Direct and Inner Semidirect Products

P. Reany

October 8, 2023

Abstract

In this paper I try to present the notions of direct and inner semidirect products of groups as clearly as is possible. There is a concept of the outer semidirect products of groups, which I won't deal with in this paper.

1 The direct product of two groups

I assume that the reader is already famliar with very basic group theory, up to group homomorphisms and normal subgroups.

Definition: Let S be a set. Then, we denote the number of elements of S (also referred to as the *order* of S) as $|\,S\,|$. Similarly, Let G be a group. Then, we denote the order of G as $|\,G\,|$.

Perhaps every paper on group theory should motivate the subject by stating that: The purpose of group theory is to investigate the structure of every possible group. There are basically three ways to do this. The first is to find ways to combine two already existing groups, and the second is to find all the subgroups of a given group. The third is to figure out how to 'factor' a group into the nontrivial product of smaller groups. By the way, one of the primary characteristcs of any group is its order.[1] Another primary characteristic of groups iis whther it is *simple* or not.[2]

Let H and K be any two groups. Since groups are also sets, let's begin by looking at the direct product of these sets. Let h be any element of set H, let k be any element of set K. Then we can form an element (h,k) of a new set S of ordered pairs, where[3]

$$S \equiv H \times K = \{(h,k)\,|\,h \in H, k \in K\}\,. \tag{1}$$

So, if H and K are finite groups, then they're also finite sets. Then the order of $H \times K$ has to be $|\,H\,||\,K\,|$, that is, the product of the orders of each set (group). Therefore, if some group G can be 'factored' into a direct product of two finite groups, then we know the order of G is given by

$$|\,G\,| = |\,H\,||\,K\,|\,. \tag{2}$$

Thus, if we can factor a finite group into a direct product of two or more finite groups whose orders we know, then we can calculate the order of the original group.[4]

[1] Another way to help us characerize one group is by homomorphism from it to other groups, or by homorphisms to it from other groups.

[2] A group is said to be simple if it has no nontrivial normal subgroups.

[3] The direct product of sets is called the *cartesian product* of sets. We can think of the direct product as the generalization of the cartesian product on mere sets.

[4] Though I will only discuss the direct product of two groups here, one can form the direct product of any finite number of groups.

The question arises if we can add some properties to set S to turn it into a group. The direct product of two groups is easily seen to be itself a group, using the group properties of H and K.

Let's begin with looking at direct product of these sets. Let h_1 and h_2 be any two elements of set H. Similarly, k_1 and k_2 be any two elements of set K. The first thing we need to add to S is a closed binary operation. We'll take the obvious: For (h_1, k_1) and (h_2, k_2), we define their product as[5]

$$(h_1, k_1)(h_2, k_2) \equiv (h_1 h_2, k_1 k_2)\,. \tag{3}$$

So, since $h_1 h_2 \in H$ and $k_1 k_2 \in K$, then $(h_1 h_2, k_1 k_2) \in H \times K = S$. Thus, the definition provided in (3) provides for us a closed binary operation in S.

What else do we need to make S a group? For one, we'll need a two-sided identity element. The logical candidate for that is (e_H, e_K), where e_H is the identity element in H and e_K is the identity element in K. Thus, for any $h \in H$ and any $k \in K$

$$(e_H, e_K)(h, k) = (e_H h, e_K k) = (h, k)\,, \tag{4}$$

and

$$(h, k)(e_H, e_K) = (h e_H, k e_K) = (h, k)\,. \tag{5}$$

Therefore, the element (e_H, e_K) is the identity element for the set S.

We'll also need inverses for each element (h, k). Again, the logical choice for an inverse is given by

$$(h, k)^{-1} = (h^{-1}, k^{-1})\,. \tag{6}$$

Let's try it.

$$(h, k)(h^{-1}, k^{-1}) = (h h^{-1}, k k^{-1}) = (e_H, e_K)\,, \tag{7}$$

and

$$(h^{-1}, k^{-1})(h, k) = (h^{-1} h, k^{-1} k) = (e_H, e_K)\,. \tag{8}$$

So, we see that, up to this point, all the group actions are performed componentwise. That's what makes working with the direct product so simple. I leave as an exercise for the reader to prove that the product of three elements of S is associative, which completes the proof that S has been extended to a group in its own right.

So, if the direct product is so trivial, what good is it? Well, for one thing, if H and K are finite groups, then the order of $H \times K$ has to be $|\,H\,||\,K\,|$, that is, the product of the orders of each group. Therefore, if some group G can be 'factored' into a direct product of two finite group then we know the order of G.

$$|\,G\,| = |\,H\,||\,K\,|\,. \tag{9}$$

2 The (Inner) Semidirect Product

In the direct product case, all internal multiplications[6] are performed between any two elements of S strictly componentwise. That is to say that there is no crossover of one component affecting the results of any other component. But this is not so with the (inner) semidirect product. In this product, one component is strictly isolated from the other, but the other is influenced by the other.

