# Lecture 8 - Examples: Groups of low order

Note Title 2/12/2008

**Def** If $H$ and $K$ are groups, then the direct product of $H$ and $K$ is: $H \times K$

$$(h_1,k_1)\cdot(h_2,k_2) = (h_1h_2, k_1k_2).$$

$H$ and $K$ are both subgroups and quotients of $H \times K$:

$$\iota_H : H \longrightarrow H\times K \qquad\qquad \pi_H : H\times K \longrightarrow H$$
$$h \longmapsto (h,e) \qquad\qquad (h,k) \longmapsto h$$
$$\iota_K : K \longrightarrow H\times K \qquad\qquad \pi_K : H\times K \longrightarrow K$$
$$k \longmapsto (e,k) \qquad\qquad (h,k) \longmapsto k$$

underlying set theory map

$\rightsquigarrow$ $H\times K$ is the product in the category $\mathcal{G}rp$.

i.e.

$$\begin{tikzcd} G \arrow[r] \arrow[d] \arrow[dr, dashed] & H \arrow[d] \\ K \arrow[r] & \{e\} \end{tikzcd} \qquad H\times K \to H,\ H\times K \to K$$

$$\pi_H \circ \iota_H = Id_H \qquad\qquad h \longmapsto (h,e) \longmapsto h$$

$$\pi_K \circ \iota_K = Id_K$$

$$\pi_H \circ \iota_K = \text{constant map w/ value } e. \qquad\qquad k \longmapsto (e,k) \longmapsto e$$

$$K \longrightarrow \{e\}$$

$\longleftrightarrow$ $Im(\iota_K) = ker(\pi_H)$

$$K \xrightarrow{\iota_K} H\times K \xrightarrow{\pi_H} H$$ is exact at $H\times K$.

$(ker(\pi_H) = Im(\iota_K))$

**Def** A short exact sequence is a sequence $N \xrightarrow{f} G \xrightarrow{g} H$ of homomorphisms s.t.

$N \to G$ is injective $\leftrightarrow$ $\{e\} \to N \to G$ is exact at $N$

$G \to H$ is surjective $\leftrightarrow$ $G \to H \to \{e\}$ is exact at $H$.

$\ker(g) = \operatorname{Im}(f)$ $\leftrightarrow$ $H \cong G/N$ via $\underset{\substack{\uparrow \\ G/N}}{aN} \mapsto g(a)$

$\updownarrow$ $\{e\} \to N \to G \to H \to \{e\}$ is exact.

A S.E.S. splits $G$ into two smaller pieces $\Rightarrow$

**Def** An extension of $N$ by $H$ is a S.E.S.:

$$\{e\} \to N \to G \to H \to \{e\}.$$

**Ex:** $N = H = \mathbb{Z}/2$

- $\{e\} \to \mathbb{Z}/2 \xrightarrow{\iota_1} \underline{\mathbb{Z}/2 \times \mathbb{Z}/2} \xrightarrow{\pi_2} \mathbb{Z}/2 \to \{e\}$
- $\{e\} \to \mathbb{Z}/2 \to \mathbb{Z}/4 \xrightarrow{\pi} \mathbb{Z}/2 \to \{e\}$

  $a \mapsto 2a$

**Def** A S.E.S. is split if there is a homomorphism

$\{e\} \to N \xrightarrow{\iota} G \xrightarrow{\pi} H \to \{e\}$

$$H \xrightarrow{\sigma} G \quad \text{s.t.} \quad \begin{tikzcd} H \arrow[r, "\sigma"] \arrow[rr, bend right, "\mathrm{Id}_H"'] & G \arrow[r, "\pi"] & H \end{tikzcd}$$

**Ex:** - Any direct product is split exact.

- $\{e\} \to \mathbb{Z}/p \to \mathbb{Z}/p^2 \to \mathbb{Z}/p \to \{e\}$ is not split.

If a S.E.S. is split, then $G = H \cdot N$, where $H$ and $N$ are identified with their images in $G$.

**Def** $G$ is the internal direct product of $H$ & $K$ if

$$G = HK, \quad H \cap K = \{e\}, \quad H \trianglelefteq G \trianglerighteq K.$$

$G$ is the internal semidirect product of $H$ & $K$ if

$$G = HK, \quad H \cap K = \{e\}, \quad K \trianglelefteq G.$$

Given a decomp of $G$ as the semidirect prod of $H$ and $K$, get a split S.E.S.:

$$\{e\} \to K \to G \xrightarrow{k} H \to \{e\}$$

inclusion of $H$

$$G/K = HK/K \underset{\substack{2^{nd}\text{ iso}\\ \text{thm}}}{\cong} H/H\cap K \underset{\substack{\uparrow\\ H\cap K = \{e\}}}{=} H$$

**Prop 29** If $G$ is the internal direct product of $H$ and $K$, then

$$G \cong H \times K.$$
$$hk \leftarrow (h,k)$$

Pf: Given $h \in H$, $k \in K$, $h$ and $k$ commute.

