Lecture 10: Short exact sequences

Last Time: 2 characterizations of semidirect products

① $H < G$, $N \lhd G$

$G = NH \ (= HN)$

$H \cap N = \{e\}$

$\rightsquigarrow G = N \rtimes H$

② $\alpha : H \longrightarrow \mathrm{Aut}_{Gp}(N)$ gp hom.

$G = N \times H$ as a set with group operation

$(n_1, h_1) \cdot (n_2, h_2) = (n_1\, \alpha(h_1)(n_2),\ h_1 h_2)$

$\rightsquigarrow G = N \rtimes_\alpha H$

① $\Longrightarrow$ ②
$$\begin{aligned} \alpha = H &\longrightarrow \mathrm{Aut}_{Gp}(N) \\ h &\longmapsto (g \longmapsto h g h^{-1}) \end{aligned}$$

② $\Longrightarrow$ ①
$$\begin{aligned} N &\hookrightarrow G \\ n &\longmapsto (n, e_H) \end{aligned} \quad , \quad \begin{aligned} H &\hookrightarrow G \\ h &\longmapsto (e_N, h) \end{aligned}$$
group hom injective.

Last characterization: using short exact sequences.

§1. Short Exact Sequences:

Recall (1st Isomorphism Theorem) $\varphi\ G \twoheadrightarrow G'$ gp hom, then $\frac{G}{\mathrm{Ker}\,\varphi} \overset{\bar{\varphi}}{\simeq} G'$.

This statement is often written as:

Theorem: We have an exact sequence (see definition below):

$$\mathbb{1} \longrightarrow \mathrm{Ker}(\varphi) \xrightarrow{i} G \xrightarrow{\varphi} G' \longrightarrow \mathbb{1}$$

where:
- $\mathbb{1} = \{1\}$ is the trivial group
- $i : \mathrm{Ker}(\varphi) \longrightarrow G$ is the natural inclusion
- $\mathbb{1} \longrightarrow \mathrm{Ker}(\varphi) \ : \ 1 \longrightarrow e_G$

  $G' \longrightarrow \mathbb{1} \ : \ g' \longrightarrow 1 \quad \forall g' \in G'$.

Definition: A sequence of group homomorphisms

$$G_1 \xrightarrow{\varphi} G_2 \xrightarrow{\Psi} G_3$$

is said to be exact (or exact at G_2) if $\mathrm{Im}\,\varphi = \mathrm{Ker}\,\Psi$.

Obs: $\mathrm{Ker}\,\Psi \lhd G_2$ but in general $\mathrm{Im}\,\varphi$ is not (unless G_2 is abelian), so this is a strong condition to impose!

Examples: ① $1 \longrightarrow G_1 \xrightarrow{\Psi} G_2$ is exact $\Longleftrightarrow$ Ψ is injective

② $G_1 \xrightarrow{\varphi} G_2 \longrightarrow 1$ is exact $\Longleftrightarrow$ φ is surjective.

Def.: An exact sequence of the form

$$1 \longrightarrow G_1 \xrightarrow{\varphi} G_2 \xrightarrow{\Psi} G_3 \longrightarrow 1$$

is usually referred to as a short exact sequence (ses). It signifies that:

(i) G_1 can be viewed as a normal subgroup of G_2 because $G_1 \xrightarrow{\sim} \underset{\substack{\parallel \\ \operatorname{Ker}\Psi \triangleleft G_2}}{\operatorname{Im}\varphi} < G_2$

(ii) $G_2/\operatorname{Im}\varphi = G_2/\operatorname{Ker}\Psi \xrightarrow[\sim]{\overline{\Psi}} G_3$ is an iso.

Ex.: 1st Isomorphism Theorem:

$$\begin{tikzcd} G \arrow[r, "\varphi"] & G' \text{ gp hom} & {} \arrow[r, squiggly] & 1 \arrow[r] & \operatorname{Ker}\varphi \arrow[r] & G \arrow[r, "\varphi"] & \operatorname{Im}(\varphi) \arrow[r] & 1 \\ & & & 1 \arrow[r] & \operatorname{Ker}\varphi \arrow[r] \arrow[u, equal, "\wr\,\text{id}"'] & G \arrow[r, "\pi"] \arrow[u, equal, "\wr\,\text{id}"'] & G/\operatorname{Ker}\varphi \arrow[r] \arrow[u, "\overline{\varphi}"', "\wr"] & 1 \end{tikzcd}$$

Obs: These 2 short exact sequences are called equivalent (vertical maps should be isos.

