Lecture XXIV: Semi-direct Products III

Recall: We have 2 constructions of semi-direct products

① A group G is a semi-direct product of subgroups H and N if
(1) $H \leq G$ and $N \trianglelefteq G$
(2) $HN = NH = G$ — Write $G = N \rtimes H$
(3) $H \cap N = \{e\}$

Conjugation gives an action $G \circlearrowright N$, restricting it to H we get $H \circlearrowright N$ left-action, or equivalently, a group homomorphism
$$\alpha : H \longrightarrow \mathrm{Aut}_{Gp}(N)$$
$$h \longmapsto \mathrm{Conj}(h)$$

② Given 2 groups H & N, and a group homomorphism $\alpha : H \longrightarrow \mathrm{Aut}_{Gp}(N)$ we define a group $N \rtimes_\alpha H = (N \times H, *_\alpha)$ where

$$\boxed{(n_1, h_1) *_\alpha (n_2, h_2) = (n_1\, \alpha(h_1)(n_2),\ h_1 h_2)} \qquad \forall\, n_1, n_2 \in N,\ h_1, h_2 \in H$$

- $e_{N \rtimes_\alpha H} = (e_N, e_H)$
- $(n, h)^{-1} = (\alpha(h^{-1})(n^{-1}), h^{-1}) \qquad \forall n \in N \ \forall h \in H.$

Proposition: $N \hookrightarrow N \rtimes_\alpha H$, $n \longmapsto (n, e_H)$ and $H \hookrightarrow N \rtimes_\alpha H$, $h \longmapsto (h, e_H)$ are injective group homomorphisms.

Furthermore
(1) $H \leq N \rtimes_\alpha H$, $N \trianglelefteq N \rtimes_\alpha H$
(2) $H \cdot N = N \cdot H = N \rtimes_\alpha H$
(3) $H \cap N = \{e\}$

So $N \rtimes_\alpha H = N \rtimes H$.

§24.1 Equivalence of two constructions:

Our next goal: show both constructions of semi-direct products (internal and external)

- Let G be a group which is a semi-direct product of two subgroups H & N

Let $\alpha : H \longrightarrow \mathrm{Aut}_{Gp}(N)$ be the group homomorphism induced by the conjugation act of H on N, ie $\alpha(h)(n) = h n h^{-1} \in N \qquad \forall h \in H \quad \forall n \in N.$

Next, we set $G = N \rtimes_\alpha H$ as in Lemma §23.1

Proposition 1: $f: G \longrightarrow \mathcal{G}$ is a group isomorphism.
$(n,h) \longmapsto nh$

Proof: First, we check this is a group homomorphism:

$$f((n_1,h_1) *_\alpha (n_2,h_2)) = f((n_1\, \alpha(h_1)(n_2), h_1h_2)) = n_1 \alpha(h_1)(n_2)\cdot h_1h_2$$
$$= n_1\, h_1 n_2 h_1^{-1} h_1 h_2 = n_1 h_1 n_2 h_2 = f((n_1,h_1))\, f((n_2,h_2))$$

- f is surjective because $NH = \mathcal{G}$.
- f is injective because $f(n,h) = nh = e \iff n = h^{-1} \in N \cap H = \{e\}$

So $n = e = h$. Thus, $\mathrm{Ker}(f) = \{(e,e)\}$. $\square$

- Conversely, given $G = N \rtimes_\alpha H$, we have G is the semi-direct product of N & H.

Proposition 2: The map $\beta: H \longrightarrow \mathrm{Aut}_{Gp}(N)$ induced by the action by conjugation agrees with α

Proof: $N \trianglelefteq N \rtimes_\alpha H$ & $H \leq N \rtimes_\alpha H$
$n \mapsto (n, e_H)$ $\quad h \mapsto (e_N, h)$

$$h *_\alpha n *_\alpha h^{-1} = (e_N, h) *_\alpha (n, e_H) *_\alpha (e_N, h^{-1}) = (e_N\, \alpha(h)(n), \overset{h}{\overset{\shortparallel}{h e_H}}) *_\alpha (e_N, h^{-1})$$
$$= (e_N\, \alpha(h)(n)\, \underbrace{\alpha(h)(e_N)}_{= e_N \ \alpha(h)\text{ gp hom.}}, h h^{-1}) = (\alpha(h)(n), e_H)$$

So $\beta(h)(n) = \alpha(h)(n)$ $\forall n \in N$ $\forall h \in H$ $\implies \beta = \alpha$. $\square$

Corollary 1: Given N, H groups we have a 1-to-1 correspondence:

$$\left\{\begin{array}{l}\text{Group structures on } N \times H \\ \text{with } \cdot N \trianglelefteq N\times H,\ H \leq N \times H \\ \quad\ \cdot HN = NH = N \times H \\ \quad\ \cdot H \cap N = \{e\}\end{array}\right\} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \left\{\begin{array}{l}\text{Group homomorphisms} \\ \alpha: H \longrightarrow \mathrm{Aut}_{Gp}(N)\end{array}\right\}$$

$G = N \rtimes_\alpha H \longleftarrow\!\shortmid\ \alpha$

$G = N \rtimes H \longmapsto \alpha(h) = \mathrm{Conj}(h)\ \forall h$

Proof: Proposition 1 says $\Psi \circ \Phi = id$ Proposition 2 says $\Phi \circ \Psi = id$. $\square$

⚠ Different $\alpha: H \longrightarrow \mathrm{Aut}_{Gp}(N)$ can give rise to isomorphic groups $N \rtimes_\alpha H$.

