# SEMIDIRECT PRODUCT OF GROUPS

Jack Michaels

November 2022

## 1 Introduction to Semidirect Products

Group theory is the study of groups. While it is tempting to immediately jump in and derive the properties associated with certain group constructions, it is natural to step aside and ask the rather dense question: how can you create a new group? And if you have a process that guarantees the creation of a group, can you in some way classify all finite groups? The magnitude of these questions is large, but by answering them we would gain an extremely powerful tool in group theory, specifically via the latter via our ability to recognize all finite groups as we have already seen with the classification of all finite simple groups.

This paper will go about answering these questions using semidirect products, a general way to combine groups. Note, to leverage expectations, the classification of all finite groups is currently an open question. This paper does not serve to solve this problem but instead to offer a discussion of the semidirect product and its role in partially answering this question. This paper will start with a reintroduction to **direct products**, building a foundation on the more intuitive construction. From there, we will proceed with the matured and more general construction: **semidirect products**. An explanation of both **inner** and **outer** semidirect products will be described, along with examples interspersed throughout.

## 2 A Reacquaintance with Direct Products

To aid in your investigation of semidirect products, it will be useful to remind yourself of semidirect products' sibling: direct products.

**Definition 1.** *Let $H$ and $K$ be any two groups and consider the set $S$ of all ordered pairs such that $S = \{(h,k)|h \in H, k \in K\}$. If we define the binary operation (*) on the elements in $S$ as:*

$$(h_1, k_1) * (h_2, k_2) = (h_1h_2, k_1k_2)$$

*for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$ then $S$ becomes a group with (*) becoming the group operation. We call $S$ the **external direct product** of $H$ and $K$ and write it as $H \times K$. Since this formulation is more often used, it is colloquially named as just the **direct product**.*

**Definition 2.** *Let $S$ be any group with subgroups $H$ and $K$ with:*

1. $G = HK$
2. $H \cap K = \{e\}$
3. $H \lhd G$, $K \lhd G$

*then we call $S$ the **internal direct product** of $H$ and $K$. We write this as $S = H \times K$ with $H \times K$ representing the group consiting of elements $\{(h,k)|h \in H, k \in K\}$ with group operation (*) defined by $(h_1, k_1) * (h_2, k_2) = (h_1h_2, k_1k_2)$.*

Both definitions are quite similar, in fact, they result in the same outcome just from different directions. The difference between them comes from the fact that internal direct products form a direct product by investigating what's inside a particular group while external direct products construct an external group from any two groups. Both construct a direct product at the end, however, the external direct product is of more interest since it doesn't require the prior knowledge of $S$. Though these differences largely boil down to semantics, these constructions offer a foundation which will aid our intuition on understanding internal and external semidirect products.

**Corollary 1.** *If $H$ and $K$ are groups, $H \times K$ is indeed a group itself.*

It is left as an exercise to confirm **Corollary 1** and verify that the direct product is indeed a group. This is a trivial proof, it will follow naturally from direct products' construction.

**Corollary 2.** *If $H$ and $K$ are groups, $H$ and $K$ are normal subgroups of $H \times K$*

*Proof.* We will start with proving $H$ is a normal subgroup. Since $K$ is a group, we can imagine the group $H \times \{e\} \subset H \times K$. Let $(h_1, k_1)$ be any element in $H \times K$ and $(h_2, e)$ be any element in $H \times \{e\}$. We see that:

$$\begin{aligned}(h_1,k_1)(h_2,e)(h_1,k_1)^{-1} &= (h_1,k_1)(h_2,e)(h_1^{-1},k_1^{-1})\\ &= (h_1h_2h_1^{-1}, k_1k_1^{-1})\\ &= (h_1h_2h_1^{-1}, e)\\ &\in H \times \{e\}\end{aligned}$$

Thus demonstrating that $H \times \{e\}$ is normal in $H \times K$. All that remains is to prove that $H \times \{e\}$ is indeed a group and that $H \cong H \times \{e\}$. Trivially, we see that $H \times \{e\}$ is indeed a group since $H$ is a group. To see that $H \cong H \times \{e\}$, we can imagine the homomorphism $\phi$ where

$$\begin{aligned}\phi : H \times \{e\} &\to H\\ (h,e) &\mapsto h\end{aligned}$$

We know that

$$\begin{aligned}\phi((h_1,e))\phi((h_2,e)) &= \phi((h_1,e)(h_2,e))\\ h_1h_2 &= \phi((h_1h_2,e))\\ &= h_1h_2\end{aligned}$$

demonstrating that $\phi$ is a valid homomorphism. It is immediately obvious that $\ker(\phi) = \{(e,e)\}$ and $\text{Im}(\phi) = H$ under inspection. This then demonstrates that $\phi$ is a bijection, proving that $\phi$ is an isomorphism so that $H \times \{e\} \cong H$, demonstrating that $H \triangleleft H \times K$. The same argument holds for $K$, demonstrating that $K \triangleleft H \times K$. ■

Now, remind yourself of the question posed in the introduction: how can you create a new group? By leveraging the direct product, we can do just that.