$$hk \overset{?}{=} kh \quad \longleftrightarrow \quad hkh^{-1}k^{-1} \overset{?}{=} e$$

$$(hkh^{-1})k^{-1} \in K$$
$$\Big(\Big( \ \underset{}{K} \ \cdot \ K \qquad \Rightarrow \quad hkh^{-1}k^{-1} \in H\cap K = \{e\}$$
$$\underset{H}{h}(\underset{H}{kh^{-1}k^{-1}}) \in H \qquad \Rightarrow \quad hkh^{-1}k^{-1} = e.$$

$$H \times K \longrightarrow G$$
$$(h,k) \longmapsto hk$$

$$(h_1,k_1)\cdot(h_2,k_2) \longmapsto (h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2$$
$$\| \qquad\qquad\qquad\qquad \|$$
$$(h_1h_2, k_1k_2) \longmapsto h_1h_2k_1k_2 = h_1(h_2k_1)k_2$$

Since $G = HK$, any $g \in G$ can be written as $g = h\cdot k = \mathrm{im}(h,k)$

$$(h,k) \longmapsto e$$

$$\Rightarrow hk = e \Rightarrow \underset{H}{h} = \underset{K}{k^{-1}} \Rightarrow h \in H\cap K = \{e\}$$
$$k$$
$$\Rightarrow h = k = e. \qquad \square$$

**Def** An automorphism of $G$ is an isomorphism from $G$ to itself.

**Def** Given a homomorphism $H \xrightarrow{\phi} \mathrm{Aut}(K) = \{f \mid f: K \xrightarrow{\sim} K\}$, get a group, the semidirect product $H \ltimes K$

$$K \rtimes H$$

$$(k_1,h_1)\cdot(k_2,h_2) = (k_1\cdot\phi(h_1)(k_2),\ h_1h_2)$$

$$\Big(\ h_1k_2 = k'\cdot h_1 \quad \longleftrightarrow \quad h_1k_2h_1^{-1} = k'\Big)$$
$$= \phi(h)(k_2)$$

$$k_1h_1k_2h_2 = k_1(\phi(h)(k_2)h_1)h_2 = k_1\phi(h)(k_2)\,h_1h_2$$

**Prop 30** If $G$ is the internal semidirect prod of $H$ and $K$, then
$G \cong H \ltimes K$, $H \to \mathrm{Aut}(K)$ is conjugation in $G$.

Since $H \leq G$, $K \trianglelefteq G$, $H$ acts on $K$ via conjugation
= an automorphism.

$$hk \longrightarrow (k, h)$$
$$\overset{\cap}{G} = HK \longrightarrow H \ltimes K.$$

**Prop 31**: $\mathrm{Aut}(\mathbb{Z}/n) = (\mathbb{Z}/n)^* = \{m \in \mathbb{Z}/n \mid (m, n) = 1\}$
$= \{m \in \mathbb{Z}/n \mid \exists \underset{\in \mathbb{Z}}{k \in \mathbb{Z}/n} \quad m \cdot k = 1\}$

**Cor 32**: $\mathrm{Aut}(\mathbb{Z}/p) = \mathbb{Z}/p-1$

**Thm 33**: If $|G| = p \cdot q$, $p, q$ prime, then $q > p$
$G = \mathbb{Z}/p \times \mathbb{Z}/q$ if $p \nmid q-1$
$G = \mathbb{Z}/q \rtimes \mathbb{Z}/p$ $\quad p \mid q-1$

**Pf**: Know have $\mathbb{Z}/p = H$, $\mathbb{Z}/q = K \subseteq G$.

$g \in H \cap K = \{e\} \Rightarrow g^p = e$ ; $g^q = e \Rightarrow (p, q) = 1 \Rightarrow g^1 = e$

$|G| = |H| \cdot |K| \Rightarrow G = H \cdot K$

$\mathbb{Z}/q$ is normal:

1) $[G : K] = p$, the smallest prime dividing $|G|$. $\Rightarrow K$ normal.

2) $K$ is a $q$-Sylow s.g. $\Rightarrow$ # of s.g conjugate to $K$ divides $|G|$ and is $1 \bmod q$
$\Rightarrow$ divides $p \Rightarrow 1$. $(q > p)$.

$\Rightarrow$ $G$ is the semidirect product of $\underset{\text{normal}}{\underset{\uparrow}{\mathbb{Z}/q}}$ and $\mathbb{Z}/p$

$\Leftrightarrow \mathbb{Z}/p \longrightarrow \mathrm{Aut}(\mathbb{Z}/q) = \mathbb{Z}/q-1$

if $(p, q-1) = 1$, then there are no maps.
$\leftrightarrow p \nmid q-1$

if $p \mid q-1$, then there are maps : $\mathbb{Z}/p \to \mathbb{Z}/q-1$