Semidirect Product

Liming Pang

1 Semidirect Product

Definition 1. $G$ and $G'$ are groups, and $\phi : G' \rightarrow Aut(G)$ is a homomorphism. The semidirect product of $G$ and $G'$ with respect to $\phi$ is the group $G \rtimes_{\phi} G'$ whose underlying set is same as that of $G \times G'$, and the law of composition is defined by

$$(g_1, g'_1)(g_2, g'_2) = (g_1\phi_{g'_1}(g_2), g'_1g'_2)$$

Proposition 2. $G \rtimes_{\phi} G'$ defined above is a group.

Proof. (1). For any $(g_1, g'_1), (g_2, g'_2), (g_3, g'_3) \in G \rtimes_{\phi} G'$,

$$(g_1, g'_1)(g_2, g'_2)(g_3, g'_3) = (g_1\phi_{g'_1}(g_2), g'_1g'_2)(g_3, g'_3)$$

$$(g_1, g'_1)(g_2, g'_2)g_3(g_2, g'_2) = (g_1\phi_{g'_1}(g_2g_3), (g_1g_2)g_3)$$

$$(g_1, g'_1)(g_2\phi_{g'_2}(g_3), g'_2g'_3)$$

$$(g_1, g'_1)((g_2, g'_2)(g_3, g'_3)) = (g_1, g'_1)(g_2, g'_2)(g_3, g'_3)$$

(2). The identity element is $(1, 1')$: for any $(g, g')$

$$(1, 1')(g, g') = (1\phi_{1'}(g), 1'g') = (g, g')$$

and $(g, g')(1, 1') = (g\phi_{g'}(1), g'1') = (g, g')$

(3). $(g, g')^{-1} = (\phi_{(g')}^{-1}(g^{-1}), (g')^{-1})$:

$$(g, g')(\phi_{(g')}^{-1}(g^{-1}), (g')^{-1}) = (g\phi_{g'}(\phi_{(g')}^{-1}(g^{-1})), g'(g')^{-1})$$

$$(g\phi_{g'}(\phi_{(g')}^{-1}(g^{-1})), g'(g')^{-1}) = (g\phi_{g'}(g^{-1}), 1') = (1, 1')$$

$$(\phi_{(g')}^{-1}(g^{-1}), (g')^{-1})(g, g') = (\phi_{(g')}^{-1}(g^{-1})\phi_{(g')}^{-1}(g), (g')^{-1}g') = (\phi_{(g')}^{-1}(g^{-1}g), 1') = (1, 1')$$

$\square$
Example 3. If $G' \longrightarrow \text{Aut}(G)$ is the trivial homomorphism, then $G \rtimes_\phi G' = G \times G'$, so the product group is a special case of the semidirect product group.

We can regard $G$ and $G'$ as subgroups of $G \rtimes_\phi G'$ via the inclusion maps

$$i_1 : G \longrightarrow G \rtimes_\phi G'$$

$$g \mapsto (g, 1')$$

$$i_2 : G' \longrightarrow G \rtimes_\phi G'$$

$$g \mapsto (1, g')$$

**Proposition 4.** $i_1(G)$ is a normal subgroup of $G \rtimes_\phi G'$. In particular, for any $g \in G$, $g' \in G'$:

$$(1, g')(g, 1')(1, g')^{-1} = (\phi_{g'}(g), 1')$$

**Proof.** For any $(x, y) \in G \rtimes_\phi G'$, $(g, 1') \in i_1(G)$:

$$(x, y)(g, 1')(x, y)^{-1} = (x\phi_y(g), y)(\phi_{y^{-1}}(x^{-1}), y^{-1})$$

$$= (x\phi_y(g)\phi_y(\phi_{y^{-1}}(x^{-1})), yy^{-1})$$

$$= (x\phi_y(g)x^{-1}, yy^{-1})$$

So $i_1(G)$ is a normal subgroup of $G \rtimes_\phi G'$, and the above computation implies

$$(1, g')(g, 1')(1, g')^{-1} = (\phi_{g'}(g), 1')$$

by taking $(x, y) = (1, g')$.

**Corollary 5.** If $\phi : G' \longrightarrow \text{Aut}(G)$ is not the trivial homomorphism, then $G \rtimes_\phi G'$ is a non-abelian group.

Similar to the study of product groups, we are interested in the question: Given a group $G$, can we find its subgroups $H$ and $K$ such that $G$ is the semidirect product of $H$ and $K$?