The exact sequence $1 \longrightarrow G_1 \xrightarrow{\varphi} G_2 \xrightarrow{\Psi} G_3 \longrightarrow 1$ also signifies that we can "build G_2 out of G_1 & G_3". More precisely "G_2 is an extension of G_3 by G_1"

§2 Examples

Ex 1: (Abelian case: write trivial gp as 0)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Z}/5\mathbb{Z} & \longrightarrow & 0 \\ & & \psi & & & & & & \\ & & m & \longmapsto & 5m & & & & \end{array}$$

is a s.e.s.

Ex 2. $\det: GL_2(\mathbb{C}) \longrightarrow \mathbb{C} \setminus \{0\} =: \mathbb{C}^*$ (group under usual multiplication)

$A \longmapsto \det(A)$

is a surjective group homomorphism ($\begin{bmatrix} 1 & 0 \\ 0 & \lambda \end{bmatrix} \longmapsto \lambda$)

$\operatorname{Ker}(\det) = 2\times2$ matrices of determinant $1 =: SL_2(\mathbb{C})$.

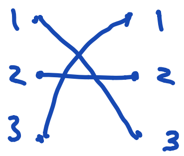
$1 \longrightarrow SL_2(\mathbb{C}) \longrightarrow GL_2(\mathbb{C}) \longrightarrow \mathbb{C}^* \longrightarrow 1$ is a s.e.s.

Ex 3. (Defining A_n = alternating group)

Fix $\sigma \in S_n$ By HW2, $\ell(\sigma) = \#\{i<j : \sigma(i) > \sigma(j)\}$. Also, $\ell(\sigma)$ = min # of simple transpositions used to write σ.

Eg: $\sigma = (13) = (12)(23)(12)$ so $\ell((13)) = 3$.

$\ell((13))$ = # crossings in



(general statement)

Set sign: $S_n \longrightarrow \{\pm 1\}$

$\sigma \longmapsto \text{sign}(\sigma) := (-1)^{\ell(\sigma)}$ (gp homomorphism by HW2)

(Proof by picture; $\ell(\sigma\tau) \equiv \ell(\sigma) + \ell(\tau) \pmod 2$.)

Def $\boxed{A_n := \text{Ker}\,(\text{sign})}$ = subgroup of even permutations ($A_n \lhd S_n$)

Ex: $A_2 = \{1\!\!1\}$, $A_3 = \langle (123) \rangle$, $A_4 = \langle (123), (12)(34) \rangle$

(Later in the course: we'll see A_n is simple for $n \geq 5$.)

A_4 is not simple: $H = \{1, (12)(34), (13)(24), (14)(23)\} \lhd A_4$.

$\Rightarrow$ $1\!\!1 \longrightarrow A_n \longrightarrow S_n \longrightarrow \{\pm 1\} \longrightarrow 1\!\!1$ is a s.e.s.

§3. Sections & Retractions:

Fix
$$\begin{tikzcd}
1\!\!1 \arrow[r] & G_1 \arrow[r, "\varphi"] & G_2 \arrow[r, "\psi"] \arrow[l, bend left, dashed, "\exists r?"] & G_3 \arrow[r] \arrow[l, bend left, dashed, "\exists s?"] & 0
\end{tikzcd}$$
ses

Q: Can we use $G_1 \lhd G_2$ & G_3 to understand/characterize G_2?

A: Usually knowing $N \lhd G$ & G/N does not characterize G!

Ex!
$$\begin{tikzcd}
1\!\!1 \arrow[r] & \langle \rho^2 \rangle \arrow[r] \arrow[d, phantom, "\cong"] & D_4 \arrow[r] & D_4/\langle \rho^2 \rangle \arrow[r] \arrow[d, phantom, "\cong"] & 1\!\!1 \\
 & \mathbb{Z}/2\mathbb{Z} \arrow[d, phantom, "\cong"] & & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \arrow[d, phantom, "\cong"] & (\langle \rho \rangle \times \langle s \rangle) \\
1\!\!1 \arrow[r] & \{\pm 1\} \arrow[r] & Q_8 \arrow[r] & Q_8/\{\pm 1\} \arrow[r] & 1\!\!1 .
\end{tikzcd}$$
$(\langle i \rangle \times \langle j \rangle)$

order $4 = 2^2$ & non cyclic.

But $D_4 \not\cong Q_8$

Conclude: Answer will depend on extra properties of φ and/or Ψ!

Definition: A ses is split if we have a section, that is, a gp hom $s : G_3 \longrightarrow G_2$ with $\Psi \circ s = id_{G_3}$ (⇒ s is injective!)

Definition: A ses is trivial if we have a retraction (or projection), that is, a gp hom $r : G_2 \longrightarrow G_1$ with $r \circ \varphi = id_{G_1}$. (⇒ r is surjective!)

Obs 1: Not every ses splits!

