Semidirect Products

Aaryan Sukhadia

Math 120, Spring 2022
Instructor: Hunter Spink

Contents

1 Introduction 2

2 Definition 2
2.1 Key Terms 2
2.2 Two Semidirect Product Definitions 3

3 Basic Properties 4
3.1 Group Verification 4
3.2 Equivalence of Definitions 5

4 Examples and Applications 7
4.1 Holomorphs 7
4.2 Dihedral Groups 7
4.3 Classification of Groups 8

5 Conclusion and Acknowledgements 8

1 Introduction

The abstract algebraist is primarily concerned about 2 things: finding examples of algebraic structures, and combining them in different ways. It's a little like a Lego set, you have different pieces ($\mathbb{Z}$, A_4, C_7, whatever it may be) that you can interlock together to create interesting emergent structures.

One example of an 'interlocking' method is taking the direct product of two groups. Given two groups A, B we can create a group $A \times B := \{(a, b) : a \in A, b \in B\}$. We can also 'break apart' groups into the direct product of two subgroups. For example, the cyclic group C_{mn} for m, n co-prime is isomorphic to $C_m \times C_n$. More generally, let G be a group with **normal** subgroups H, K such that $H \cap K = \{1\}$ and $HK = G$. Then, it can be shown that $G \cong H \times K$ (i.e it is isomorphic to the direct product of those subgroups).

An issue with the direct product, however, is that, when it comes to decomoposition, it only works to decomopose G into normal subgroups. What makes group theory more interesting than Legos, however, is the fact that there are different ways of interlocking things. In this paper, we'll be exploring one such way: the **semidirect product**. It'll help us not only break apart groups in ways we previously couldn't, but also create new unfamiliar groups for us to explore.

We'll be looking at how to define this concept rigorously in multiple ways, prove some important properties of the semidirect product, and then explore some englightening examples.

2 Definition

2.1 Key Terms

Firstly, we list off some basic prior prerequisite key terms and ideas which won't be proved or explored here, but they will be required in order for us to construct the semi-direct product.

- Given 2 subgroups $H, K \leq G$, the **product of group subsets** $HK := \{hk : h \in H, k \in K\}$. If $H \cap K = 1$, then every element of HK has a unique representation hk, for some $h \in H, k \in k$. If that property holds *and* $HK = G$, then K is called a **complement** for H.

- A **normal** subgroup denoted $N \trianglelefteq G$ is one such that, given any $g \in G$, it holds that $gNg^{-1} = N$. In other words, it is invariant under (left) **conjugation** by any element in the group.

- We define $Aut(G)$ as the set of all **automorphisms** of G onto itself, which, with the operation of composition, form a group.

- A **homomorphism** between 2 groups is a map $\phi : G \to H$ with the property that $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$. An important property of homomorphisms is that the identity of G necessarily maps to the identity of H,

- If $N \trianglelefteq G$, then given any $H \leq G$, there is a **group action** $H \curvearrowright N$ by conjugation that behaves like automorphisms of N. Specifically, we have $h \cdot n = hnh^{-1}$, and for each $h \in H$ there is a corresponding automorphism of N.

We now have the necessary background to discuss the 2 different classes of semi-direct products

2.2 Two Semidirect Product Definitions

We will now give *two* technically different but conceptually equivalent definitions of the semi-direct product: one for building up groups and one for breaking down groups

Definition (1)**.** Given two groups H and K, and a homomorphism $\phi : K \to Aut(H)$, the **outer semidirect product** of H and K with respect to ϕ is:

$$H \rtimes_\phi K = \{(h,k) : h \in H, k \in K\}$$

with group operation:

$$(h_1,k_1)(h_2,k_2) := (h_1\phi(k_1)(h_2), k_1k_2)$$

We now unpack what it means and show why it is a group. In simple terms, the underlying set of the group is the Cartesian product $H \times K$ (note the times symbol here is *not* a direct product).

For the operation, the second element of the output is noticeably well-defined; we multiply k_1 and k_2 with the group operation on K. The first element of the output is more complex. Recall that ϕ is a map from all $k \in K$ to some automorphism $\Upsilon : H \to H$. Thus, $\phi(k)(h_2) = \Upsilon(h_2) \in H$. Then, we multiply that by h_1 with a group operation in H. Thus, this operation obeys closure and is well defined.

Thus, the outer semidirect product allows us to take two groups and construct a new group. The proof that this structure obeys the group axioms is in Section 2.3.

