Math 210A Lecture 12 Notes

Daniel Raban

October 24, 2018

1 Automorphisms, Lagrange's Theorem, Isomorphism Theorems, and Semidirect Products

1.1 Automorphisms and Lagrange's theorem

Last time, we had $\gamma : G \to \mathrm{Inn}(G)$ given by $g \mapsto \gamma_g$, where $\gamma_g(x) = gxg^{-1}$. Then $\ker(\gamma) = Z(G)$, so $G/Z(G) \cong \mathrm{Inn}(G)$.

Theorem 1.1 (Lagrange)**.** *Let $H \leq G$, where H and G are finite, then $|G| = [G : H]|H|$. Also, if $K \leq H \leq G$, then $[G : K] = [G : H][H : K]$.*

Proof. $G = \coprod gH$, where the g are a set of coset representatives. Then, since $H \to gH$ given by $h \mapsto gh$ is a bijection, $G = (\#\text{ left cosets})|H| = [G : H]|H|$. $\square$

Definition 1.1. The **order** of $g \in G$ is the smallest $n \geq 1$ such that $g^n = e$. The **exponent** of G is the smallest n such that $g^n = e$ for all $g \in G$.

Example 1.1. $\mathrm{Aut}(D_n) \cong \mathrm{Aff}(\mathbb{Z}/n\mathbb{Z}) \leq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, where

$$\mathrm{Aff}(\mathbb{Z}/n\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : a \in (\mathbb{Z}/n\mathbb{Z})^\times, b \in \mathbb{Z}/n\mathbb{Z} \right\}.$$

The map is $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \mapsto \phi_{a,b}$, where $\phi_{a,b}(r) = r^a$ and $\phi_{a,b}(s) = r^b s$. Let's check that this is an isomorphism.

First, we check that we can use the presentation $D_n = \langle r, s \mid r^2, s^2, rsrs \rangle$. Let $\Phi : F_{\{r,s\}} \to D_n$ be a homomorphism such that $\Phi(f) = r^a$ and $\Phi(s) = r^b s$.

$$\begin{tikzcd} F_{\{r,s\}} \arrow[r] \arrow[d] & D_n \\ D_n \arrow[ur, dashed, "\phi_{a,b}"'] & \end{tikzcd}$$

Then we can check that this agrees.

$$\Phi(r^n) = r^{an} = e$$
$$\Phi(s^2) = r^b s r^b s = r^b r^{-b} = e$$
$$\Phi(rsrs) = r^{a+b} s r^{a+b} s = e$$

As an exercise, check that this map is injective.

In this example, $\langle r \rangle$ was a characteristic subgroup.

Definition 1.2. A subgroup is **characteristic** if it is preserved by all automorphisms ($\varphi(N) \leq N$ for all φ).

Remark 1.1. Even if $K \trianglelefteq N$ and $N \trianglelefteq G$, we cannot conclude that $K \trianglelefteq G$. However,if $K \leq N$ is characteristic and $N \leq G$ is characteristic, then $K \leq G$ is characteristic.

Lemma 1.1. *Let G be a group.*

1. *$Z(G)$ is characteristic in G.*
2. *$G' = [G, G] = \langle [x, y] \mid x, y \in G \rangle$ is characteristic in G.*

Proof. Let's prove the second statement. If ϕ is an automorphism, $\varphi([x, y]) = [\varphi(x), \varphi(y)] \in G'$. $\square$

1.2 The second and third isomorphism theorems

For $H, K \leq G$, let $HK = \{hk : h \in H, k \in K\}$. This may not be a subgroup of G. When is it a subgroup?

Lemma 1.2. *$HK \leq G$ if and only if $HK = KH$.*

Proof. If $KH \subseteq HK$, then $kh \in HK$ for all $k \in K, h \in K$. So $KH \subseteq HK$. This means that for $k \in K, h \in H$, there exists $h' \in H$ and $k' \in K$ such that $kh = h'k'$. So then $h_1 k_1 \cdots h_r k_r = h_k$ for some $h \in H$ and $k \in K$ by moving all the ks to the right. So $HK \leq G$.

Now observe that $(h^{-1}k^{-1}) = (kh)^{-1} \in HK$. So if HK is group, then $HK = KH$. $\square$

Theorem 1.2 (2nd isomorphism theorem)**.** *Let $K \trianglelefteq G$ and $H \leq G$. Then $HK/K \cong H/(H \cap K)$.*

Proof. Let $\varphi : H \to HK/K$ be $\varphi(h) = hK$. This is surjective, and $\ker(\varphi) = H \cap K$. Now apply the first isomorphism theorem. $\square$

Theorem 1.3 (3rd isomorphism theorem)**.** *Let $K \trianglelefteq G$, $H \trianglelefteq G$, and $K \leq H$. Then $G/H \cong (G/K)/(H/K)$.*

Proof. Let $\pi(gK) = gH$. This is a surjective homomorphism. Then $\ker(\pi) = \{gK : gH = H\} = H/K \leq G/K$. Then use the 1st isomorphism theorem. $\square$

1.3 Semidirect products

Let H, N be groups with a homomorphism $H \to \mathrm{Aut}(N)$.

Definition 1.3. The **(external) semidirect product** of N and H is $N \rtimes_\varphi H = N \times H$ with the group operation

$$(n,h)(n',h') = (n\varphi(h)(n'), hh').$$

Let's check that this is a group:

1. The identity is (e,e).
2. Inverses are given by $(n,h)^{-1} = (\phi(h^{-1})(n^{-1}), h^{-1})$.
3. Associativity is left as an exercise.

How does conjugation work in the semidirect product? We can identify $N \leq N \rtimes_\varphi H$ and $H \leq N \rtimes_\varphi H$ by $n \mapsto (n,e)$ and $h \mapsto (e,h)$. Then $NH = N \rtimes_\varphi H$. Then

$$hnh^{-1} = (e,h)(n,e)(e,h^{-1}) = (\phi(h)(n),h)(e,h^{-1}) = (\phi(h)(n),e)$$

Example 1.2. $\mathrm{Aff}(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z} \rtimes_\varphi (\mathbb{Z}/n\mathbb{Z})^\times$. The isomorphism is $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \mapsto (b,a)$. Here, $\varphi(a)(b) = ab$.

Example 1.3. $D_n \cong \mathbb{Z}/n\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$, where $\varphi(1)(a) = -a$.

Definition 1.4. Let $N \trianglelefteq G$ and $H \leq G$ be such that $N \cap H = \{e\}$ and $NH = G$. Then G is the **internal semidirect product** $N \rtimes H$ of N and H.

Really, these are the same thing. $G = N \rtimes H \cong N \rtimes_\varphi H$, where $\varphi(h)(n) = hnh^{-1}$.