Ex:
$$\begin{tikzcd}
 & & & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \arrow[d, phantom, "12"] & \\
\mathbb{1} \arrow[r] & \{\pm 1\} \arrow[r] & Q_8 \arrow[r] & Q_8/\{\pm 1\} \arrow[r] \arrow[l, bend right, dashed, "\nexists s"] & \mathbb{1}.
\end{tikzcd}$$

only elements of order 2 $= \pm 1$

all elements have order 2 (except $\{\pm 1\}$)

Obs 2: trivial & split ses are different things!

Ex:
$$\begin{tikzcd}
\mathbb{1} \arrow[r] & A_3 \arrow[r, "i"] & S_3 \arrow[r, "sign"] \arrow[l, bend left, dashed, "\nexists r \text{ gp hom}"] & \{\pm 1\} \arrow[r] \arrow[l, bend left, dashed, "\exists s \text{ gp hom}"] & \mathbb{1}
\end{tikzcd}$$

Claim 1: $s(-1) = (12)$ satisfies $sign \circ s = id_{\{\pm 1\}}$.
(⇒ ses splits)

$$\begin{tikzcd}
1 \arrow[r, mapsto, "s"] & id \arrow[r, mapsto, "sign"] & 1 \\
(-1) \arrow[r] & (12) \arrow[r] & -1.
\end{tikzcd}$$

Claim 2: $\nexists\, r : S_3 \longrightarrow A_3$ gp hom s.t. $r \circ i = id_{A_3}$ (⇒ ses not trivial!)

Why? Set $\sigma = r((ij))$ $(i \neq j)$ $o((ij)) = 2$ but $o(\sigma) \mid |A_3| = \frac{|S_3|}{2} = 3$

so $o(\sigma) = 1$.

But every permutation in S_3 is a product of transpositions so r must be trivial on S_3 : $Im\, r = \mathbb{1} \lneq A_3$. Contr! since r is surjective □

Lemma: A trivial ses always splits

Pf/
$$\begin{tikzcd}
\mathbb{1} \arrow[r] & A \arrow[r, "\varphi"] & B \arrow[r, "\Psi"] \arrow[l, bend left, dashed, "\exists r"] & C \arrow[r] & \mathbb{1}
\end{tikzcd}$$
A, B, C gps.

$r : B \twoheadrightarrow A$ $\quad r \circ \varphi = id_A$

Want to build a gp hom $s : C \hookrightarrow B$ with $\Psi \circ s = id_C$.

We write $\ker r \xrightarrow{\Psi|_{\ker}} C$ gp homomorphism.

Claim 1: $\Psi|_{\ker r}$ is injective.

Pf/ Pick $b \in \ker r$ with $\Psi(b) = e_C$. so $b \in \ker \Psi \overset{\text{exactness}}{=} \operatorname{Im} \varphi$

so $b = \varphi(a)$ for $a \in A$.

Then $e_A = r(b) = \underbrace{r \circ \varphi}_{1_A}(a) = a$ $\Big\}$ $\Rightarrow b = \varphi(e_A) = e_B$

□

Claim 2: $\Psi|_{\ker r}$ is surjective

Pf/ Given $c \in C$ pick $b \in B$ with $\Psi(b) = c$. This choice is not unique, but if $\Psi(b') = c$ then $b' = b\varphi(a)$ for $a \in A$

Pick $b' = b\, \varphi \circ \underbrace{r(b^{-1})}_{\in A}$. Note: $b' \in \ker r$. because

$r(b') = r(b) \underbrace{r \circ \varphi}_{=1_A} \circ r(b^{-1}) = r(b) r(b^{-1}) = e_B$

Then $\exists\ s : C \longrightarrow \ker r \hookrightarrow B$ gp homomorphism with $\Psi \circ s = 1_C$. $\Rightarrow$ the ses splits. □

Split & Trivial ses will characterize G_2 as $G_1 \rtimes_\alpha G_3$ or $G_1 \times G_3$

Proposition 1: If the ses $1 \longrightarrow N \xrightarrow{\varphi} G \xrightarrow{\Psi} H \longrightarrow 1$ is Trivial, then $G \simeq N \times H$ (direct product) when $N \overset{\varphi}{\hookrightarrow} G$ & $H \overset{s}{\hookrightarrow} G$

Proof: Assume $\exists\ r : G \longrightarrow N$ retraction Then:

$$\begin{tikzcd}
1 \arrow[r] & N \arrow[r, "i"] \arrow[d, equal] & N \times H \arrow[r, "\pi_2"] \arrow[l, bend left, dashed, "\pi_1"] & H \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & N \arrow[r, "\varphi"] & G \arrow[r, "\Psi"] \arrow[u, "\wr"', "\eta"] \arrow[l, bend left, dashed, "\exists r"] & H \arrow[r] & 1
\end{tikzcd}$$

$$\begin{tikzcd}
& N \times H \arrow[dl, "\pi_1"'] \arrow[dr, "\pi_2"] & \\
N & & H
\end{tikzcd}$$

Define $\eta : G \longrightarrow N \times H$ via $\eta(g) = (r(g), \Psi(g))$.

