

# The Semidirect Product

Julien De Mori

May 30, 2014

## 1 Introduction

### 1.1 Overview

We have seen that if  $G$  is a group with normal subgroups  $H$  and  $K$  that only share the identity operator in common, then  $HK \cong H \times K$ , where  $H \times K$  is the direct product. In this paper we will generalize the notion of the direct product to allow for one of these groups to not be a normal subgroup of a group  $G$ , and will denote it the *semidirect product*. In general, the direct product of two abelian groups  $H$  and  $K$  is abelian, but the semidirect product need not be. In the next section I will precisely define how one takes the semidirect product of two groups  $K$  and  $H$  with a homomorphism  $\phi$  from  $K$  into  $\text{Aut}(H)$ . I will subsequently also give a criterion for determining whether a group is the semi-direct product of two subgroups, enabling us to classify further groups that the direct product doesn't allow us to classify.

### 1.2 Motivation

We would first like to motivate the desire to define and recognize semidirect products.

One of the primary reasons to construct the semidirect product is that there exist groups that cannot be generated by the direct product of two of its subgroups. Consider the dihedral group  $D_6 = \{1, r, r^2, s, sr, sr^2\}$  of order 6. Consider its only normal subgroup of order 3,  $H = \{1, r, r^2\}$ , and its subgroup (not normal) of order 2, denoted  $K = \{1, s\}$ . Note that  $H \cong \mathbb{Z}/3\mathbb{Z}$ , and  $K \cong \mathbb{Z}/2\mathbb{Z}$  since both are prime order groups, so that  $H \times K \cong \mathbb{Z}/6\mathbb{Z}$ , which would be abelian, since the direct product of abelian groups must be abelian. But  $D_6$  is not abelian, and since there is no normal subgroup of order 2 in  $D_6$ , there is no way to generate  $D_6$  by taking the direct product of two groups. This motivates us to define another product between groups that can generate groups such as  $D_6$ .

As in the example above, let us consider a group  $G$  that contains subgroups  $H$  and  $K$  such that

- (a)  $H \trianglelefteq G$
- (b)  $H \cap K = 1$ .

$HK$  is a subgroup of  $G$  since  $H$  is a normal subgroup and  $K$  is a subgroup of  $G$ . Since  $H \cap K = 1$ , every element of  $HK$  can be written uniquely as the product  $hk$  for  $h \in H$  and  $k \in K$ . Consider  $h_1k_1$  and  $h_2k_2$  in  $HK$ . Then we can write

$$(h_1k_1)(h_2k_2) = h_1k_1h_2(k_1k_1^{-1})k_2 \quad (1)$$

$$= h_1(k_1h_2k_1^{-1})k_1k_2 \quad (2)$$

$$= h_3k_3 \quad (3)$$

where we have let  $h_3 = h_1(k_1h_2k_1^{-1})$  and  $k_3 = k_1k_2$ . It follows that  $h_3 \in H$  because  $H \trianglelefteq G$ , so that conjugating  $h_2$  by some element in  $K \leq G$  keeps the element in  $H$ . Also, clearly  $k_3 \in K$  since it is closed under multiplication.

We would now like to do the reverse. That is, given two groups  $K$  and  $H$ , we would like to define a product between them such that the resulting group  $G$  contains them and (a) and (b) hold. Notice that in the multiplication above,  $k_3 = k_1k_2$  is simply the product of two elements in  $K$ , whereas  $h_3$  is obtained by conjugating  $h_2 \in H$  by  $k_1 \in K$ . We note that the action of  $K$  on  $H$  by conjugation is a homomorphism  $\phi$  of  $K$  into  $\text{Aut}(H)$ , where an automorphism  $\sigma \in \text{Aut}(H)$  is an isomorphism from  $H$  into itself. Letting  $\phi(k)(h) = k \cdot h$  denote the left action of  $K$  on  $H$  determined by the homomorphism  $\phi$ , we can define the product

$$(h_1k_1)(h_2k_2) = (h_1(k_1 \cdot h_2))(k_1k_2) \quad (4)$$

so that multiplication in the group  $HK$  depends only on the multiplication in  $K$ , that in  $H$  and the homomorphism  $\phi$ . We now make precise how we generate a larger group  $G$  via the *semidirect* product of two groups  $H$  and  $K$  with a homomorphism from  $K$  into  $\text{Aut}(H)$ .