So, the idea of an inner semidirect product is to factor a given group G by two iof its subgroups, which we'll see how this works following. The idea of an outer semidirect product is about taking two arbitrary groups together and forming a semidirect product in much the same way as is done with the

[5] We are in the process of constructing a group out of the set S. When we have completed that task the rule in Eq. (3) will be its group product rule.

[6] When I say 'multiplications' I mean any given group operation.

inner semidirect product. But, whereas the inner semidirect product is easy to understand because the elements of the two subgroups that one uses to form it naturally interact with each other as they both reside wihiin the same group G; it takes some care to find an appropriate interaction between two arbiitrary groups. Maybe it can't always be done. Anyway, the outer semidirect product will be left for another time.

Let G be a group and let H, K be subgroups of G such that the following properties hold:

Prop. 1) $G = HK$

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

Prop. 3) H is normal in G.

(We have a lot of basic foundation to lay before we use this condition.)[7]

What 1) implies is that every element g of G can be written as

$$g = hk\,, \tag{10}$$

for some $h \in H$ and for some $k \in K$.

So, we see that this group G is of a special form. Its particular special form allows us to construct a semidirect product on it (which we will soon prove) for the purpose of analyzing G by analyzing the semidirect product isomorphic to it. We base this on the general principle that any two groups that are isomorphic have to share all the same structures and properties.

Now, let's go back to [8]

$$S \equiv H \times K = \{(h,k)\,|\,h \in H, k \in K\}\,. \tag{11}$$

What if there were a function ϕ going from the set S and the group G? If we could establish that ϕ is a homomorphism (or better yet, an isomorphism), then we could infer properties of G by properties of S.

Let h_1 and h_2 be any two elements of set H. Let k_1 and k_2 be any two elements of set K. Then, for ϕ to be a homomorphism, we need to show that

$$\phi((h_1,k_1)(h_2,k_2)) = \phi((h_1,k_1))\phi((h_2,k_2))\,. \tag{12}$$

Before we can finish (12), we need to establish that ϕ is both one-to-one (injective) and onto. We'll start off by suggesting the obvious assignment of (h,k) under ϕ.

$$\phi((h,k)) = hk\,. \tag{13}$$

The standard way to show that a mapping is one-to-one is to show that whenever two elements of S get mapped to the same element of G, that those elements of S must be the same. Therefore, say,

$$\phi((h_1,k_1)) = \phi((h_2,k_2))\,, \tag{14}$$

then

$$h_1k_1 = h_2k_2\,. \tag{15}$$

But we're allowed to employ group operations on this equation, such as by multiplying through on the right by k_2^{-1} and on the left through by h_1^{-1}, to get

$$k_1k_2^{-1} = h_1^{-1}h_2\,. \tag{16}$$

[7] It's important to note that in the above cases, H and K were any two random groups, but now they are related by both being subgroups of G.

[8] We have to start all over with the set S because we do not as yet know how to define the group product rule in this particullar set off group specifications.

Now, the LHS of this equation tells us that we have an element of K, and the RHS of the equation tells us that we have an element of H. But because of Prop. 2) above, the only element that is both Kish and Hish at the same time is the group identity e of G. Therefore,

$$k_1 k_2^{-1} = e \quad \text{and} \quad h_1^{-1} h_2 = e\,. \tag{17}$$

From this we get that

$$k_1 = k_2 \quad \text{and} \quad h_1 = h_2\,, \tag{18}$$

which proves that $(h_1, k_1) = (h_2, k_2)$, which is what we needed to show to prove that ϕ is one-to-one.

To show that ϕ is a bijection from S to G, have only to show that ϕ is also onto (surjective). But this is trivial because we already said that every element of G can be represent by some element hk, and there must be an element $(h, k) \in S$, so that

$$(h, k) = \phi^{-1}(hk)\,. \tag{19}$$

Thus we have shown that ϕ is a bijection of S to G. And this brings us back to the question: Is ϕ an isomorphism from (almost) group S to group G? And that brings us back to Eq. (12). If we use (13) in (12), we get

$$\phi((h_1, k_1)(h_2, k_2)) = h_1 k_1\, h_2 k_2\,. \tag{20}$$

Let's try a simpler case to begin with. Let's assume that G is an abelian group, then

$$\phi((h_1, k_1)(h_2, k_2)) = h_1 h_2\, k_1 k_2 = h' k'\,, \tag{21}$$

where $h' = h_1 h_2$ and $k' = k_1 k_2$. Putting this into (19), we get

$$\phi^{-1}(h'k') = (h', k') = (h_1 h_2, k_1 k_2)\,. \tag{22}$$

And this forces us to adopt the group product rule:

$$(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2)\,. \tag{23}$$

It turns out that we don't have to demand that G be abelian to use the direct product trick. All we really need is that every element of H commute with every element of K.