More specifically, if $G$ is a group, $H$ is a normal subgroup of $G$ and $K$ is a subgroups of $G$, define $\phi : K \longrightarrow \text{Aut}(H)$ by $\phi_k(h) = khk^{-1}$. Then we can define a map

$$f : H \rtimes_\phi K \longrightarrow G$$

$$(h, k) \mapsto hk$$

and we would like to see when $f$ is an isomorphism.
Theorem 6. $G$ is a group, $H$ is normal subgroup of $G$ and $K$ is a subgroup of $G$. Then

$$f : H \rtimes_{\phi} K \longrightarrow G$$

defined above is an isomorphism if and only if $H \cap K = \{1\}$, and $HK = G$.

Proof. If $f$ is an isomorphism, it follows easily that $H \cap K = \{1\}$, and $HK = G$.

If $H \cap K = \{1\}$, and $HK = G$, we will show that $f$ is an isomorphism. First, for any $(h_1, k_1), (h_2, k_2) \in H \rtimes_{\phi} K$:

$$f((h_1, k_1(h_2, k_2)) = f((h_1(k_1 h_2 k_1^{-1}), k_1 k_2))$$
$$= h_1(k_1 h_2 k_1^{-1}) k_1 k_2$$
$$= h_1 k_1 h_2 k_2$$
$$= f((h_1, k_1)) f(h_2, k_2)$$

So $f$ is a homomorphism.

If $f((h, k)) = hk = 1$, then $h = k^{-1} \in H \cap K = \{1\}$, $h = k = 1$, so $\ker(f)$ is trivial, $f$ is injective. $f$ is surjective since $G = HK = \text{Im}(f)$. \hfill $\square$

Remark 7. If the above map $f : H \rtimes_{\phi} K \longrightarrow G$ is an isomorphism, we usually write $G = H \rtimes K$. The symbol $\phi$, which stands for the conjugation action of $K$ on $H$, is omitted.

Example 8. Consider the group $M_n$ of isometries on $\mathbb{R}^n$. We know it has a normal subgroup $T_n$ (the subgroup of translations) and a subgroup $O_n$ (the subgroup of orthogonal linear operators). Since $T_n \cap O_n = \{\text{id}\}$ and $T_n O_n = M_n$ (recall that each isometry can be written as a composition of the form $t_{\vec{a}} \phi$), so we conclude $M_n = T_n \rtimes O_n$.

Example 9. $S_3$ has a normal subgroup $H = \langle (1 \ 2 \ 3) \rangle$ and a subgroup $K = \langle (1 \ 2) \rangle$. $H \cap K = \{\text{id}\}$ and $HK = S_3$, so $S_3 = H \rtimes K$.

2 Classification of Groups of Certain Order

Proposition 10. If $p$ is a prime and $G$ is a group of order $2p$, then $G$ is isomorphic to either $\mathbb{Z}/2p\mathbb{Z}$ or $D_p$. 

3
Proof. If $|G| = 2 \times 2 = 4$, we have done the classification before.

If $|G| = 2p$ for some odd prime $p$, by Sylow Theorem, there exists Sylow $p$-subgroup $H$ and Sylow 2-subgroup $K$ of $G$. The number of Sylow $p$-subgroups divides 2 and congruent to 1 modulo $p$, so it has to be 1, we get $H$ is a normal subgroup of $G$.

$H \cap K = \{1\}$ since $|H| = p$ and $|K| = 2$ are relatively prime.

$HK = G$ since $|HK| = \frac{|H| |K|}{|H \cap K|} = 2p = |G|$

By Theorem 6,

$$G = H \times K \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

where $\phi : \mathbb{Z}/2\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/p\mathbb{Z})$ is a homomorphism.

The homomorphism is determined by $\phi(\bar{1})$. Since the order of $\bar{1} \in \mathbb{Z}/2\mathbb{Z}$ is 2, the order of $\phi(\bar{1}) \in \text{Aut}(\mathbb{Z}/p\mathbb{Z})$ has to be 1 or 2.

Recall that $\text{Aut}(\mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$, the group of units. If $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$ satisfies $\bar{a}^2 = \bar{1}$, then $p$ divides $a^2 - 1 = (a - 1)(a + 1)$, so $p$ divides $a - 1$ or $p$ divides $a + 1$, i.e. $\bar{a} = \bar{1}$ or $\bar{a} = -\bar{1}$. This implies the only automorphisms whose order is divisible by 2 is the identity map $\phi(\bar{1})(\bar{k}) = \bar{k}$ and the map $\phi(\bar{1})(\bar{k}) = -\bar{k}$.

If $\phi(\bar{1})(\bar{k}) = \bar{k}$, then $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2p\mathbb{Z}$.

If $\phi(\bar{1})(\bar{k}) = -\bar{k}$, then $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is not abelian, so it is not isomorphic to the first case.