## 2 Theorem + Definition: *The Semidirect Product*

**Theorem 2.1.** *Let  $H$  and  $K$  be groups and let  $\phi$  be a homomorphism from  $K$  into  $\text{Aut}(H)$ . Denote  $\phi(k)(g)$  by  $k \cdot g$ , i.e. the (left) action of  $K$  on  $H$  determined by  $\phi$ . Let  $G$  be the set of ordered pairs  $(h, k)$  with  $h \in H$ , and  $k \in K$  and define the following multiplication on  $G$ :*

$$(h_1, k_1)(h_2, k_2) = (h_1(k_1 \cdot h_2), k_1k_2). \quad (5)$$

1. *This multiplication gives  $G$  the structure of a group of order  $|G| = |H||K|$ .*
2. *The sets  $\{(h, 1) | h \in H\}$  and  $\{(1, k) | k \in K\}$  are subgroups of  $G$  such that  $H \cong \{(h, 1) | h \in H\}$  and  $K \cong \{(1, k) | k \in K\}$ .*
3.  *$H \trianglelefteq G$*
4.  *$H \cap K = 1$*

5. for all  $h \in H$  and  $k \in K$ ,  $\phi(k)(h)$  is defined as  $k \cdot h = khk^{-1}$ .

Note that in the (3) - (5) above,  $H$  and  $K$  are the isomorphic copies described in (2). The group  $G$  is denoted the **semidirect product** of  $H$  and  $K$  with respect to  $\phi$  and is denoted  $G = H \rtimes_{\phi} K$ .

*Proof.* (1) We first prove that  $G$  indeed satisfies all the group axioms.

To verify associativity, consider the following multiplication in  $G$ :

$$((a, b), (c, d))(e, f) = (a(b \cdot c), bd)(e, f) \quad (6)$$

$$= (a(b \cdot c))((bd) \cdot e), bdf) \quad (7)$$

$$= (a(b \cdot c)(b \cdot (d \cdot e)), bdf) \quad (8)$$

$$= (a(b \cdot (c(d \cdot e))), bdf) \quad (9)$$

$$= (a, b)(c(d \cdot e), df) \quad (10)$$

$$= (a, b)((c, d)(e, f)) \quad (11)$$

for any  $(a, b), (c, d), (e, f) \in G$ , where we have used the fact that  $\cdot$  is a group action of  $K$  on  $H$ , such that  $k \cdot (h_1 h_2) = k \cdot h_1 k \cdot h_2$ , for  $k \in K$  and  $h_1, h_2 \in H$ .

We now prove the existence of the identity and inverses. Consider the element  $(1, 1) \in G$  and another arbitrary element  $(a, b) \in G$ . Then the multiplication of these elements in  $G$  is

$$(1, 1)(a, b) = (1a \cdot 1, 1b) = (1a, 1b) = (a, b) \quad (12)$$

verifying that  $e_G = (1, 1)$  is the identity of the group  $G$ . Now consider an arbitrary element  $x = (a, b) \in G$ . Consider the element  $x' = (b^{-1} \cdot a^{-1}, b^{-1})$ . We see that

$$(a, b)(b^{-1} \cdot a^{-1}, b^{-1}) = (ab \cdot b^{-1} \cdot a^{-1}, bb^{-1}) \quad (13)$$

$$= (abb^{-1} \cdot a^{-1}, 1) \quad (14)$$

$$= (a1 \cdot a^{-1}, 1) \quad (15)$$

$$= (1, 1) = 1_G \quad (16)$$

demonstrating that every element  $(a, b) \in G$  has a right inverse in  $G$ . One similarly demonstrates that the same element  $x'$  is the left inverse of  $x$ . So we have shown that  $G$  satisfies all the group axioms. The order of the group  $G$  must be the product of the orders of  $H$  and  $K$  since it is the set of ordered pairs of the form  $(h, k)$  for  $h \in H$  and  $k \in K$ . Therefore, there are  $|H|$  choices for the element  $h$  and  $|K|$  choices for the element  $k$ , so there are a total of  $|H||K| = |G|$  ordered pairs, proving assertion (1).

(2) Now to prove the second assertion, we let  $\tilde{H} = \{(h, 1) | h \in H\}$  and  $\tilde{K} = \{(k, 1) | k \in K\}$ . Note that, for any  $a, b \in H$  and  $c, d \in K$

$$(a, 1)(b, 1) = (a1 \cdot b, 1) = (ab, 1) \quad (17)$$

and

$$(1, c)(1, d) = (1, cd) \quad (18)$$

so both  $\tilde{H}$  and  $\tilde{K}$  are closed under multiplication. The inverse of  $(a, 1) \in \tilde{H}$  under the operation in group  $G$  is given by  $(1 \cdot a^{-1}, 1) = (a^{-1}, 1) \in \tilde{H}$  since  $a^{-1} \in H$ . Similarly, the inverse of  $(1, c) \in \tilde{K}$  is given by  $(1, c^{-1}) \in \tilde{K}$ , so both  $\tilde{K}$  and  $\tilde{H}$  are closed under inverses. As both groups clearly contain the identity, they are subgroups of  $G$ . The maps defined in assertion (2) are clearly surjective since they map to all possible values in  $\tilde{H}$  and  $\tilde{K}$  and are also injective since each  $h$  and  $k$  in  $H$  and  $K$  respectively map to exactly one value of  $\tilde{H}$  and  $\tilde{K}$ . Consider  $h_1, h_2 \in H$  and  $k_1, k_2 \in K$ , and denote the mappings from  $K$  and  $H$  to be  $\phi_K$  and  $\phi_H$  respectively. Note that