Definition (2)**.** Given a group G, let H be a normal subgroup and let K a complement for H. Let $K \curvearrowright H$ be the conjugation action of K on H. Then, G is the **inner semidirect product** of K acting on H:

$$G \cong H \rtimes K = \{hk : h \in H, k \in K\}$$

with group operation:

$$(h_1k_1)(h_2k_2) = (h_1k_1 \cdot h_2)(k_1k_2)$$

Clearly, all multiplication here is well-defined, since we are operating within a group. The action of k on h is simply given by $k \cdot h = khk^{-1} \in H$, since H is a normal subgroup. This will come up in more detail later.

This definition allows us to 'break down' a group and express it as the semidirect product of 2 subgroups, up to isomorphism. Specifically, if K is a complement of H, then $H \rtimes K \cong G$.

3 Basic Properties

3.1 Group Verification

We verify that the construction of the outer semidirect product is indeed a group. We now use the following fact:

Fact. *The homomorphism $\phi : K \to Aut(H)$ is associated with a left action of K on H given by $k \cdot h = \phi(k)(h)$*

The verification that this follows the axioms of the group action is trivial, but we can use this fact to show that $H \rtimes_\phi K$ is a group.

Theorem 3.1.1. *Given two groups H, K, their outer semidirect product (wrt ϕ) $H \rtimes_\phi K$ is a group (i.e obeys associativity, identity and inverses).*

Proof. Take $a, b, c \in H$ and $x, y, z \in K$. Temporarily writing with a group operation symbol $\circ$ for clarity's sake, we now work out $((a, x) \circ (b, y)) \circ (c, z)$:

$$\begin{aligned}
((a, x) \circ (b, y)) \circ (c, z) &= (ax \cdot b, xy) \circ (c, z) \\
&= (ax \cdot b(xy) \cdot c, xyz) \\
\text{Using properties of group actions,} \quad &= (ax \cdot bx \cdot (y \cdot c), xyz) \\
&= (ax \cdot (b(y \cdot c)), xyz) \\
&= (a, x) \circ (by \cdot c, yz) \\
&= (a, x) \circ ((b, y) \circ (c, z)),
\end{aligned}$$

which shows associativity.

Claim. *We claim that $(1_H, 1_K)$ is the identity of $H \rtimes_\phi K$., where 1_H and 1_K represent the identities of H and K respectively.*

Take any $(h, k) \in H \rtimes_\phi K$. We have:

$$(1_H, 1_K)(h, k) = (1_H, 1_K \cdot h, 1_K k)$$

Using the fact that identities map to identities under homomorphisms, we infer that $\phi(1_K)$ is the identity automorphism of H. Thus, $1_K \cdot h = h \forall h \in H$. This gives us $(1_H, 1_K)(h, k) = (1_H h, 1_K k = (h, k)$. The right multiplication case is also simple, since it doesn't matter what automorphism k maps to, it can only act on 1_H by taking it to 1_H. Thus, $(h, k)(1_H, 1_K) = (h, k)$ as well, and the identity is proven.

Claim. *The inverse $(h, k)^{-1} = (k^{-1} \cdot h^{-1}, k^{-1})$*

This is checked by straightforward calculation:

$$\begin{aligned}(h,k)(k^{-1}\cdot h,k^{-1}) &= (hk\cdot(k^{-1}\cdot h^{-1}),kk^{-1})\\ &= (h(kk^{-1})\cdot h^{-1},1_K)\\ &= (h1_K\cdot h^{-1},1_K) = (hh^{-1},1_K)\\ &= (1_H,1_K)\end{aligned}$$

which we showed was the identity of $H \rtimes_\phi K$. The left multiplication by inverse is left as a trivial verification

□

3.2 Equivalence of Definitions

We want to show that the inner and outer semidirect products are essentially giving us the same thing. The only salient difference between them is in one we are starting with arbitrary groups and constructing new ones, whereas in the other we are starting with a global group and taking the product of subgroups of it.

Suppose we start off with a group G with normal subgroup H for which K is a complement. By definition (2), G is the inner semidirect product of K acting on H. Supposing ϕ maps each k to the the automorphism of H given by conjugation, we now show that $H \rtimes_\phi K \cong G$:

Theorem 3.2.1. *If G can be broken down into $H \rtimes K$, as in definition (2), then $H \rtimes_\phi K \cong G$*

Proof. We define a map $\psi : G \to H \rtimes_\phi K$ given by $\psi(g) = \psi(hk) = (h,k)$. We will show that ψ is an isomorphism. This is well-defined by the fact that $G = HK$ and $H \cap K = 1$, and so every $g \in G$ can be written as a unique product of $h \in H, k \in K$ giving us a unique $(h,k) \in H \rtimes_\phi K$. The same reasoning tells us the inverse ψ^{-1} is also well defined.