Since these are the only two possible isomorphic classes for a group of order $2p$, and $|D_p|$ is a non-abelian group of order $2p$, so $D_p$ has to be isomorphic to the second case. We conclude that a group of order $2p$ is isomorphic to either $\mathbb{Z}/2p\mathbb{Z}$ or $D_p$.

The proof of the following proposition is a great summary of what we have learned about group theory in this course.

**Proposition 11.** There are five isomorphic classes of groups of order 12.

Proof. $|G| = 12 = 2^2 \times 3$, so it has a Sylow 2-subgroup $H$ and a Sylow 3-subgroup $K$. The number of Sylow 2-subgroups can be 1 or 3, and the number of Sylow 3-subgroups can be 1 or 4.

If there are 4 subgroups of order 3, then there are only $12 - 1 - 4 \times (3 - 1) = 3$ elements outside the union of there four Sylow 3-subgroups, so there is only space for at most 1 Sylow 2-subgroup. We conclude either $H$ or $K$ is a normal subgroup of $G$.

$|H|$ and $|K|$ are relatively prime, so $H \cap K = \{1\}$. $|KH| = |HK| = \frac{|H| |K|}{|H \cap K|} = 12$, so $G = HK = KH$. 

4
\[ |H| = 4 \text{ implies } H \cong \mathbb{Z}/4\mathbb{Z} \text{ or } H \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}; \ |K| = 3 \text{ implies } K = \mathbb{Z}/3\mathbb{Z}. \]

Case 1. If both of \(|H|\) and \(|K|\) are normal subgroups of \(G\), then \(G = H \times K\).
  
  Case 1.(a) \(G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}\)
  
  Case 1.(b) \(G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}\).

Case 2. If \(H\) is normal and \(K\) is not normal, \(G = H \rtimes K\) and it is not direct product.
  
  Case 2a. \(G \cong \mathbb{Z}/4\mathbb{Z} \times \phi \mathbb{Z}/3\mathbb{Z}, \ \phi : \mathbb{Z}/3\mathbb{Z} \longrightarrow \text{Aut}(\mathbb{Z}/4\mathbb{Z}) \cong (\mathbb{Z}/4\mathbb{Z})^\times = \{1_4, 3_4\}\). So \(|\text{Aut}(\mathbb{Z}/4\mathbb{Z})| = 2\) and \(|\mathbb{Z}/3\mathbb{Z}| = 3\), there is no nontrivial homomorphism \(\phi\) in this case.
  
  Case 2b. \(G \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \ltimes \phi \mathbb{Z}/3\mathbb{Z}, \ \phi : \mathbb{Z}/3\mathbb{Z} \longrightarrow \text{Aut}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong S_3\). \(\phi\) is determined by \(\phi(1_3)\), and \(|1_3| = 3\), so \(1\) is mapped to one of the two 3-cycles in \(S_3\). These two choices will give isomorphic semi-direct product group structure since there is an automorphism of \(S_3\) switching the two 3-cycles. In this case there is a unique semi-direct product structure.

Case 3. If \(K\) is normal and \(H\) is not normal, \(G = K \rtimes H\) and it is not direct product.
  
  Case 3a. \(G \cong \mathbb{Z}/3\mathbb{Z} \times \phi \mathbb{Z}/4\mathbb{Z}, \ \phi : \mathbb{Z}/4\mathbb{Z} \longrightarrow \text{Aut}(\mathbb{Z}/3\mathbb{Z}) \cong (\mathbb{Z}/3\mathbb{Z})^\times = \{1_3, 2_3\}\). \(\phi\) is determined by \(\phi(1_4)\) and \(\phi\) is not trivial, so \(\phi(1_4)\) is the map \(k_3 \mapsto 2\bar{k}_3 = -\bar{k}_3\), and \(\phi(\bar{m}_4) = (\bar{k}_3 \mapsto (-1)^m\bar{k}_3)\). In this case there is a unique semi-direct product structure.
  
  Case 3b. \(G \cong \mathbb{Z}/3\mathbb{Z} \times \phi(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}), \ \phi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow \text{Aut}(\mathbb{Z}/3\mathbb{Z}) \cong (\mathbb{Z}/3\mathbb{Z})^\times = \{1_3, 2_3\}\). The three non-identity elements in \(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\) are all of order 2, so if \(\phi\) is not trivial, it has to be the case two of these three elements map to \(2_3\) and the remaining one maps to \(1_3\). And the difference choices of the element sending to \(1_4\) give isomorphic semidirect product groups. In this case this is a unique semi-direct product structure.
  