Example: $H = N = G$ non-abelian $\alpha: G \to \mathrm{Aut}_{Gp}(G)$ induced by conjugation

Then: $\alpha \neq$ Trivial but $G \rtimes_\alpha G \overset{\varphi}{\simeq} G \times G$ $\quad (a,b) \longmapsto (ab, b)$ is group iso since

- $\varphi((a_1,b_1) *_\alpha (a_2,b_2)) = \varphi(a_1 b_1 a_2 b_1^{-1}, b_1 b_2) = (a_1 b_1 a_2 b_1^{-1} b_1 b_2, b_1 b_2) = (a_1 b_1 a_2 b_2, b_1 b_2)$
$= (a_1 b_1, b_1)\cdot(a_2 b_2, b_2) = \varphi((a_1,b_1))\cdot\varphi((a_2,b_2))$. $\Rightarrow$ gp. homomorphism
- φ surjective $\varphi((ab^{-1},b)) = (a,b)$;
- φ injective. $\varphi(a,b) = (e,e) \Rightarrow ab = e$ & $b = e \Rightarrow (a,b) = (e,e)$. $\square$

Next, we state a Corollary of the 3rd Isomorphism Thm when $G = H\cdot N$ & $H \cap N = \{e\}$

Corollary 2: Let G be a semi-direct product of H & N. Then, the natural projection

$$\pi : G \longrightarrow G/N \qquad g \longmapsto gN$$

restricted to H induces an isomorphism
$$\pi|_H : H \xrightarrow{\sim} G/N \qquad h \longmapsto hN$$

Proof:
- $\pi|H$ is group homomorphism
- $G = H\cdot N$ so $\pi|_H$ is surjective
- $H \cap N$ so $\pi|_H$ is injective $\square$

Q: What does this mean?

A: For every coset $\bar{y} \in G/N$, we can find a representative $\bar{y} = \sigma_y N$ such that
- $\mathrm{ord}_G(\sigma_y) = \mathrm{ord}_{G/N}(\bar{y})$
- $\sigma_{y_1 y_2} = \sigma_{y_1}\sigma_{y_2}$

Namely: $\sigma_y = (\pi|_H)^{-1}(\bar{y}) \in H \leq G$.

Summary: $N \trianglelefteq G$ and $H \leq G$

- 3rd Iso Theorem: $H \leq G \Rightarrow H/_{H\cap N} \simeq H\cdot N/_N$
- If $NH = G$, $H\cap N = \{e\}$ $\Rightarrow$
$$\begin{tikzcd} \pi : G \arrow[r, two heads] & G/N \arrow[l, dashed, bend left] \\ \sigma_y & \bar{y} \arrow[l, mapsto] \end{tikzcd}$$
"lifting"

STEP 1 to build semi-direct products & distinguish them, is to understand $\mathrm{Aut}_{Gp}(N)$.

§ 25.2 Computing $\mathrm{Aut}_{Gp}(G)$:

We focus on some examples first. We start with the case when G is cyclic

Example 1: $\mathrm{Aut}_{Gp}(\mathbb{Z}) = \{f : \mathbb{Z} \longrightarrow \mathbb{Z}$ gp iso$\}$ $\qquad \mathbb{Z} = \langle 1\rangle = \langle -1\rangle$
only generators: 1 & -1.

Iso 1 : $f(1) = 1$ so identity.

Iso 2 : $f(1) = -1$ so $-\mathrm{id}_{\mathbb{Z}}$. It has order 2 : $f^2_{(1)} = -(-1) = 1$.

$\Rightarrow \mathrm{Aut}_{Gp}(\mathbb{Z}) = \{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z}$.

Example 2: $\mathrm{Aut}_{Gp}(\mathbb{Z}/p\mathbb{Z}) = \{ f : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \text{ gp iso} \}$ p prime.

Write $f \in \mathrm{Aut}_{Gp}(\mathbb{Z}/p\mathbb{Z})$ as
$$\sigma_x : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}, \quad 1 \longmapsto x$$

Group structure on $\mathrm{Aut}_{Gp}(\mathbb{Z}/p\mathbb{Z})$?