Inside G, we have:

$$(h_1k_1)(h_2k_2) = (h_1k_1\cdot h_2)(k_1k_2) = h_1k_1h_2k_1^{-1}k_1k_2 = h_1k_1h_2k_2$$

Thus, given $a = h_1k_1, b = h_2k_2$ we get:

$$\begin{aligned}\psi(ab) &= \psi(h_1k_1h_2k_2) = \psi((h_1k_1\cdot h_2)(k_1k_2))\\ &= (h_1k_1\cdot h_2, k_1k_2) = (h_1,k_1)(h_2,k_2)\\ &= \psi(h_1k_1)\psi(h_2k_2) = \psi(a)\psi(b)\end{aligned}$$

Thus, ψ is a bijective homomorphism, and therefore an isomorphism.

□

Now we take arbitrary groups H, K with some $\phi : K \to Aut(H)$, and construct $H \rtimes_\phi$ as by Definition (1). We now see how to express this group as a semidirect product of some of its subgroups, as in Definition (2).

Theorem 3.2.2. *Let $G := H \rtimes_\phi K$, as by definition (1). Moreover, define $H' := \{(h, 1_k) : h \in H\}$ and $K' := \{(1_H, k) : k \in K\}$. Then, the following hold:*

a) $H \cong H', K \cong K'$

b) $H' \trianglelefteq G$

c) $H' \cap K' = 1$

d) For any $(h, 1_K) \in H'$ and $(1_H, k) \in K'$, $(1_H, k)(h, 1_K)(1_H, k)^{-1} = (\phi(k)(h), 1_K)$

And as a consequence of $a), b), c), d)$, $G = H' \rtimes K'$ as in definition (2).

Proof. We go part by part.

For a), we note that $(h_1, 1_K)(h_2, 1_K) = (h_1\phi(1_K)(h_2), 1_K) = (h_1h_2, 1_K)$. Thus, we define a surjective homomorphism (and thus an isomorphism $\varphi(h) = (h, 1_K)$. The exact same logic is used to show $K \cong K'$.

For b), a simple calculatory verification for any $(h, k) \in G$ suffices:

$$\begin{aligned}(h, k)(h_0, 1_K)(h, k)^{-1} &= (h, k)(h_0, 1_K)(\phi(k)^{-1}(h^{-1}), k^{-1})\\ &= (h, k)(h_0\phi(k)^{-1}(h^{-1}), k^{-1})\\ &= (h', kk^{-1}) = (h', 1_K) \in H'\end{aligned}$$

We didn't actually need to compute what exactly h' evaluated to, since to check for normality we just need to check that the resultant product after conjugation is in H', which indeed it is.

Part c) is almost too trivial to go over, but basically the only overlap between H' and K' are when both elements of the pair are the respective identities of the groups.

Part d) is done with another simple calculation:

$$\begin{aligned}(1_H, k)(h, 1_K)(1_H, k)^{-1} &= (1_H, k)(h\phi(1_k)^{-1}(1_H), 1_K k^{-1})\\ &= (1_H, k)(h, k) = (1_H\phi(k)(h), kk^{-1})\\ &= (\phi(k)(h), 1_K),\end{aligned}$$

as desired.

□

Note that this equivalence does not imply that the semidirect product is *unique* however, since it depends on our choice of homomorphism. More formally, consider the outer semidirect product $G := H \rtimes_\phi K$ for two groups H, K. Now suppose there exists a group G' with a normal subgroup H' which has complement K', and suppose that $H \cong H', K \cong K'$. Then we know G' is the inner semidirect product of $H' \rtimes K'$, but, depending on ϕ, it does *not* follow that $G' \cong G$.

4 Examples and Applications

In this section we discuss various places in group theory where semidirect products pop-up. We will not explore any one result or application in rigour, but instead will get a taste of several different ideas.

4.1 Holomorphs

In the definition of the outer-semidirect product, consider the case if $K = Aut(H)$. Then, we would have $H \rtimes_\phi Aut(H)$, and we can take $\phi : Aut(H) \to Aut(H)$ to simply be the identity map. This is a special type of group constructed from H, and it is known as the **holomorph** of H, denoted $\text{Hol}(H)$.

