Fri, Oct 10, 2014

Last time I claimed:

Prop'n Any homomorphism

$$\phi : R \to \mathrm{Aut}(L)$$

Automorphism of L as a group.

I.e., $\mathrm{Aut}(L) = \{\text{group isomorphisms } L \to L\}$.

This is in contrast to $\mathrm{Aut}_{Set}(L)$.

defines a group H and a split SES

$$\begin{tikzcd} L \arrow[r] & H \arrow[r] & R \arrow[l, bend right, "j"'] \end{tikzcd}.$$

Well, let $H = L \times R$ as a set.

Define

$$H \times H \longrightarrow H$$

as follows:

$$(l_1, r_1) \cdot (l_2, r_2) = \underbrace{(l_1 \cdot \phi_{r_1}(l_2), r_1 r_2)}$$

almost the group operation of $L \times R$, but before we multiply by l_1, we "twist" l_2 to another element of L — namely, $\phi_{r_1}(l_2)$.

The value of r_1 under the homomorphism $\phi : R \to \mathrm{Aut}(L)$.

Prop'n This is a group.

Pf. $(l_1, r_1) \cdot ((l_2, r_2) \cdot (l_3, r_3))$

$= (l_1, r_1) \cdot (l_2 \cdot \phi_{r_2}(l_3), r_2 r_3)$ by def'n of operation

$= (l_1 \cdot \underbrace{\phi_{r_1}(l_2 \cdot \phi_{r_2}(l_3))}, r_1(r_2 r_3))$ by def'n of operation

$\downarrow$ since ϕ_{r_1} is a homom.

$= (\underbrace{l_1 \cdot \phi_{r_1}(l_2) \cdot \phi_{r_1}(\phi_{r_2}(l_3))}, (r_1 r_2) r_3)$

$\downarrow$ since $\phi : R \to \mathrm{Aut}(L)$ is a homom.

$= (l_1 \phi_{r_1}(l_2) \cdot \underbrace{\phi_{r_1 r_2}(l_3)}, (r_1 r_2) r_3)$

$= (l_1 \phi_{r_1}(l_2), r_1 r_2) \cdot (l_3, r_3)$ by def'n of operation

$= ((l_1, r_1) \cdot (l_2, r_2)) \cdot (l_3, r_3)$. "

$\Longrightarrow$ associativity.

identity:

since ϕ is a homom, $\phi_1 = 1$.

$$(1_L, 1_R)\cdot(\ell, r) = (1_L \cdot \phi_{1_R}(\ell), 1_R \cdot r)$$
$$= (1_L \cdot \ell, 1_R \cdot r)$$
$$= (\ell, r).$$

$$(\ell, r)\cdot(1_L, 1_R) = (\ell \cdot \phi_r(1_L), r\cdot 1_R)$$

since $\phi_r : L \to L$ is a homom, $\phi_r(1) = 1$.

$$= (\ell \cdot 1_L, r \cdot 1_R)$$
$$= (\ell, r).$$

inverses:

I claim $(\ell, r)^{-1} = (\phi_{r^{-1}}(\ell^{-1}), r^{-1})$

Pf: $(\ell, r)\cdot(\phi_{r^{-1}}(\ell^{-1}), r^{-1}) = (\ell \cdot \phi_r(\phi_{r^{-1}}(\ell^{-1})), rr^{-1})$ Defn of operation

$= (\ell \cdot \phi_{rr^{-1}}(\ell^{-1}), rr^{-1})$ $\phi: R \to \mathrm{Aut}\, L$ is a homom, so $\phi_r \circ \phi_{r^{-1}} = \phi_{rr^{-1}}$.

$= (\ell \cdot \ell^{-1}, rr^{-1})$ ϕ is a gp homom, so $\phi_1 = \mathrm{id}_L$.

$= (1_L, 1_R)$.

$(\phi_{r^{-1}}(\ell^{-1}), r^{-1})\cdot(\ell, r) = (\phi_{r^{-1}}(\ell^{-1}) \cdot \phi_{r^{-1}}(\ell), r^{-1}r)$ defn of operation

$= (\phi_{r^{-1}}(\ell^{-1}\ell), r^{-1}r)$ $\phi_{r^{-1}} : L \to L$ is a gp homom

$= (\phi_{r^{-1}}(1_L), 1_R)$

$= (1_L, 1_R)$. $\phi_{r^{-1}}$ is a gp homom, so $\phi_{r^{-1}}(1) = 1$.

//

Defn We denote this group by

$$L \rtimes_\phi R.$$

When ϕ is implicit, we write

$$L \rtimes R,$$

and say $L \rtimes R$ is a semi-direct product of $\underbrace{L \text{ and } R}$.

Since different ϕ may yield different groups

though "and" is a conjunction that's usually apathetic of order, L and R play vastly different roles!

Rmk Why $\rtimes$? Usually, people write $N \triangleleft G$ when N is a normal subgroup of G. $\rtimes$ is the bastard child of $\triangleleft$ (normal) and $\times$ (product).

Be warned: $L \rtimes R$ does NOT mean $L \triangleleft R$.

