Lecture 17

Examples of semidirect products

Example $\mathrm{Aff}(\mathbb{R}^n) = \{T_{M,b} \mid M \in GL(n,\mathbb{R}),\ b \in \mathbb{R}^n\}$
where $T_{M,b}(x) = Mx + b$.

let $N = \mathrm{Transl}(\mathbb{R}^n) = \{T_{I,b} \mid b \in \mathbb{R}^n\}$ $\quad T_{I,b}(x) = x + b$
Let $A = \{T_{M,0} \mid M \in GL(n,\mathbb{R})\}$ $\quad T_{M,0}(x) = Mx$

Then $N \leq \mathrm{Aff}(\mathbb{R}^n)$ $\quad A \leq \mathrm{Aff}(\mathbb{R}^n)$
N is normal: $\quad T_{M,b}\, T_{I,c}\, T_{M,b}^{-1} = T_{I,Mc}$

$NA = \mathrm{Aff}(\mathbb{R}^n)$ for $\quad T_{M,b} = \underbrace{T_{I,b}}_{\in N} \circ \underbrace{T_{M,0}}_{\in A}$

And $N \cap A = \{T_{I,0}\}$ which is the trivial subgroup.

The map $c : A \to \mathrm{Aut}(N)$ is the conjugation homomorphism.

$$c_{T_{M,0}}(T_{I,b}) = T_{I,Mb}$$

By the proposition, we see that $N \rtimes_c A \cong \mathrm{Aff}(\mathbb{R}^n)$

The group N is isomorphic to $(\mathbb{R}^n, +)$, while A is isomorphic to $GL(n,\mathbb{R})$
the homomorphism $c : A \to \mathrm{Aut}(N)$ corresponds to

$$\alpha : GL(n,\mathbb{R}) \to \mathrm{Aut}(\mathbb{R}^n)$$
$$\alpha_M(b) = M \cdot b$$

So we can also say $\quad \mathbb{R}^n \rtimes_\alpha GL(n,\mathbb{R}) \cong \mathrm{Aff}(\mathbb{R}^n)$.

<u>Another example</u>: Let $N = \mathbb{Z}_7$. There is an automorphism

$$\varphi : \mathbb{Z}_7 \to \mathbb{Z}_7 \qquad \varphi([k]) = [2k]$$

$$\varphi^2([k]) = [4k] \quad , \quad \varphi^3([k]) = [8k] = [k]$$

Thus φ has order 3 in $Aut(\mathbb{Z}_7)$.

Then there is a homomorphism

$$\alpha : \mathbb{Z}_3 \longrightarrow Aut(\mathbb{Z}_7)$$
$$\alpha([k]) = \varphi^k$$

and we can form the semidirect product $\mathbb{Z}_7 \rtimes_\alpha \mathbb{Z}_3$

This is a nonabelian group with 21 elements. Let's do some calculations.

$$([3],[1])([4],[0])$$

$$= ([3] + \alpha_{[1]}([4]) \, , \, [1] + [0])$$

$$= ([3] + \varphi([4]), [1])$$

$$= ([3] + [2 \cdot 4], [1])$$

$$= ([3] + [1], [1])$$

$$= ([4],[1])$$

More generally $([n]_7, [a]_3)([n']_7, [a']_3)$

$$= ([n]_7 + \alpha_{[a]_3}([n']_7), [a]_3 + [a']_3)$$

$$= ([n]_7 + [2^a n']_7 \, , \, [a+a']_3)$$

$$= ([n + 2^a n']_7, [a+a']_3)$$

Group actions

"Group" is an abstract concept, but many examples are "Groups of symmetry transformations" like $Sym(X)$, D_n, $GL(n,\mathbb{R})$, and so on.

Given a group G, it is then natural to ask if we can think of G as symmetries of <u>something</u> (in an abstract sense).

Let X be a set, and let G be a group.

<u>Definition</u>: An <u>action of G on X</u> is a function

$$G \times X \to X \quad \text{denoted} \quad (g,x) \longmapsto g \cdot x$$

Satisfying
(i) $e \cdot x = x$ for all $x \in X$, where e is the idenlity element of G.
(ii) $g \cdot (h \cdot x) = (gh) \cdot x$ for all $g, h \in G$, $x \in X$.

There is another way to think about actions, which is as a homomorphism $\alpha : G \to Sym(X)$, where $Sym(X) = \{ f : X \to X \mid f \text{ bijective} \}$ is the symmetric group of X.

<u>Lemma</u> An action $G \times X \to X$ of a group G on a set X determines and is determined by a homomorphism

$$\alpha : G \to Sym(X)$$
$$g \mapsto \alpha_g$$

where $\alpha_g(x) = g \cdot x$

Proof * Let $G \times X \to X$ $(g,x) \mapsto g\cdot x$ be a group action.
For each $g \in G$, let $\alpha_g : X \to X$ be the function $\alpha_g(x) = g\cdot x$. We claim α_g is bijective. In fact, its inverse is $\alpha_{g^{-1}}$ for $\alpha_{g^{-1}}(\alpha_g(x)) = g^{-1}\cdot(g\cdot x)$

$= (g^{-1}g)\cdot x = e\cdot x = x$ by axioms of a group action.

