G : H\right]$.

Definition 9.1.4:

For $H \leq G$ we define its **center** to be:

$$C_G(H) = \{g \in G \mid \forall h \in H : gh = hg\} = \bigcap_{h \in H} C_G(h)$$

Note that as the intersection of subgroups, $C_G(H)$ itself is a subgroup.

Definition 9.1.5:

We define the **center** of a group G to be

$$Z(G) = C_G(G) = \{g \in G \mid \forall a \in G : ag = ga\}$$

Notice that $Z(G) \trianglelefteq G$ since for every $a \in G$ and for every $g \in Z(G)$ we have that $aga^{-1} = aa^{-1}g = g \in Z(G)$. And $Z(G)$ is abelian since if $a \in Z(G)$ and $b \in Z(G)$, since $b \in G$ we have that $ab = ba$. And for every $a \in G$ since a commutes with every element in $Z(G)$, $\langle Z(G), a\rangle$ is abelian.

Proposition 9.1.6:

If ${}^{G}/_{Z(G)}$ is cyclic then G is abelian (and in particular ${}^{G}/_{Z(G)} \cong \{e\}$).

Proof:

Suppose ${}^{G}/_{Z(G)} = \langle aZ(G)\rangle$. And since the quotient group partitions G, we have that:

$$G = \dot{\bigcup} a^i Z(G) = \langle Z(G), a\rangle$$

which we know is abelian, and therefore G is abelian.

■

Suppose $H \leq G$ (not necessarily normal), we define a group action of G on ${}^{G}/_{H}$ by:

$$g \cdot (aH) = gaH$$

This is indeed a group action since $e \cdot (aH) = eaH = aH$ and $g \cdot (h \cdot aH) = ghaH = (gh) \cdot (aH)$.

Let $k = [G : H]$, then by this group action we have a homomorphism $\varphi\colon G \longrightarrow S_{G/H} \cong S_k$. Let us take a moment to consider the stabilizer of cosets: the stabilizer of H is H itself, and the stabilizer of aH is

$$G_{aH} = \{g \in G \mid g \cdot aH = aH\} = \left\{g \in G \;\middle|\; a^{-1}gaH = H\right\} = \left\{g \in G \;\middle|\; a^{-1}ga \in H\right\} = aHa^{-1}$$

And the orbit of H is ${}^{G}\!/_{H}$ since $a \cdot H = aH$. In this case we get that $|G \cdot H| = \left|{}^{G}\!/_{H}\right| = \left[G : G_H\right] = \left[G : H\right]$ which we know. We know that

$$\operatorname{Ker}\varphi = \{g \in G \mid \forall x \in X : g \cdot x = x\} = \bigcap_{x \in X} G_x$$

So in this case

$$\operatorname{Ker}\varphi = \bigcap_{a \in G} G_{aH} = \bigcap_{a \in G} aHa^{-1}$$

Definition 9.1.7:

If $H \leq G$ we define the core of H to be the kernel of the homomorphism induced by the group action of G on ${}^{G}\!/_{H}$ as defined above. That is

$$\operatorname{Core}(H) = \bigcap_{a \in G} aHa^{-1}$$

Proposition 9.1.8:

$\operatorname{Core}(H)$ is the largest normal group in G contained in H.

Proof:

Since the core of a group is defined as the kernel of a homomorphism, it is necessarily normal. Suppose $K \trianglelefteq G$ and $K \subseteq H$ then for every $a \in G$ we must have that $K = aKa^{-1} \subseteq aHa^{-1}$ and thus $K \subseteq \operatorname{Core}(H)$.

■

What this means is that if H is normal, $\operatorname{Core}(H) = H$.
By the first isomorphism theorem, since $\varphi\colon G \longrightarrow S_{[G:H]}$ we have that:

$${}^{G}\!/_{\operatorname{Core}(H)} = {}^{G}\!/_{\operatorname{Ker}\varphi} \cong \operatorname{Im}\varphi \leq S_{[G:H]}$$

And thus there is a monomorphism

$${}^{G}\!/_{\operatorname{Core}(H)} \longrightarrow S_{[G:H]}$$

We summarize this result in the following theorem:

Theorem 9.1.9:

If H is a subgroup of G then there is a monomorphism

$${}^{G}\!/_{\operatorname{Core}(H)} \longrightarrow S_{[G:H]}$$

This is useful since the core of a subgroup may be significantly smaller than the subgroup itself, and so ${}^{G}\!/_{\operatorname{Core}(H)}$ is larger than ${}^{G}\!/_{H}$, and so $S_{[G:H]}$ is smaller than $S_{[G:\operatorname{Core}(H)]}$.