Rather, it means $L \triangleleft L \rtimes R$.

Last time I told you

that any

$$L \longrightarrow H \underset{j}{\overset{}{\rightleftarrows}} R$$

gave rise to a map

$$R \longrightarrow \mathrm{Aut}(L).$$

How? By conjugation. Since

$$L \subset H \text{ is normal},$$

$$C_h : L \longrightarrow L$$
$$l \longmapsto h l h^{-1}$$

is a group automorphism of L.

By essentially the same arguments

as in your homework, we have a

homom.

$$H \longrightarrow \mathrm{Aut}(L)$$
$$h \longmapsto C_h.$$

The composition

$$R \xrightarrow{j} H \longrightarrow \mathrm{Aut}(L)$$

is the homomorphism ϕ.

So how does R act on $L \triangleleft L \rtimes R$?

Prop'n

$$(1_L, r)\cdot(\ell, 1_R)\cdot(1_L, r^{-1})$$

$$= (\phi_r(\ell), 1_R).$$

In other words, in $L \rtimes R$, conjugation by r recovers ϕ_r.

Pf $(1_L, r)\cdot(\ell, 1_R)\cdot(1_L, r^{-1})$

$= (1_L \cdot \phi_r(\ell), r\cdot 1_R)\cdot(1_L, r^{-1})$

$= (\phi_r(\ell)\cdot\phi_r(1_L), r\cdot r^{-1})$

$= (\phi_r(\ell\cdot 1_L), 1_R)$

$= (\phi_r(\ell), 1_R)$ //

We now have enough ingredients to prove the theorem from last time.

The spine of thought is:

- If $L \subset H$ is normal, $H \curvearrowright L$ by conjugation.
- Given a splitting $L \subset H \underset{j}{\leftrightarrows} R$, so does R. $\rightsquigarrow R \xrightarrow{\phi} \mathrm{Aut}(L)$
- $L \rtimes R$ is a group where R's conjugation action on L agrees w/ ϕ.

Now let's prove $H \cong L \rtimes R$!

To see why $L \rtimes R \cong H$, we need a lemma. I asserted it without proof before.

Lemma ① $\forall\, h \in H$, $\exists!$ $\ell \in L$, $r \in R$ s.t.

$$h = \ell \cdot j(r).$$

Lemma ② Consider the homomorphisms

$$\begin{array}{ccc} h & H & \xrightarrow{\psi} R. \\ \downarrow & {\scriptstyle q}\downarrow & \\ Lh & H/L & \end{array}$$

homom. in the SES $L \to H \xrightarrow{\psi} R$.

Then the function
$$\begin{aligned} H/L &\xrightarrow{z} R \\ [h] &\longmapsto \psi(h) \end{aligned}$$

is a gp isom s.t. $\psi = z \circ q$.

Pf (of lemma ②):

This is well-defined because if

$$[h] = [h'],$$

then $h = \ell' h'$ for some $\ell' \in L$,

so

$$\psi(h) = \psi(\ell' h') = \psi(\ell')\cdot\psi(h') = 1_L\, \psi(h') = \psi(h')$$

Now $\psi = z \circ q$ is obvious:

$$z \circ q(h) = z([h]) = \psi(h).$$

It's injective because

$$\begin{aligned} z([h]) = 1_R &\Rightarrow \psi(h) = 1_R \\ &\Rightarrow h \in \mathrm{Ker}(\psi) = L \\ &\Rightarrow [h] = L = 1_{H/L} \end{aligned}$$

It's surjective b/c $\psi: H \to R$ is — $\forall r$, $r = \psi(h)$ for some $h \in H$, so

$$r = z([h]). \quad //$$

Pf (of Lemma ①):

We know that the diagram

$$\begin{tikzcd} H \arrow[r, "\psi"] \arrow[d, "q"'] & R \\ H/L \arrow[ur, "z"'] & \end{tikzcd}$$

is commutative. (I.e., $z \circ q = \psi$.)

Given a splitting $H \xleftarrow{j} R$,

we see that

$$z \circ q \circ j = \psi \circ j \underbrace{=}_{\text{defn of splitting}} id_R$$

Since z is an isomorphism,

it has an inverse z^{-1}:

$$q \circ j = z^{-1}.$$

z^{-1} is also a grp $\cong$ (by your homework, for instance).

That z^{-1} is a bijection means $\forall\ h \in H$,

$\exists!\ r$ s.t. $\quad q \circ j(r) = [h] \in H/L$

$\Rightarrow \exists!\ r \in R$ s.t. $j(r) \in Lh = [h]$.

$\Rightarrow \exists!\ r \in R$ s.t. $[j(r)] = [h]$

$\Rightarrow \exists!\ r \in R$ s.t. $h = l \cdot j(r)$ for some $l \in L$.

