Lecture XXII: Semi-direct Products

§22.1 General 3rd Isomorphism Theorem

Recall In §9.3 we discussed the 3rd Isomorphism Theorem for groups:

Theorem: Given $N \trianglelefteq G$, let $H \trianglelefteq G$ with $N \subseteq H$. Then:

(1) $H/N \trianglelefteq G/N$ and (2) $G/H \simeq \dfrac{G/N}{H/N}$

Q: What can we say if $N \not\subseteq H$ or if $H \not\trianglelefteq G$?

Lemma: Let $N \trianglelefteq G$ and $H \leq G$. Then, the set $H\cdot N := \{hn : h \in H, n \in N\}$ satisfies (1) $H\cdot N = N\cdot H \leq G$

(2) $H \subseteq H\cdot N$, $N \trianglelefteq H\cdot N$

Proof:
- We show $H\cdot N = NH$ by double-inclusion.
- $\forall h \in H, n \in N$: $h\cdot n = (hnh^{-1})h \in NH$ because $N \trianglelefteq G$ $\Rightarrow H\cdot N \subseteq N\cdot H$

  $nh = h(h^{-1}n\,h) \in HN$ ——— $\Rightarrow NH \subseteq H\cdot N$
- We check $HN \leq G$ by using Lemma §2.2

  (1) $e = e\cdot e \in HN \Rightarrow HN \neq \emptyset$

  (2) $h_1n_1,\ h_2n_2 \in HN$ $(h_i \in H, n_i \in N)$ $\overset{?}{\Rightarrow} (h_1n_1)(h_2n_2)^{-1} \in HN$

Indeed: $(h_1n_1)(h_2n_2)^{-1} = h_1n_1n_2^{-1}h_2 = \underbrace{(h_1h_2)}_{\in H}\underbrace{(h_2^{-1}n_1n_2^{-1}h_2)}_{\in N} \in H\cdot N$ $(n_1n_2^{-1} \in N \trianglelefteq G)$ ✓

- $N \subseteq H\cdot N$ because $n = e\cdot n \in H\cdot N$ $\forall n \in N$
- $H \subseteq H\cdot N$ because $h = h\cdot e \in H\cdot N$ $\forall h \in H$
- $\forall h \in H, n \in N, x \in N$: $hnx(hn)^{-1} = h(\underbrace{nxn^{-1}}_{\in N})h^{-1} \in N \Rightarrow N \trianglelefteq H\cdot N$ □

Using the Lemma we can generalize the Third Iso Theorem

Theorem (Generalized Third Isomorphism Theorem):

Let G be a group, $N \trianglelefteq G$ a normal subgroup and $H \leq G$ a subgroup.

Then (1) $H \cap N \trianglelefteq H$

(2) $\varphi: H/H\cap N \longrightarrow H\cdot N/N$ is a group isomorphism

$h(H\cap N) \longmapsto hN$

<u>Proof:</u> By the Lemma, we can consider the group $G' = H\cdot N$. Then G'/N is a group.

First, we show (1). Pick $h \in H$ and $x \in H\cap N$. Then:

$$\underset{(x\in H)}{h x h^{-1} \in H} \cap \underset{(x\in N\trianglelefteq G)}{hNh^{-1}} = H\cap N$$

So $H\cap N \trianglelefteq H$.

To show (2) we must prove φ is well-defined & that it is a group isomorphism.

• <u>φ is well-defined</u>, $h(H\cap N) = x(H\cap N)$ for $h, x \in H \iff x^{-1}h \in H\cap N$.

Now: $hN \overset{?}{=} xN \iff x^{-1}h \in N$.

Since $x^{-1}h \in H\cap N \subseteq N$, the result follows.

• <u>φ is a group homomorphism:</u> $\varphi(h(H\cap N)\, h'(H\cap N)) \underset{\text{gp operation in } H/H\cap N}{=} \varphi((hh')H\cap N) = hh'N$

$\underset{\text{group operation in } G'}{=} hN\, h'N = \varphi(h(H\cap N))\ \varphi(h'(H\cap N))$ $\forall h, h' \in H$.