But what if we can't claim that $h_1 k_1\, h_2 k_2 = h_1 h_2 k_1 k_2$ for all h_1, k_1, h_2, k_2? Then we're going to have to be a bit more clever. And this is where the normality of H comes in.[9]

I know I said that I expect that the reader has already encountered the concept of the normal subgroup, but I prefer to state clearly how we are about to use it in the design of the inner semidirect product.

A subgroup H of G is denoted as normal in G by the symbol $H \lhd G$ if it has the property that for all $h \in H$ and for all $g \in G$,

$$ghg^{-1} = h' \in H\,. \tag{24}$$

Now, we go back to Eq. (20):

$$\phi((h_1, k_1)(h_2, k_2)) = h_1 k_1\, h_2 k_2\,. \tag{25}$$

[9] It's arbitrary which of H and K we choose to be the normal subgroup of G. If we choose K instead, the proof will follow similarly to this one.

Can we by some clever means make the RHS equal to h_0k_0 for some $h_0 \in H$ and some $k_0 \in K$? The answer is Yes. From this point, it's really just a minor puzzle to solve. How do we manipulate $h_1k_1\, h_2k_2$ to get h_0k_0, using the normality property of H? Watch:

$$h_1k_1\, h_2k_2 = h_1k_1\, h_2(k_1^{-1}k_1)k_2\,, \tag{26}$$

where the identity element $k_1^{-1}k_1$ was inserted by a virtual emplacement. Next, we just re-associate:

$$h_1k_1\, h_2k_2 = h_1(k_1h_2k_1^{-1})(k_1k_2) = h_0k_0\,, \tag{27}$$

where $h_1(k_1h_2k_1^{-1}) = h_0$ and $k_1k_2 = k_0$.

So, why again is $h_1(k_1h_2k_1^{-1}) \in H$? Because $k_1h_2k_1^{-1} \in H$, because $H \lhd G$, and it doesn't matter what k_1 is so long as it's an element of G, which it is.

Anyway, we are almost there. All we have left to do is to use the information we have accumulated to this point to tell us how to define the product of two elements of S (to form its group product rule) given that

$$\phi((h_1,k_1)(h_2,k_2)) = \phi((x,y)) = xy = h_1(k_1h_2k_1^{-1})k_1k_2\,. \tag{28}$$

The obvious way to parse this is to set $x = h_1(k_1h_2k_1^{-1})$ and $y = k_1k_2$, giving us the product rule in S as:

$$(h_1,k_1)(h_2,k_2) = (h_1k_1h_2k_1^{-1}, k_1k_2)\,. \tag{29}$$

And that's our semidirect product rule!

But wait! We still have to use this product definition on S with (29) satisfies: 1) the elements of S have a two-sided identity element, 2) that S has a two-sided inverse for each element, and 3) that the product is associative.

The reasonable attempt to settle on an identity element for S is to use $(e_H, e_K) = (e,e)$.

$$(e,e)(h_2,k_2) = (eeh_2e^{-1}, ek_2) = (h_2,k_2)\,. \tag{30}$$

And

$$(h_1,k_1)(e,e) = (h_1k_1ek_1^{-1}, k_1e) = (h_1,k_1)\,. \tag{31}$$

Next, the two-sided inverse for each element. To accomplish this, we just need to do some algebra. So, let $x \in H$ and $y \in K$, such that

$$(x,y)(h_2,k_2) = (xyh_2y^{-1}, yk_2) = (e,e)\,. \tag{32}$$

Solving for y first, we get

$$y = k_2^{-1}\,. \tag{33}$$

Solving for x, we get

$$xk_2^{-1}h_2k_2 = e\,, \tag{34}$$

which gives us

$$x = k_2^{-1}h_2^{-1}k_2\,, \tag{35}$$

I leave it as an exercise to show that

$$(h_1,k_1)(k_1^{-1}h_1^{-1}k_1, k_1^{-1}) = (e,e)\,. \tag{36}$$

I also leave to the reader the proof that this product rule is also associative. That is, show that

$$[\,(h_1,k_1)(h_2,k_2)\,](h_3,k_3) = (h_1,k_1)[\,(h_2,k_2))(h_3,k_3)\,]\,. \tag{37}$$

Now that we've formulated our inner semidirect product on S (that is, our second product version of S), we need a different symbol to represent it. Hence,

$$S = H \rtimes K \,. \tag{38}$$

3 Conclusion

There's a lot more to say about this subject. Perhaps I can return to it soon.