**Example 2.1.** Let $H = \mathbb{Z}_2$ and $K = \mathbb{Z}_3$, or the cyclic groups of order 2 and 3 respectively.

$$\begin{aligned}\mathbb{Z}_2 &= \{0,1\}\\ \mathbb{Z}_3 &= \{0,1,2\}\end{aligned}$$

Meaning that:

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\}$$

Note that $\mathbb{Z}_2 \times \mathbb{Z}_3$ is generated by $(1,1)$, which has order 6. Thus, $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$, demonstrating how an entirely new group can be constructed from the smaller groups $\mathbb{Z}_2$ and $\mathbb{Z}_3$. However, it need **not** always be the case that a **new** group is created.

**Example 2.2.** Let $H = \{e\}$ and $K = \{e\}$, i.e. both $H$ and $K$ are equal to the trivial group.

$$H \times K = \{e\} \times \{e\}$$

Yet, it is trivial that $H \times K \cong \{e\}$ since we can imagine the homomorphism $\phi$ where

$$\begin{aligned}\phi : H \times K &\to H\\ (h,k) &\mapsto h\end{aligned}$$

Since $H$ and $K$ are equal to the trivial group, $\phi$ is trivially a homomorphism since

$$\begin{aligned}\phi((h_1,k_1)(h_2,k_2)) &= \phi((h_1,k_1))\phi((h_2,k_2))\\ \phi((e,e)(e,e)) &= \phi((e,e))\phi((e,e))\\ e &= ee\\ &= e\end{aligned}$$

We trivially know that $\ker(\phi) = \{(e, e)\}$ and $\text{Im}(\phi) = \{e\} = H$, thus $\phi$ is bijective, meaning it is an isomorphism, proving that $H \times K \cong \{e\}$. This thus shows an example of how the direct product doesn't necessarily create a **new** group.

This property is not necessarily bad. When asking how to classify all finite groups, it is trivial that there are a countably infinite number of finite groups (consider all cyclic groups of prime order $p$). Thus, to be able to classify all finite groups, we **must** be able to generalize particular types of finite groups. You may go about this by generating new finite groups via the direct product from a base list of finite groups, for example the already classified simple finite groups. By recursively applying the direct product, you may be able to generate an infinite list of finite groups from two root groups (we see step one of that process in **Example 2.1**). Or on the other hand, the recursive application of the direct product may repeat on itself, trivially demonstrated by **Example 2.2**. In any case, we can identity an infinite number of finite groups by recursively applying the direct product, thus giving us a way to classify all finite groups.

**Lemma 2.1.** *If $H$ and $K$ are abelian groups, then the direct product $H \times K$ must also be abelian.*

*Proof.* Let $H$ and $K$ be abelian groups with $(h_1, k_1), (h_2, k_2) \in H \times K$. We see that:

$$\begin{aligned}(h_1, k_1)(h_2, k_2) &= (h_1h_2, k_1k_2) \\ &= (h_2h_1, k_2k_1) \text{ since } H \text{ and } K \text{ are abelian} \\ &= (h_2, k_2)(h_1, k_1) \quad \blacksquare\end{aligned}$$

Confirming that $H \times K$ is abelian. If you step back to **Example 2.1** you can see how two abelian groups, $\mathbb{Z}_2$ and $\mathbb{Z}_3$ generate the abelian group $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$ via the direct product. Thus, one can leverage direct products to not only classify finite groups, but to aid in the classification of all finite **abelian** groups. This property is one of the largest applications of direct products.