- $\sigma_x \circ \sigma_y(1) = \sigma_x(y) = \sigma_x(y\cdot 1) = y\,\sigma_x(1) = y\cdot x = \sigma_{xy}(1)$

  $y\cdot 1 = \underbrace{1+\cdots+1}_{y \text{ times}}$

Thus $\sigma_x \circ \sigma_y = \sigma_{xy}$. $\Longrightarrow$ $\mathrm{Aut}_{Gp}(\mathbb{Z}/p\mathbb{Z})$ is abelian.

- We need σ_x invertible $\sigma_1 = \mathrm{id}_{\mathbb{Z}/p\mathbb{Z}}$ so $(\sigma_x)^{-1} = \sigma_y \iff \sigma_{xy} = \sigma_1$

This means x is invertible in $\mathbb{Z}/p\mathbb{Z}$. Only non-valid choice: $x = 0$. (because p is prime)

Conclude: $\mathrm{Aut}_{Gp}(\mathbb{Z}/p\mathbb{Z}) = \mathbb{F}_p^* =$ multiplicative group of non-zero elements.

Example 3: $W := \mathrm{Aut}_{Gp}(\mathbb{Z}/8\mathbb{Z}) = \{ \sigma_x : \mathbb{Z}/8\mathbb{Z} \longrightarrow \mathbb{Z}/8\mathbb{Z} \text{ gp iso} \}$
$$1 \longmapsto x$$

As before, $\sigma_x \circ \sigma_y = \sigma_{xy}$ & $\sigma_1 = \mathrm{id}_{\mathbb{Z}/8\mathbb{Z}}$ $\rightsquigarrow$ $\mathrm{Aut}_{Gp}(\mathbb{Z}/8\mathbb{Z})$ is abelian.

σ_x is invertible $\iff \exists y : xy = 1 \mod 8$

Options for x: $x = 1, 3, 5, 7$

$(\sigma_3)^{-1} = \sigma_3$; $(\sigma_5)^{-1} = \sigma_5$; $(\sigma_7)^{-1} = \sigma_7$.

$\sigma_3 \circ \sigma_5 = \sigma_{15} = \sigma_7$.

$\langle\sigma_3\rangle \cap \langle\sigma_5\rangle = \{e\}$, $\langle\sigma_3\rangle \trianglelefteq W$, $\langle\sigma_5\rangle \trianglelefteq W$, $\langle\sigma_3\rangle\langle\sigma_5\rangle = W$

$$\Rightarrow W \simeq \underset{\langle\sigma_3\rangle}{\mathbb{Z}/2\mathbb{Z}} \times \underset{\langle\sigma_5\rangle}{\mathbb{Z}/2\mathbb{Z}}$$

Lemma: G cyclic $\Longrightarrow W = \mathrm{Aut}_{Gp}(G)$ is abelian

Proof: Fix a generator $\sigma \in G$. Then, any group homomorphism $f : G \to G$ is completely determined by $x = f(\sigma) \in G$.

Since we have a classification of cyclic groups, we write $G = \mathbb{Z}/m\mathbb{Z}$ for $m = 0, 1, \ldots$

($\mathbb{Z} = \mathbb{Z}/0\cdot\mathbb{Z}$) Then, $f \in W$ becomes $f: G \longrightarrow G$, $1 \longmapsto x \pmod{m}$. Write $f = \sigma_x$.

- $\sigma_x \circ \sigma_y\,(1) = \sigma_x(y \bmod m) = \sigma_x(\underbrace{1 + \cdots + 1}_{y \,(\text{mod } m)\text{ times}}) = \underbrace{x + \cdots + x}_{y\,(\text{mod } m)\text{ times}} \pmod{m} = xy \pmod{m}$

$= \sigma_{xy}(1)$ Thus, $\sigma_x \circ \sigma_y = \sigma_{xy} = \sigma_y \circ \sigma_x \quad \forall x, y$

- $\sigma_1 = id_G$

$\Rightarrow$ W is abelian. $\square$

Q: What values of x ensure $\sigma_x \in \mathrm{Aut}_{Gp}(\mathbb{Z}/m\mathbb{Z})$?

A: We need σ_x to be invertible!

σ_x is an iso if and only if $\exists\, y \in \mathbb{Z}/m\mathbb{Z}$ such that $xy \equiv 1 \bmod (m)$

$\Leftrightarrow \gcd(m, x) = 1$.

Corollary: For all $m \in \mathbb{Z}_{\geq 0}$: $\mathrm{Aut}_{Gp}(\mathbb{Z}/m\mathbb{Z}) = \{x \in \mathbb{Z}/m\mathbb{Z} : \gcd(m,x) = 1\}$ with $\circ$ operation. In particular: $|\mathrm{Aut}_{Gp}(\mathbb{Z}/m\mathbb{Z})| = \varphi(n)$ (Euler's φ function).