• <u>φ is surjective:</u> Given $h \in H$, $n \in N$ $(hn)N = h(nN) = hN = \varphi(h(H\cap N))$

So $\operatorname{Im}\varphi = H\cdot N/N$

• <u>φ is injective:</u> $h(H\cap N) \in \operatorname{Ker}\varphi \iff hN = eN \iff h \in N$

Since $h \in H$ by construction we conclude: $h(H\cap N) \in \operatorname{Ker}\varphi \iff h \in H\cap N$, i.e. $h(H\cap N) = \bar{e}$ in $H/H\cap N$. □

<u>Remark:</u> φ is obtain as $\bar{f}$ for $f = H \hookrightarrow HN \xrightarrow{\pi|_{HN}} HN/N$ group homomorphism

$h \longmapsto hN$

$\operatorname{Ker} f = H\cap N$ and f is surjective. By the 1st Isomorphism Theorem:

$\bar{f}: H/\operatorname{Ker} f \xrightarrow{\sim} HN/N$ is an iso.

⚠ Even though $H \simeq G/N$ and $HN = G$, it is not true that

$G \simeq N \times G/N$ if $N\times G/N$ is endowed with the standard coordinatewise group structure. Next time, we will define a "funky" operation on $N\times G/N$ that will make
$$N \times G/N \longrightarrow G$$
$$(n, hN) \longmapsto nh$$
a group isomorphism.

§22.2 Semi-direct Products:

Definition: We say a group G is a semi-direct product of H and N if
(1) $H \leq G$ and $N \trianglelefteq G$
(2) $HN = NH = G$
(3) $H \cap N = \{e\}$

Write $G = N \rtimes H$

Remark: If G is a semi-direct product of H & N, by Theorem §22.1 we conclude

$$\begin{aligned} H &\xrightarrow{\sim} G/N \\ h &\longmapsto hN \end{aligned}$$

Examples: ① $G = D_{2n}$ $\quad H = \langle s \rangle \leq G \quad H \simeq \mathbb{Z}/2\mathbb{Z}$

$N = \langle r \rangle \trianglelefteq G \quad N \simeq \mathbb{Z}/n\mathbb{Z}$

② $G = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} : a, b, d \in \mathbb{C},\ ad \neq 0 \right\}$ upper triangular matrices $\quad G \subseteq GL_2(\mathbb{C})$

$H = \left\{ \begin{bmatrix} a_1 & 0 \\ 0 & a_2 \end{bmatrix} : a_1, a_2 \in \mathbb{C} \setminus \{0\} \right\} \leq G$

$N = \left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} : x \in \mathbb{C} \right\} \trianglelefteq G$

Reason: $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}^{-1} = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \frac{1}{a} & -b \\ 0 & \frac{1}{d} \end{bmatrix} = \begin{bmatrix} a & ax+b \\ 0 & d \end{bmatrix} \begin{bmatrix} \frac{1}{a} & -b \\ 0 & \frac{1}{d} \end{bmatrix}$

$= \begin{bmatrix} 1 & a/d \\ 0 & 1 \end{bmatrix} \in N \quad \forall x \in \mathbb{C} \quad \forall a, b, d \in \mathbb{C},\ a, d \neq 0.$

$G = H \cdot N = N \cdot H$ because

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \begin{bmatrix} 1 & b/a \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & b/d \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix}$$

Q: Where do semi-direct products come from?
A: There are many examples!
(1) Affine linear transformations in $\mathbb{R}^n$ ($H = GL_n(\mathbb{R})$, $N \cong \mathbb{R}^n$ (translations))
(2) Groups of order $p \cdot q$ where p, q primes and $p < q$ with $q \equiv 1 \mod p$

§22.3 A motivating example:

Let G be a group with 21 elements

Write $21 = 3 \cdot 7 \rightsquigarrow p = 3$ or 7 are the primes to consider

- $n_3 \equiv 1 \mod 3$, $n_3 \mid 7$ $\Longrightarrow$ $n_3 = 1$ or 7
- $n_7 \equiv 1 \mod 7$, $n_7 \mid 3$ $\Longrightarrow$ $n_7 = 1$

by Sylow Theorem (3).