  The above discussion produces all the five possible isomorphic classes of groups of order 12.

\[ \square \]

Remark 12. The group \(A_4\) is isomorphic Case 2b, and the group \(D_6\) is isomorphic to Case 3b.
3 Semidirect Product Structure of Rubik’s Cube Group

The Rubik’s Cube is a famous mathematical toy that is invented by Ernő Rubik in 1974. It is a cube each of whose faces has a distinct colour. For the classic $3 \times 3 \times 3$ Rubik’s Cube, each face is subdivided into 9 sub-faces so that the cube is made up by 26 blocks of small cubes: 8 corner blocks (each contains 3 colours), 12 edge blocks (each contains 2 colours) and 6 centre blocks (each contains 1 colour). The 9 pieces forming one of the faces of the cube can be rotated together by multiples of 90 degrees. The goal of the game is to recover a given rotated cube to its original configuration.

After invention, solution algorithms have been found (if you search online, you can find many articles about how to solve a Rubik’s Cube), and generalisations to higher orders and other shapes have also been developed. From a mathematical point of view, it is a good game for the applications of group theory.

Definition 13. The Rubik’s Cube Groups $\Gamma$ is the group of all moves of a $3 \times 3 \times 3$ Rubik’s Cube, with the law of composition be the composition of moves. (Two moves are identified to be the same if the configurations of the Rubik’s cube under these moves are the same)

An important but obvious observation is that each element in $\Gamma$ can be written as a finite sequence of composition of the following elements:

$$U, D, F, B, L, R$$
These elements denote the clockwise rotation by 90 degree of the Up, Down, Front, Back, Left and Right face respectively. Each of these six elements is of order 4.

Let $V$ denote the set of 8 corner blocks and $E$ the set of 12 edge blocks of the Rubik’s Cube. Each move will induce a permutation on $V$ and on $E$ respectively. We obtain a homomorphism:

$$\psi : \Gamma \longrightarrow S_V \times S_E$$

sending each move to its permutation effect on $V$ and $E$, where $S_V \cong S_8$ and $S_E \cong S_{12}$ are the permutation groups of $V$ and $E$ respectively.

The kernel of this homomorphism, $\Gamma_0 = \ker \psi$, is the normal subgroup of $\Gamma$ consisting of those moves that do not permute the blocks.

Next, we can mark some of the faces of the Rubik’s cube in the way that there is a unique marked face in each Vertex block and each edge block. We call a way of such markings an orientation. Once the orientation is determined, the moves that will fix the position of the set of marks will be denoted by $\Gamma_1$.

If a move lies in $\Gamma_0 \cap \Gamma_1$, the it will not permute the blocks and will not change the orientation of any block, so it has to be the identity move, we get $\Gamma_0 \cap \Gamma_1 = \{1\}$

Each move can be decomposed into a move that changes the orientations while fixing the blocks followed by a move that permute the blocks while keeping the orientations, so $\Gamma = \Gamma_0 \Gamma_1$

We conclude that

$$\Gamma = \Gamma_0 \rtimes \Gamma_1$$

There are also further decomposition of $\Gamma_0$ and $\Gamma_1$ into direct or semidirect products of smaller subgroups. With more work, it can be shown that:

$$\Gamma_0 \cong \mathbb{Z}/3\mathbb{Z} \times \ldots \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \ldots \times \mathbb{Z}/2\mathbb{Z}$$

and

$$\Gamma_1 \cong (A_8 \times A_{12}) \rtimes \mathbb{Z}/2\mathbb{Z}$$

There are many interesting topics and results related to the Rubik’s Cube Group $\Gamma$. For example, $|\Gamma| = 2^{27} \times 3^{14} \times 5^3 \times 7^2 \times 11$. It is a finite group implies each element is of finite order, so it follows that if you repeat any
move for some finite number of times, you will turn the Rubik’s cube back to its starting configuration.

What’s more, it has been shown that any element in $\Gamma$ can be written as a composition of at most 26 letters in $U^{\pm 1}, D^{\pm 1}, F^{\pm 1}, B^{\pm 1}, L^{\pm 1}, R^{\pm 1}$. This means the Rubik’s Cube can always be solved within 26 steps of counter clockwise or clockwise 90 degree rotations. If we also count each of $U^2, D^2, F^2, B^2, L^2, R^2$ as a letter, then it can be shown that any element in $\Gamma$ can be written as a composition of at most 20 letters. This means the Rubik’s cube can always be solved within 20 steps of rotations. This number 20 is often referred to as the “God’s number” for Rubik’s Cube.

The reader may refer to some books and articles for more explorations and discussions, for example, “Inside Rubik’s Cube and Beyond” (Birkhuser Boston, 1982) by Christoph Bandelow, and “Adventures in Group Theory” (The Johns Hopkins University Press, 2008) by David Joyner.