Of course, given h and $j(r)$,

l is uniquely determined:

$$l = h \cdot j(r)^{-1}.$$

So indeed, $\forall h \in H, \exists!\ l, r$ s.t. $h = l \cdot j(r)$. //

Now we can prove:

Thm Let $L \to H \overset{j}{\leftrightarrows} R$ be a split SES, and $\phi : R \to \mathrm{Aut}(L)$ the induced action. Then

$$H \cong L \rtimes_\phi R.$$

ϕ_r is the homom

$$L \longrightarrow L$$
$$l \longmapsto j(r)\, l\, j(r)^{-1}.$$

Pf: Consider the map

$$L \rtimes_\phi R \xrightarrow{\alpha} H$$
$$(l, r) \longmapsto l \cdot j(r)$$

Then

$$(l_1 \cdot \phi_{r_1}(l_2), r_1 r_2) \mapsto l_1 \phi_{r_1}(l_2)\, j(r_1) j(r_2)$$

But by definition,

$$\phi_{r_1}(l_2) = j(r_1)\, l_2\, j(r_1)^{-1}$$

Hence

$$\begin{aligned}
\alpha\big((l_1, r_1)(l_2, r_2)\big) &= \alpha\big((l_1 \phi_{r_1}(l_2), r_1 r_2)\big) \\
&= l_1 \phi_{r_1}(l_2)\, j(r_1) j(r_2) \\
&= l_1\, j(r_1)\, l_2\, j(r_1)^{-1} j(r_1) j(r_2) \\
&= l_1\, j(r_1)\, l_2\, j(r_2) \\
&= \alpha\big((l_1, r_1)\big)\, \alpha\big((l_2, r_2)\big).
\end{aligned}$$

So α is a homomorphism.

By Lemma ①, $\forall\, h \in H$, $\exists!\, l \in L$, $r \in R$ s.t.

$$h = l \cdot j(r).$$

Hence α is a bijection. //

This is enough to show that split SESs are the same amount of data as semidirect products:

- Given $\begin{tikzcd} L \arrow[r] & H \arrow[r, "\psi"'] & R \arrow[l, bend right, "j"'] \end{tikzcd}$, we get $\Phi: R \to \mathrm{Aut}(L)$ by conjugation
- By theorem, $H \xleftarrow{\alpha} L \rtimes R$ is an $\cong$.
- So we have a surjection $L \rtimes R \xrightarrow{\alpha} H \xrightarrow{\psi} R$.
- Since α is an $\cong$, $\mathrm{Ker}(\psi \circ \alpha) = \alpha^{-1}(\mathrm{Ker}\,\psi)$.

$$= \alpha^{-1}(L).$$
$$= \{(\ell, 1_R)\} \subset L \rtimes R$$

by Lemma 1.

- So we have a SES

$$\begin{array}{ccccc} L & \longrightarrow & L \rtimes R & \xrightarrow{\psi \circ \alpha} & R \\ \ell & \longmapsto & (\ell, 1_R) & & \end{array}$$

with splitting

$$\begin{array}{ccc} L \rtimes R & \longleftarrow & R \\ (1_L, r) & \longleftarrow\!\shortmid & r \end{array}.$$

The situation can be summarized by saying that the following diagram is commutative:

$$\begin{tikzcd} L \arrow[r] \arrow[d, shift left] & H \arrow[r, "\psi"'] \arrow[d, shift left, "\alpha^{-1}"] & R \arrow[l, bend right, "j"'] \arrow[d, shift left, "id"] \\ L \arrow[r, "\ell \mapsto (\ell, 1_R)"'] \arrow[u, shift left, "id_L"] & L \rtimes R \arrow[r, "\psi \circ \alpha"] \arrow[u, shift left, "\alpha"] & R \arrow[l, bend left, "(1_L, r) \leftarrow\!\shortmid r"] \arrow[u, shift left] \end{tikzcd}$$

(ie, any sub-square you can draw is a commutative square.)

__Ex__ Recall that

$$SO_n(\mathbb{R}) \subset O_n(\mathbb{R})$$

is a subgroup of index 2.

It's also normal. — By def'n, $SO_n(\mathbb{R}) = \mathrm{Kernel}(O_n(\mathbb{R}) \xrightarrow{\det} \mathbb{R}^\times)$, and any kernel is a normal subgroup.

or, by homework, any subgp of index two is normal.

So we have a short exact sequence

$$1 \to SO_n(\mathbb{R}) \to O_n(\mathbb{R}) \to \underset{\substack{\cap \\ \mathbb{R}^\times}}{\overset{\substack{\mathbb{Z}/2\mathbb{Z} \\ \cong}}{\{\pm 1\}}} \to 1$$

This sequence admits many different splittings!

For concreteness, take $n=2$.

$$\begin{tikzcd} SO_2(\mathbb{R}) \arrow[r] & O_2(\mathbb{R}) \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[l, bend left, dashed, "j"] \end{tikzcd}$$

For instance,

$$\begin{array}{ccc} O_2(\mathbb{R}) & \leftarrow & \mathbb{Z}/2\mathbb{Z} : j \\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \longleftarrow & [0] \\ \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} & \longleftarrow & [1] \\ & \text{or} & \\ \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} & \longleftarrow & [1] \\ & \text{or} & \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & \longleftarrow & [1]. \end{array}$$