Lecture notes for Introduction to Modern Algebra I: Lecture 15

1 Semidirect product

1.1 Inner semidirect product

In general the product of two subgroups is not a subgroup. Take for example H=$\langle(12)\rangle$ and K=$\langle(13)\rangle$ in S_3, where $KH = \{(1), (12), (13), (132)\}$, which can not be a subgroup because the order is 4 and does not divide 6. However when one of the subgroups, say for example K is normal, we do have a subgroup. We have the identity:

$$(kh)(k'h') = (k(hk'h^{-1})hh') \in KH \quad \text{and} \quad (kh)^{-1} = h^{-1}k^{-1} = ((h^{-1}k^{-1}h)h^{-1}) \in KH.$$

What this formula is saying is that the group H acts on the normal group K via the inner automorphism $\varphi_h(k') = hk'h^{-1}$.

Definition 1. Let G be a group and H, K subgroups of G. Let us assume:

(1) K is normal in G. (H may not be necessarily normal).

(2) $K \cap H = \{e\}$.

(3) $KH = G$.

Then we say that G is the internal semidirect product of K and H and it is written $K \rtimes H = G$.

Example 2. The semidirect product of abelian subgroups can result on a group that is not abelian. For example, the dihedral group $\mathbb{D}_n$ is isomorphic to the semidirect product $\mathbb{Z}_n \rtimes \mathbb{Z}_2$. In this example $K = \langle r\rangle \cong \mathbb{Z}_n$ is the cyclic subgroup of rotations and $H = \langle s\rangle \cong \mathbb{Z}_2$ is the subgroup generated by s.

Example 3. Let $G = \mathrm{SL}(2, \mathbb{R})$, $K = \mathrm{SL}(2, \mathbb{R})$ and $H = \{\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{R}^\times\}$

1.2 Group Automorphisms

Definition 4. Let G be a group. A group automorphism is a group isomorphism $\sigma\colon G \longrightarrow G$. This means that we have:

(1) A bijection $\sigma\colon G \longrightarrow G$,

(2) such that $\sigma(g * g') = \sigma(g) * \sigma(g')$ for all elements $g, g' \in G$.

Example 5. The identity $\mathrm{Id}\colon G \longrightarrow G$ is a group automorphism in any group G. For any isomorphism $\sigma\colon G \longrightarrow G$, we have also the inverse map as an isomorphism $\sigma^{-1}\colon G \longrightarrow G$.

Proposition 6. *The set of isomorphisms $\sigma\colon G \longrightarrow G$ form a group under composition, with the identity isomorphism as neutral element. This group is denoted by $Aut(G)$.*

Example 7. For any group G and $x \in G$, the group isomorphism $\varphi_x\colon G \longrightarrow G$ given by $\varphi_x(y) = xyx^{-1}$ is an element of $\mathrm{Aut}(G)$. Isomorphisms of this kind are called inner automorphisms of G. It can be shown that inner automorphisms form a normal subgroup $\mathrm{Inn}(G)$ in $\mathrm{Aut}(G)$.

Example 8. Since the element 1 generates $\mathbb{Z}$, the image $\sigma(1)$ must be a generator as well. As a consequence, for the group $G = (\mathbb{Z}, +)$ the group of automorphisms is $\mathrm{Aut}(\mathbb{Z}) = \{\mathrm{Id}, -\mathrm{Id}\}$.

Example 9. Consider the group $G = (\mathbb{Z}_n, +)$. Again, the image $\sigma(1) = k$ must be a generator of G and the group of automorphisms $\mathrm{Aut}(\mathbb{Z}_n)$ becomes the multiplicative group $\mathbb{Z}_n^\times$ of residues mod n.

1.3 Outer semidirect product

Let G be a group. In our study of the product of two subgroups groups K and H, we saw how, when the group K normal, we obtain a subgroup KH and the the group H acts on K via inner automorphisms. For any two groups K and H, we consider actions of H in K via elements in $\mathrm{Aut}(K)$.

Definition 10. For two groups H and K and an action $\varphi\colon H \longrightarrow \mathrm{Aut}(K)$ of H on K, we define the semidirect product $K \rtimes_\varphi H$ as follows: as a set is just the cartesian product $K \times H$ and the group law is

$$(k, h)(k', h') = (k\varphi_h(k'), hh')$$

1. $(k, h)(1, 1) = (k\varphi_k(1), h) = (k, h)$ and $(1, 1)(k, h) = (1\varphi_1(k), h) = (k, h)$.
2. $(k, h)(\varphi_{h^{-1}}(k^{-1}), h^{-1}) = (\varphi_{h^{-1}}(k^{-1}), h^{-1})(k, h) = (1, 1)$.

Proposition 11. *Inside $K \rtimes_\varphi H$, we have copies*

$$K \cong \{(k, 1)\,|k \in K\} \qquad H \cong \{(1, h)\,|h \in H\}$$

and $(k, h) = (k, 1)(1, h) = (1, h)(\varphi_h^{-1}(k), 1)$. The copy of K in $K \rtimes_\varphi H$ is a normal subgroup with conjugation by h being described by the map φ_h as:

$$(1, h)(k, 1)(1, h)^{-1} = (\varphi_h(k), 1)$$

In particular, every $(k, 1)$ commutes with every $(1, h)$ if and only the action of H in K given by $\varphi\colon H \longrightarrow Aut(H)$, is the trivial action.