Proposition 9.1.10:

If G has a subgroup with a finite index, it has a normal subgroup with a finite index.

Proof:

Suppose H has a finite index, then since ${}^{G}\!/_{\operatorname{Core}(H)}$ is isomorphic to a subgroup of $S_{[G:H]}$, its order must divide $[G : H]!$ and therefore must be finite.

■

If we define for every $g \in G$ the homomorphism:

$$\gamma_g \colon G \longrightarrow G, \quad \gamma_g(x) = gxg^{-1}$$

This is a homomorphism since $\gamma_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \gamma_g(x)\gamma_g(y)$. And notice that

$$\left(\gamma_g \circ \gamma_h\right)(x) = \gamma_g\left(\gamma_h(x)\right) = ghxh^{-1}g^{-1} = (gh)x(gh)^{-1} = \gamma_{gh}(x)$$

And so $\gamma_g \circ \gamma_h = \gamma_{gh}$ which means $\gamma_g^{-1} = \gamma_{g^{-1}}$ so γ_g is a bijection and thus an automorphism.

Definition 9.1.11:

We define the **inner automorphism group** of the group G to be:

$$\mathrm{Inn}(G) = \{\gamma_g \mid g \in G\} \leq \mathrm{Aut}(G)$$

This is a group since $\gamma_e = \mathrm{id}$ and as we showed above it is closed under inversions and compositions. We can define the canonical epimorphism

$$\Gamma \colon G \longrightarrow \mathrm{Inn}(G)$$

by $\Gamma(g) = \gamma_g$. This is obviously surjective and it is a homomorphism since $\Gamma(gh) = \gamma_{gh} = \gamma_g\gamma_h = \Gamma(g)\Gamma(h)$. Its kernel is

$$\operatorname{Ker}\Gamma = \{g \in G \mid \gamma_g = \Gamma(g) = \mathrm{id}\} = \left\{g \in G \,\middle|\, \forall x : gxg^{-1} = x\right\} = Z(G)$$

And thus by the first isomorphism theorem:

$$G/\operatorname{Ker}\Gamma = G/Z(G) \cong \mathrm{Inn}(G)$$

Now suppose $\sigma \in \mathrm{Aut}(G)$, then notice

$$\sigma\gamma_g\sigma^{-1}(x) = \sigma\left(g\sigma^{-1}(x)g^{-1}\right) = \sigma(g)x\sigma(g)^{-1} = \gamma_{\sigma(g)}$$

Thus for every $\sigma \in \mathrm{Aut}(G)$, $\sigma\,\mathrm{Inn}(G)\sigma^{-1} \subseteq \mathrm{Inn}(G)$ and so $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

Definition 9.1.12:

The **outer group of automorphisms** of G is defined to be

$$\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$$

(note that the outer group does not contain automorphisms rather equivalence classes of automorphisms).

A brief overview of the groups we have defined:

$$\begin{tikzcd}
 & 1 \arrow[d] & & & \\
 & Z(G) \arrow[d] & & & \\
 & G \arrow[d] & & & \\
1 \arrow[r] & \mathrm{Inn}(G) \arrow[r] \arrow[d] & \mathrm{Aut}(G) \arrow[r] & \mathrm{Out}(G) \arrow[r] & 1 \\
 & 1 & & &
\end{tikzcd}$$

The following are interesting relations which are left as a proof to the reader

(1) $\mathrm{Aut}(\mathbb{Z}_n) \cong \mathrm{Euler}(n)$

(2) $\mathrm{Aut}\left(\mathbb{Z}_p^n\right) \cong \mathrm{GL}(\mathbb{Z}_p)$ (this is interesting since we don't require the automorphisms to preserve linear structure)

(3) $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_4) \cong D_4$ (annoying)

(4) $\mathrm{Aut}(S_n) \cong S_n$

(5) $\mathrm{Out}(S_n) \cong \{e\}$ if $n \neq 6$ and $\mathbb{Z}_2$ if $n = 6$.