# 3 Semidirect Products

Now, let us define the two forms of the semidirect product:

**Definition 3.** *Let $H$ and $K$ be any two group such that $K$ is a group acting on $H$. Thus, there exists a group homomorphism $\phi : K \to Aut(H)$ which sends $k \in K$ to automorphisms $\phi_k$ of $H$. Consider the set $S$ of all ordered pairs such that $S = \{(h, k) | h \in H, k \in K\}$. If we define the binary operation (*) on the elements in $S$ as:*

$$\begin{aligned}(h_1, k_1) * (h_2, k_2) &= (h_1\phi(k_1)(h_2), k_1k_2) \\ &= (h_1\phi_{k_1}(h_2), k_1k_2)\end{aligned}$$

*then $S$ becomes a group with (*) becoming the group operation. We call $S$ the **outer semidirect product** of $H$ and $K$ and write it as $H \rtimes_\phi K$.*

**Definition 4.** *Let $S$ be any group with subgroups $H$ and $K$ with:*

1. *$G = HK$*
2. *$H \cap K = \{e\}$*
3. *$H \lhd G$*

*then we call $S$ the **inner semidirect product** of $H$ and $K$. We write this as $S = H \rtimes K$ with $H \rtimes K$ representing the group consisting of elements $\{(h, k) | h \in H, k \in K\}$ with group operation (*) defined by $(h_1, k_1) * (h_2, k_2) = (h_1k_1h_2k_1^{-1}, k_1k_2)$. Since conjugation is an automorphism, and since $H \lhd G$, the inner semidirect product restricts our choice of $\phi$:*

$$\begin{gathered}h_1k_1h_2k_1^{-1} = h_1\phi_{k_1}(h_2) \\ (h_1, k_1) * (h_2, k_2) = (h_1\phi_{k_1}(h_2), k_1k_2) \\ \textit{with} \\ \phi : K \to Aut(H)\end{gathered}$$

As was the case for the two types of direct products, the inner and outer semidirect product yield the same results from different directions. The inner semidirect product constructs a semidirect product from inside some known group $S$ while the outer semidirect product constructs $S$ externally using certain groups $H$ and $K$. It is left to check that the group $H \rtimes_\phi K$ is indeed a group.

**Corollary 3.** *The group $H \rtimes_\phi K$ is indeed a group for some homomorphism $\phi : K \to Aut(H)$.*

*Proof.* Any element in $H \rtimes_\phi K$ takes the form $(h, k)$ for some $h \in H$ and $k \in K$.

<u>Associativity</u>
Take any three elements $(h_1, k_1)$, $(h_2, k_2)$, and $(h_3, k_3)$ in $H \rtimes_\phi K$. We want to show that:

$$((h_1, k_1) * (h_2, k_2)) * (h_3, k_3) = (h_1, k_1) * ((h_2, k_2) * (h_3, k_3))$$

To do so, realize that:

$$\begin{aligned}((h_1, k_1) * (h_2, k_2)) * (h_3, k_3) &= (h_1\phi_{k_1}(h_2), k_1k_2) * (h_3, k_3)\\ &= (h_1\phi_{k_1}(h_2)\phi_{k_1k_2}(h_3), k_1k_2k_3)\\ &= (h_1\phi_{k_1}(h_2)\phi_{k_1}(\phi_{k_2}(h_3)), k_1k_2k_3)\\ &= (h_1\phi_{k_1}(h_2\phi_{k_2}(h_3)), k_1k_2k_3)\\ &\qquad \text{since } \phi_{k_1} \text{ is a homomorphism}\\ &= (h_1, k_1) * (h_2\phi_{k_2}(h_3), k_2k_3)\\ &= (h_1, k_1) * ((h_2, k_2) * (h_3, k_3))\end{aligned}$$

thus proving associativity.

<u>Identity</u>
Consider the element $(e_H, e_K) \in H \rtimes_\phi K$ and any other element $(h, k) \in H \rtimes_\phi K$. We know that:

$$\begin{aligned}(e_H, e_K) * (h, k) &= (e_H\phi_{e_K}(h), e_Kk)\\ &= (e_Hh, k)\\ &\qquad \text{since } \phi_{e_K} \text{ is the trivial automorphism}\\ &= (h, k)\end{aligned}$$

Furthermore, we can verify that:

$$\begin{aligned}(h, k) * (e_H, e_K) &= (h\phi_k(e_H), ke_K)\\ &= (he_H, k)\\ &\qquad \text{since } \phi_k \text{ is an isomorphism meaning } \ker(\phi_k) = \{e_H\}\\ &= (h, k)\end{aligned}$$

thus proving the identity element exists.