Perhaps the most interesting application of holomorphs comes from their connections to permutation groups. In particular, for any group G, we consider its action on itself by left multiplication, which gives rise to a permutation of G. We can construct a homomorphism $\lambda : G \to S_G$ from G to the symmetric group on G, defined by $\lambda(g) = gG$, i.e the permutation given by left multiplication by the element g. Clearly, $\lambda(G) \leq S_G$.

Claim. *The normalizer of $\lambda(G)$ is isomorphic to Hol(G)*

Sketch Proof. If we take any $n \in N(\lambda(G))$ such that $n(1) = 1$, then it does not take too much work to show that n is an automorphism of G. Let $A \leq S_G$ to be the stabilizer of the identity of G within $N(\lambda(G))$, and it is clear that $A \leq Aut(G)$. The key step now is to show $N(\lambda(G))$ is the inner semi-direct product $\lambda(G) \rtimes A$, which requires showing that every element of N can be expressed as a product of $a \in A$ and $b \in \lambda(G)$.

Here we are almost done. Clearly, $\lambda G \cong G$, and if $a \in S_G$ is an automorphism it clearly stabilizes 1, so $A \cong Aut(G)$. As a result, $N = \lambda(G) \rtimes A \cong G \rtimes Aut(G) = \text{Hol}(G)$, which is what we wanted to show. □

4.2 Dihedral Groups

Take $D_{2n} = \langle \sigma, \tau : \sigma^n = 1, \tau^2 = 1, \sigma\tau = \tau\sigma^{-1} \rangle$
Note that the group $<\sigma>\cong C_n$ and $<\tau>\cong C_2$. Moreover, $<\sigma><\tau>= D_{2n}$, and $<\sigma>\trianglelefteq D_{2n}$, since it has index 2. Moreover, $<\sigma> \cap <\tau>= 1$. These properties imply that we can express D_{2n} as the semidirect product of $C_n \rtimes C_2$. The action here is $C_2 \curvearrowright C_n$ acting by conjugation, which gives us $1 \cdot h = h, \tau \cdot h = h^{-1}$.

Building the group the other way, we define $\phi : C_2 \to Aut(C_n)$ by $\phi(1) = id$ the identity map, and $\phi(c) = inv$ the inverse map, where c is the non-identity element of C_2. Then, we get $C_n \rtimes_\phi C_2 \cong D_{2n}$.

Remark. An interesting thing occurs if we take an *infinite* cyclic group, say $\mathbb{Z}$. Then, we get $D_\infty := \mathbb{Z} \rtimes_\phi C_2$, a kind of infinite dihedral group. Moreover, since $Aut(\mathbb{Z}) \cong C_2$, we can also say $D_\infty \cong \text{Hol}(\mathbb{Z})$.

4.3 Classification of Groups

Semidirect product can be used in conjunction with Sylow theorems to classify all the possible groups of a certain order. Let us look at an example of how we might go about classifying all groups G of order 20.

Since $20 = 2^2 \times 5$, Sylow tells us that there exist a Sylow 5-subgroup H and a Sylow 2-subgroup K. More specifically, we know that there can only exist 1 Sylow 5-subgroup, and hence $C_5 \cong H \trianglelefteq G$. By Lagrange's Theorem, we also know that $H \cap K = 1$, which also tells us that $G = HK$. Compiling all this information together, using the equivalency theorem of semi-direct products, we note that $G \cong H \rtimes_\phi K$, for some homomorphism $\phi : K \to Aut(H)$.

The problem of classifying all the groups of order 20 thus reduces to finding all homomorphisms from a group of order 4 (i.e either C_4 or the Klein 4-group) to $Aut(C_5) \cong C_4$. The only caveat is that if two homomorphisms have the same image, then the semidirect product induced by them will be isomorphic, but with a little bit of checking the number of groups of order 20 up to isomorphism can be fully classified.

5 Conclusion and Acknowledgements

We have explored the semidirect product, the different ways it can be formulated, shown some key properties of groups constructed with the semi-direct product, and given some examples with familiar groups. The applications extend far, far beyond what we have covered (or what is even possible to cover) in this text: we can there's only 1 non-abelian group of order pq for primes p, q; they show up in linear transformations such as the orthogonal group, the fundamental group of wacky objects like the Klein bottle can be represented as semidirect products. They are not only a useful tool to construct new groups, but also to look at groups we already know in a different light.

The concepts, background and ideas in this text were taken primarily from the 3rd edition of Dummit and Foote's *Abstract Algebra*, along with class material taught by Hunter Spink.