- η is gp hom since both r & Ψ are

Claim 1: η is surjective :

Pf/. Pick $x \in N$ & $h \in H$. Choose $g \in G$ with $\psi(g) = h$ ($\exists$ because ψ_{surj})

Take $\boxed{\tilde{g} = g\,(\varphi \circ r(g))^{-1}\,\varphi(x) \in G}$

$$\Rightarrow \psi(\tilde{g}) = \psi(g)\,\psi(\varphi \circ r(g^{-1}))\,\underbrace{\psi\circ\varphi(x)}_{=e_H} = \underbrace{\psi(g)\psi\circ\varphi(\underbrace{r(g^{-1})}_{\in N})}_{=e_H} = \psi(g) = h$$

$$r(\tilde{g}) = r(g)\,\underbrace{r}_{id_N}(\varphi\circ r(g^{-1}))\,\underbrace{r\circ\varphi}_{id_N}(x) = \underbrace{r(g)r(g^{-1})}_{=e_G}\cdot x = x \in N$$

So $\eta(\tilde{g}) = (x, h)$ □

Claim 2: η is injective.

Pf/ If $\eta(g) = (e_N, e_H)$ then $\Psi(g) = e_H$, so $g \in \operatorname{Ker}\Psi = \operatorname{Im}\varphi$.

$$\left.\begin{aligned} &\text{Then, } \exists\, x \in N \text{ with } g = \varphi(x) \\ &\Rightarrow e_N = r(g) = r\circ\varphi(x) = x \end{aligned}\right\} \Rightarrow g = \varphi(e_N) = e_G.$$

It is easy to check all squares commute. □

Proposition 2: If a ses

$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r, "\varphi"] & G \arrow[r, "\Psi"] & H \arrow[r] \arrow[l, dashed, bend left, "s"] & 1 \end{tikzcd}$$

splits, then $G \simeq N \rtimes H$ where $N \xhookrightarrow{\varphi} G$ & $H \xhookrightarrow{s} G$

Pf/ Know: $N \underset{\varphi}{\triangleleft} G$ & $H \underset{s}{<} G$.

Claim 1: $s(H) \cap \varphi(N) = \{e\}$

Pick $g \in s(H) \cap \varphi(N)$ then $g = s(h) = \varphi(x)$ $x \in N$, $h \in H$

$$\left.\begin{aligned} \Rightarrow \Psi(g) &= \Psi\circ s(h) = h \\ &= \psi\circ\varphi(x) = e_H \end{aligned}\right\} \Rightarrow g = s(e_H) = e_G \checkmark$$

Claim 2: $NH = \{\varphi(x)s(h) \quad x \in N, h \in H\} = G$

Pick $g \in G \Rightarrow \psi(g) \in H$

Pick $\tilde{g} = s\circ\Psi(g)$. It satisfies $\psi(g) = \Psi(\tilde{g})$, so

$\tilde{g}^{-1} g \in \operatorname{Ker}\psi = \operatorname{Im}\varphi$ so $\tilde{g}^{-1} g = \varphi(x)$ for some $x \in N$.

Then : $$g = \tilde{g}\,\varphi(x) = s\circ\psi(g)\,\varphi(x) = \underbrace{s\circ\psi(g)\,\underset{\substack{\Uparrow \\ N \triangleleft G}}{\varphi(x)}\,(s\circ\psi(g))^{-1}}_{\in N}\;\underbrace{s\circ\psi(g)}_{\in H}$$

By definition, $G = \varphi(N) \rtimes s(H) \cong N \rtimes H$. □

Example : $$\begin{tikzcd} 1 \arrow[r] & A_n \arrow[r, "i"] & S_n \arrow[r, "\text{sign}"] & \{\pm 1\} \arrow[r] & 1 \\ & & (12) & -1 \arrow[l, mapsto] & \end{tikzcd}$$ splits

so $S_n = A_n \rtimes \mathbb{Z}/2\mathbb{Z}$.

Theorem : If $N < G$ has index two, then $G \cong N \rtimes \mathbb{Z}_2$
G finite

Pf/. $N \triangleleft G$ because $G/N = \{eN, gN\}$ for some $g \notin N$
$N\backslash G = \{eN, Ng\}$

so $gN = Ng$.

. Pick $h \in G \setminus N$ of order 2 ($g^2 \in N$ so $g^2 = e$ or $o(g^2) = k$, $k > 1$ so $o(g^k) = 2$)

Then
$H = \langle h \rangle < G$
$H \cap N = \{e\}$ since $h \notin N$
$NH = G$ because $|N\backslash G| = 2$

$\Big\}\; G = N \rtimes H \cong N \rtimes \mathbb{Z}_2$

□