<u>Inverses</u>
Consider the element $(h, k) \in H \rtimes_\phi K$. We want to find some $(h', k')$ such that $(h, k) * (h', k') = (e_H, e_K) = (h', k') * (h, k)$. In other words, we want:

$$\begin{aligned}h\phi_k(h') &= e_H\\ kk' &= e_K\\ h'\phi_{k'}(h) &= e_H\\ k'k &= e_K\end{aligned}$$

From the second and fourth equation, we know that $k' = k^{-1}$. And from the first and third we know that $h' = \phi_k^{-1}(h^{-1})$ and $h' = (\phi_{k'}(h))^{-1}$ respectively. Since $k' = k^{-1}$, we know that $h' = \phi_k^{-1}(h^{-1})$ and $h' = (\phi_{k^{-1}}(h))^{-1}$. And since $\phi_k$ is an automorphism, we know that $(\phi_{k^{-1}}(h))^{-1} = \phi_{k^{-1}}(h^{-1}) = \phi_k^{-1}(h^{-1})$. Thus, we have found that $(h', k') = (\phi_{k^{-1}}(h^{-1}), k^{-1})$, proving that inverses exist. ■

Furthermore, the outer semidirect product is a generalization of the external direct product. We can see this rather trivially in the inner semidirect product vs internal direct product case since the internal direct product requires $K \lhd G$ while the inner semidirect product does not.

**Lemma 3.1.** *The external direct product is a trivial case of the outer semidirect product.*

*Proof.* Let $H$ and $K$ be two groups such that $K$ is a group acting on $H$. We can construct the outer semidirect product $H \rtimes_\phi K$ for some homomorphism $\phi : K \to \mathrm{Aut}(H)$. Let $\phi$ send all $k \in K$ to the trivial automorphism $\phi_k(h) = h$ for all $h \in H$ with $\phi_k : H \to H$. We know the trivial $\phi_k$ is an automorphism since it sends all $h \in H$ to $h$ (i.e. $\ker(\phi_k) = e$ and $\mathrm{Im}(\phi_k) = H$ so it is bijective with domain equal to the codomain) and:

$$\begin{aligned}\phi_k(h_1h_2) &= \phi_k(h_1)\phi_k(h_2)\\ h_1h_2 &= h_1h_2\end{aligned}$$

thus demonstrating that $\phi_k$ is an automorphism. In this case, we see that the binary operation (*) associated with $H \rtimes_\phi K$ becomes:

$$\begin{aligned}(h_1, k_1) * (h_2, k_2) &= (h_1\phi(k_1)(h_2), k_1k_2)\\ &= (h_1\phi_{k_1}(h_2), k_1k_2)\\ &= (h_1h_2, k_1k_2)\end{aligned}$$

which is precisely equal to the binary operation on $H \times K$ or in other words the external direct product. This confirms that the external direct product is a trivial case of the outer semidirect product. ■

Since the external direct product is a trivial case of the outer semidirect product, the outer semidirect product should theoretically be able to classify more finite groups. To be clear, this isn't a proof, and it is plausible yet unlikely that every group that can be classified by a semidirect product can also be classified by a direct product. This being said, at the minimum, via **Lemma 3.1** we know that the classification of all finite groups will be more concisely described using semidirect products instead of direct products.

# 4 Semidirect Product Example

**Example 4.1.** Inner Semidirect Product (The Dihedral Group $D_{2N}$ of Order $2N$)

Take the two subgroups, $<r>$ and $<s>$ representing the subgroup generated by some rotation $r$ and the subgroup generated by some reflection $s$ respectively. Since reflections have order 2, we know that $<s> = \{e, s\}$. Similarly, since rotations have order $N$, we know that $<r> = \{e, r, r^2, ..., r^{N-1}\}$. Also note that $|D_{2N}| = 2N$. As stated in **Definition 4**, to construct the inner semidirect product these subgroups must satisfy three conditions.

First, it must be the case that:

$$<r><s> = D_{2N}$$

Thus, consider that $<r><s>= \{e, r, r^2, ..., r^{N-1}, s, rs, r^2s, ..., r^{N-1}s\}$. Since $|<r><s>| = 2N$, if every value in $<r><s>$ is unique then we will have shown that $<r><s>= D_{2N}$.

We already know that all values in $<r>$ are unique, thus, it suffices to show that the values $\{s, rs, r^2s, ..., r^{N-1}s\}$ are unique. Consider some value in this set, $r^is$ for $0 \leq i \leq N - 1$. Assume for the sake of contradiction that $r^is \in <r>$, then $r^is = r^k$ for some $0 \leq k \leq N - 1$. However, this would imply that $s = r^{k-i}$. We then have two cases:
If $k = i$, then $s = e$. This is a contradiction since $r^is$ is assumed to be some value in $\{e, s, rs, r^2s, ..., r^{N-1}s\}$ but $r^is = r^i$ when $s = e$ is not in that set.
If $k \neq i$, then $s = r^{k-i}$, meaning $s$ is some rotation. This is again a contradiction since it is impossible for a reflection to be equal to a rotation, meaning $r^is \notin <r>$.