Two situations can arise:

<u>Situation 1:</u> $n_3 = 1$, $n_7 = 1$ $\rightsquigarrow$ $G \cong P \times Q$ $\quad Syl_3(G) = \{P\}$, $Syl_7(G) = \{Q\}$.

so G is a direct product.

((i) $P, Q \triangleleft G$, (ii) $P.Q = G$ (iii) $P \cap Q = \{e\}$)

In this case, $G \cong \mathbb{Z}/_{3\mathbb{Z}} \times \mathbb{Z}/_{7\mathbb{Z}} \cong \mathbb{Z}/_{21\mathbb{Z}}$ is abelian.

<u>Situation 2:</u> $n_3 = 7$, $n_7 = 1$ $\rightsquigarrow$ $\{Q\} = Syl_7(G)$. Pick $P \in Syl_3(G)$

We still get $P \cap Q = \{e\}$ & $G = P.Q$ ($|P| \mid |P.Q|$, $|Q| \mid |P.Q|$ so $21 \mid |P.Q|$)

Since $P \ntriangleleft G$ we get G is a semi-direct product of P and Q.

- $|P| = 3$, so we write $P = \{1, x, x^2\} \leq G$ for $x \in G$

  $|Q| = 7$, ——— $Q = \{1, y, y^2, \dots, y^6\} \trianglelefteq G$ for $y \in G$

- We obtain an isomorphism $\varphi = \mathrm{Conj}(x)$

$$\begin{array}{ccc} Q & \longrightarrow & Q \\ \rotatebox{90}{$\in$} & & \\ q & \longmapsto & xqx^{-1} = \mathrm{Conj}(x)(q) \end{array}$$

since $Q \trianglelefteq G$

with the following properties:

(1) $\varphi \circ \varphi \circ \varphi = \mathrm{Conj}(x^3) = \mathrm{Conj}(e) = id_Q : Q \longrightarrow Q$ (because $x^3 = e$)

(2) φ is non-trivial since $\varphi(y) = y \ \forall y \Rightarrow P$ and Q commute, and this forces G to be the direct product of P & Q, which was Situation 1.

(3) φ is an isomorphism $Q = \mathbb{Z}/_{7\mathbb{Z}} \xrightarrow{\sim} \mathbb{Z}/_{7\mathbb{Z}} = Q$

In particular $\varphi \in \mathrm{Aut}_{Gp}(\mathbb{Z}/_{7\mathbb{Z}}) = \{ f_t : \mathbb{Z}/_{7\mathbb{Z}} \longrightarrow \mathbb{Z}/_{7\mathbb{Z}} : f_t \text{ group iso} \}$, which
$$1 \longmapsto t$$

has order 6 (any $t \in \{1, 2, \dots, 6\}$ will work).

Since the element $\varphi = f_t$ has order 3 , the possible values of t are restricted

$t = 1, 2, 4$ $\quad$ ($t^3 \equiv 1 \mod 7$)

But $t = 1$ is not an option, since $f_1 = id$. $\Rightarrow$ $t = 2$ or 4 are the only options.

- **Note:** $P = \langle x \rangle = \langle x^2 \rangle$ so we can apply the same reasoning to x^2.

$$\rightsquigarrow \quad \begin{array}{ccc} P & \longrightarrow & \mathrm{Aut}_{Gp}(Q) \\ a & \longmapsto & \mathrm{Conj}(a) \end{array}$$

a non-trivial group homomorphism.

Next time, we'll give a different way to construct semidirect products starting from two group H, N and a group homomorphism

$$\alpha : H \longrightarrow \mathrm{Aut}_{Gp}(N) := \{ \varphi : N \longrightarrow N : \varphi \text{ group isomorphism} \}$$