Example 12. Let K be an abelian group and let $\varphi\colon \mathbb{Z}_2 \longrightarrow \mathrm{Aut}(K)$ be given by $\varphi_0 = \mathrm{Id}$ and $\varphi_1 = -\mathrm{Id}$. The operation on the group $K \rtimes_\varphi \mathbb{Z}_2$ is given by:

$$(k, a)(k', a') = (k + (-1)^a k', a + a' \bmod 2).$$

In general the group obtained may not be abelian:

$$(k, 0)(0, 1) = (k, 1) \qquad \text{and} \qquad (0, 1)(k, 0) = (-k, 1).$$

For example for $K = \mathbb{Z}_n$ and $n \geq 3$, the group $\mathbb{Z}_n \rtimes_\varphi \mathbb{Z}_2$ is the Dihedral group, where we are identifying $r = (1, 0)$ and $s = (0, 1)$. For example we get our usual relation

$$sr = (0, 1)(1, 0) = (-1, 1) = (-1, 0)(0, 1) = r^{-1}s.$$

1.4 Exact sequences

We introduce here the useful language of exact sequences.

Definition 13. We say that a sequence of group homomorphisms $G \xrightarrow{f} G' \xrightarrow{g} G''$ is exact iff $\mathrm{Im}(f) = \ker(g)$. We say that a sequence $\ldots G \to G' \to G'' \ldots$ is exact when is exact in every short piece $G \to G' \to G''$.

Example 14. We have the following:
(a) $0 \to G \xrightarrow{f} G'$ is exact iff $f\colon G \longrightarrow G'$ is injective.
(b) $G \xrightarrow{f} G' \to 0$ is exact iff $f\colon G \longrightarrow G'$ is surjective.

Theorem 15. *Let $1 \to K \xrightarrow{\beta} G \xrightarrow{\alpha} H \to 1$ be a short exact sequence. There exist group a homomorphism (a retraction) $r\colon G \longrightarrow K$ such that $r \circ \beta = id_K$ if and only G is isomorphic to the direct product $\theta\colon G \cong K \times H$, in such a way that we have the commutative diagram*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K & \xrightarrow{\beta} & G & \xrightarrow{\alpha} & H & \longrightarrow & 1 \\ & & {\scriptstyle id}\big\downarrow & & {\scriptstyle \theta}\big\downarrow & & {\scriptstyle id}\big\downarrow & & \\ 1 & \longrightarrow & K & \xrightarrow{i_1} & K \times H & \xrightarrow{p_2} & H & \longrightarrow & 1 \end{array}.$$

Proof. (Sketch of the proof) If we have such homomorphism $r\colon G \longrightarrow K$, we can build the map $\theta\colon G \longrightarrow K \times H$ as $\theta = (r, \alpha)$. On the other hand, if we have a map $\theta\colon G \longrightarrow K \times H$, we get a retraction $r\colon G \longrightarrow K$ from the identity $\theta(g) = (r(g), \alpha(g))$ for all $g \in G$. $\square$

Theorem 16. *Let $1 \to K \xrightarrow{\beta} G \xrightarrow{\alpha} H \to 1$ be a short exact sequence. There exist group a homomorphism (a section) $s\colon H \longrightarrow G$ such that $\alpha \circ s = id_H$ if and only it is possible to build an action $\varphi\colon H \longrightarrow Aut(K)$ such that G is isomorphic to the* *semidirect product $K \rtimes_\varphi H$ of K and H and the map $\theta\colon G \cong K \rtimes_\varphi H$ can be fitted into a commutative diagram*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K & \xrightarrow{\beta} & G & \xrightarrow{\alpha} & H & \longrightarrow & 1 \\ & & {\scriptstyle id}\big\downarrow & & {\scriptstyle \theta}\big\downarrow & & {\scriptstyle id}\big\downarrow & & \\ 1 & \longrightarrow & K & \xrightarrow{i_1} & K \rtimes_\varphi H & \xrightarrow{p_2} & H & \longrightarrow & 1 \end{array} .$$

Proof. (Sketch of the proof) Suppose that we have a section $s\colon H \longrightarrow G$ and fix an element $h \in H$. For any $k \in K$, the element $s(h)\beta(k)s(h)^{-1} \in G$ belongs to $\ker(\alpha)$ since

$$\alpha(s(h)\beta(k)s(h)^{-1}) = \alpha(s(h))\alpha(\beta(k))\alpha(s(h))^{-1} = e_H.$$

Since the sequence is exact $\ker(\alpha) = \mathrm{Im}(\beta) \Rightarrow \exists k' \in K, \beta(k') = s(h)\beta(k)s(h)^{-1}$. The element k' satisfying this property is unique, given k and we define $\varphi_h(k) = k'$. In this way we have an action of H on K (a map $H \longrightarrow \mathrm{Aut}(K)$). To obtain a map $\theta'\colon K \rtimes_\varphi H \longrightarrow G$, we put $\theta'(k,h) = \beta(k)s(h)$.
The other way around, if we have $\theta\colon G \cong K \rtimes_\varphi H$, we get a section $s\colon H \longrightarrow G$ with the formula $s(h) = \theta'(1,h) = \theta^{-1}(1,h)$. □

Practice Questions:

1. Show that the dihedral group $\mathbb{D}_n$ is isomorphic to the semidirect product $\mathbb{Z}_n \rtimes \mathbb{Z}_2$.