Furthermore, assume for the sake of contradiction that $r^is \in \{e, s, rs, r^2s, ..., r^{N-1}s\}\backslash r^is$. This means $r^is = r^ks$ for some $0 \leq k \leq N - 1$ where $k \neq i$. However, this implies that $r^i = r^k$, which is impossible since $<r>$ is already composed of unique values, and both $r^i, r^k \in <r>$. Thus, every value in $<r><s>$ is unique, meaning $<r><s> = D_{2N}$ since their order is equal.

Secondly, we must show that:

$$<r> \cap <s> = \{e\}$$

However, this comes rather trivially. We know that a reflection is not equal to some rotation, therefore, $s \notin \langle r \rangle$. Yet, the only other element in $\langle s \rangle$ is $e$, meaning it must be the case that $\langle r \rangle \cap \langle s \rangle = \{e\}$.

Finally, we must show that some subgroup is normal, specifically we will show that:

$$\langle r \rangle \triangleleft D_{2N}$$

To realize this, take any element $r^i$ in $\langle r \rangle$ for $0 \leq i \leq N-1$. We trivially know that conjugation of $r^i$ by any other element in $\langle r \rangle$ will result in another element in $\langle r \rangle$, so it suffices to show that if we conjugate by some element in $D_{2N}$ that is not in $\langle r \rangle$ and still get an element in $\langle r \rangle$, we will have proven that $\langle r \rangle$ is normal in $D_{2N}$. Luckily, since $\langle s \rangle$ is of order 2, and since $\langle r \rangle\langle s \rangle = D_{2N}$, we know that the only element $\in D_{2N}$ but not $\in \langle r \rangle$ is $s$. Thus, consider:

$$sr^is^{-1} = r^{-i}ss^{-1}$$

by properties of the dihedral gorup

$$= r^{-i}$$
$$\in \langle r \rangle$$

thus confirming that $\langle r \rangle \triangleleft D_{2N}$.

Using all three of these properties, we see that $D_{2N} \cong \langle r \rangle \rtimes_\phi \langle s \rangle$ for some $\phi : \langle s \rangle \to \text{Aut}(\langle r \rangle)$. Thus, this semidirect product is unique up to the choice of $\phi$. Since $|\langle s \rangle| = 2$, we can brute force what $\phi$ will do on the elements of $\langle s \rangle$ to finish our example of the inner semidirect product.

Consider some $r^i \in \langle r \rangle$ with $0 \leq i \leq N-1$. Since $\langle s \rangle = \{e, s\}$, we want to define $\phi_e$ and $\phi_s$.

Trivially, we have $\phi_e$ as:

$$\phi_e(r^i) = r^i$$

Furthermore, as seen above, we will define $\phi_s$ as:

$$\begin{aligned}\phi_s(r^i) &= sr^is^{-1} \\ &= r^{-1}ss^{-1} \\ &= r^{-1}\end{aligned}$$

Thus, we have completely defined the inner semidirect product.

## 5 References

https://sites.millersville.edu/bikenaga/abstract-algebra-1/product/product.html

https://math.stackexchange.com/questions/106028/semi-direct-v-s-direct-products

https://www.youtube.com/watch?v=Pat5Qsmrdaw

https://www.youtube.com/watch?v=DvclxOaWbJM https://www.youtube.com/watch?v=McM7v1luwJU

https://proofwiki.org/wiki/Semidirect_Product_of_Groups_is_Group

https://kconrad.math.uconn.edu/blurbs/grouptheory/dihedral.pdf

https://brilliant.org/wiki/semidirect-product/inner-semidirect-product

https://en.wikipedia.org/wiki/Semidirect_product

https://groupprops.subwiki.org/wiki/External_semidirect_product

https://www.ms.uky.edu/ jack/2013-06-20-Semidirect.pdf

http://www.math.columbia.edu/ bayer/S09/ModernAlgebra/semidirect.pdf

https://sites.math.washington.edu/ morrow/336_20/papers19/Bryce.pdf

https://math.stackexchange.com/questions/393051/understanding-the-internal-direct-product-of-a-group

https://mathweb.ucsd.edu/ jmckerna/Teaching/15-16/Spring/103B/l_1.pdf

http://www.math.clemson.edu/ kevja/COURSES/Math851/NOTES/s5.2.pdf

https://math.stackexchange.com/questions/686400/what-is-the-motivation-for-semidirect-products

https://en.wikipedia.org/wiki/Dihedral_group