So for all $g \in G$, $\alpha_g \in \mathrm{Sym}(X)$, and $\alpha : G \to \mathrm{Sym}(X)$ is a function.
Last, we check α is a homomorphism:

$$\alpha_{gh}(x) = (gh)\cdot x = g\cdot(h\cdot x) = \alpha_g(\alpha_h(x)) \quad (\text{all } x \in X)$$

so $\alpha_{gh} = \alpha_g \circ \alpha_h$, as desired.

* Conversely, suppose $\alpha : G \to \mathrm{Sym}(X)$ is a homomorphism.
Define a function $G \times X \to X$ by declaring $g\cdot x = \alpha_g(x)$

We must check the axioms of a group action.
(i) since α is a homomorphism, it take identity to identity.
thus $\alpha_e = \mathrm{Id}_X$ where $\mathrm{Id}_X : X \to X$ is the identity function.
so $e\cdot x = \alpha_e(x) = \mathrm{Id}_X(x) = x$, as desired.
(ii) since α is a homomorphism, $\alpha_{gh} = \alpha_g \circ \alpha_h$
so $(gh)\cdot x = \alpha_{gh}(x) = \alpha_g(\alpha_h(x)) = g\cdot(h\cdot x)$, as desired. ▨

Due to this lemma, we will often switch between the two "pictures" of a group action: (a) A map $G \times X \to X$
(b) a map $G \to \mathrm{Sym}(X)$

Definition 5.1.1 in the book corresponds to picture (b).

__Examples__ (1) X any set, $G = \mathrm{Sym}(X)$ symmetric group.
$\mathrm{Sym}(X)$ acts on X.

$$\mathrm{Sym}(X) \times X \to X$$
$$(\sigma, x) \to \sigma(x) \quad \text{(apply function } \sigma \text{ to } x\text{)}$$

The corresponding homomorphism $\alpha : \mathrm{Sym}(X) \to \mathrm{Sym}(X)$ is the identity.

(2) Let $H \leq \mathrm{Sym}(X)$ be a subgroup. Then H acts on X similarly to example (1).

(3) $X = \mathbb{R}^n \quad G = GL(n, \mathbb{R})$

$$GL(n, \mathbb{R}) \times \mathbb{R}^n \to \mathbb{R}^n$$
$$(A, \vec{x}) \mapsto A\vec{x}$$ multiply vector and matrix.

Also any subgroup of $GL(n, \mathbb{R})$ acts on $\mathbb{R}^n$.

(4) Given a group G, we can take $X = G$, and find several actions of G on itself.

(4a) recall Left multiplication $L_g : G \to G \quad L_g(h) = gh$.
We saw in lecture 10 that this gives a homomorphism

$$L : G \to \mathrm{Sym}(G)$$
$$g \mapsto L_g$$

So this is a group action of G on G, called __left multiplication__.
(The corresponding map $G \times G \to G$ is just multiplication).

(4b) For $g \in G$, we have conjugation by g: $c_g : G \to G$
$c_g(h) = ghg^{-1}$. We saw in lecture 22 that the function $c : G \to \mathrm{Aut}(G)$, $g \mapsto c_g$.
is a homomorphism. Now $\mathrm{Aut}(G)$ is a subgroup of $\mathrm{Sym}(G)$, so we can also regard conjugation as a homomorphism.

$$c : G \to \mathrm{Sym}(G)$$

This is called the __conjugation action__.
$$G \times G \to G$$
$$(g, h) \mapsto ghg^{-1}$$

What about right multiplication? $R_g : G \to G$ $R_g(h) = hg$
This does define a function $G \to Sym(G)$
$g \mapsto R_g$
But unless G is abelian, this function is NOT A HOMOMORPHISM.
For $R_{gh}(x) = xgh = R_h R_g(x)$, so $R_{gh} = R_h \circ R_g$,
and $R_{gh} \neq R_g \circ R_h$ unless $gh = hg$.

On the other hand, $\alpha : G \to Sym(G)$ $\alpha_g(x) = xg^{-1}$
$\alpha_g = R_{g^{-1}}$
is a homomorphism!

$$\alpha_{gh}(x) = x(gh)^{-1} = xh^{-1}g^{-1} = R_g(R_h(x)) = \alpha_g(\alpha_h(x))$$

So "right multiplication by the inverse" is a group action of G on G.

Some basic sets associated to a group action.

Definition: Let $G \times X \to X$ be a group action.

(1) For $x \in X$, the set $G \cdot x = \{g \cdot x \mid g \in G\}$ is called the orbit of x (the book uses $\mathcal{O}(x)$ for this.)

(2) The action is transitive if there is an $x \in X$ such that $G \cdot x = X$.

(3) For $x \in X$, the stabilizer of x is
$$Stab(x) = \{g \in G \mid g \cdot x = x\}$$
it is a subset of G.

(4) The kernel of the action is $\ker(\alpha : G \to Sym(X))$
it equals $\bigcap_{x \in X} Stab(x)$