$$\phi_H(h_1)\phi_H(h_2) = (h_1, 1)(h_2, 1) = (h_1h_2, 1) = \phi_H(h_1h_2) \quad (19)$$

and similarly,

$$\phi_K(k_1)\phi_K(k_2) = (1, k_1)(1, k_2) = (1, k_1k_2) = \phi_K(k_1k_2) \quad (20)$$

such that both mappings are isomorphisms.

(4) We prove (4) and (5) before proving (3). Consider an element  $\tilde{h} = (h, 1) \in \tilde{H}$  that is equal to  $\tilde{k} = (1, k) \in \tilde{K}$ . This implies that  $(h, 1) = (1, k)$ , so that  $h = k = 1$ , so that the only element the groups can have in common is the identity. Therefore, we have that  $\tilde{H} \cap \tilde{K} = 1$ .

(5) Now consider an element in  $\tilde{K}$  acting by conjugation on an element in  $\tilde{H}$ . For  $(h, 1) \in \tilde{H}$  and  $(1, k) \in \tilde{K}$

$$(1, k)(h, 1)(1, k)^{-1} = ((1, k)(h, 1))(1, k^{-1}) \quad (21)$$

$$= (k \cdot h, k)(1, k^{-1}) \quad (22)$$

$$= (k \cdot h \cdot k \cdot 1, kk^{-1}) \quad (23)$$

$$= (k \cdot h, 1). \quad (24)$$

Using the inverse isomorphisms to map from  $(1, k)$  to  $k$  and  $(h, 1)$  to  $h$ , we get that  $\phi(k)\phi(h) = k \cdot h = khk^{-1}$ , proving (5).

(3) Finally, we have just shown that given (2), every element in  $K$  normalizes  $H$ , so that  $K \leq N_G(H)$ . Similarly, we already know that the product of two elements in  $\tilde{H}$  is in  $\tilde{H}$ , so that under the isomorphism in (2), every element in  $H$  normalizes itself, so  $H \leq N_G(H)$ . Since  $G = HK$ , any element  $g \in G$  can be written as the product  $hk$  for  $h \in H$  and  $k \in K$ . Since both these elements normalize  $H$ , then their product will also normalize  $H$ , implying that every element in  $G$  normalizes  $H$ , i.e.  $N_G(H) = G$ . Therefore we have shown that  $H \trianglelefteq G$ , proving (3) and completing the proof.  $\square$

### 3 Relation to the Direct Product

It is important to note that the semidirect product is a more general notion than the direct product, and it is important to realize when  $H \rtimes_{\phi} K$  is isomorphic to  $H \times K$ . Consider when  $\phi$  is the trivial homomorphism from  $K$  into  $\text{Aut}(H)$ . That is,  $\phi(k)(h) = k \cdot h = h$ , so the group operation in  $H \rtimes_{\phi} K$  becomes

$$(h_1, k_1)(h_2, k_2) = (h_1(k_1 \cdot h_2), k_1k_2) = (h_1h_2, k_1k_2) \quad (25)$$

for all  $h_1, h_2 \in H$  and  $k_1, k_2 \in K$ , so that in this case, the multiplication is the same as in the direct product.

## 4 Example : The Dihedral Group $D_{2n}$

We first show how the semidirect product allows us to construct  $D_6$  from  $H = \{1, r, r^2\}$  and  $K = \{1, s\}$ , which we were unable to do with the direct product. Consider a homomorphism  $\phi$  that maps  $1 \rightarrow 1$ , and  $s \rightarrow \text{conjugation by } s$ . Consider conjugating each of the elements in  $H$  by  $s$ :

$$1 \rightarrow s1s^{-1} = 1 \tag{26}$$

$$r \rightarrow srs^{-1} = r^{-1} = r^2 \tag{27}$$

$$r^2 \rightarrow sr^2s^{-1} = r^{-2} = r \tag{28}$$

so conjugation by  $s$  is indeed in  $\text{Aut}(H)$ , and  $\phi$  maps  $K$  to  $\text{Aut}(H)$ . Note that in this case, conjugation by  $s$  is the same as inverting an element in  $K$ . We also observe that this is the only non-trivial homomorphism from  $K$  into  $\text{Aut}(H)$ . Now we have that  $G = H \rtimes_{\phi} K = \{(1, 1), (1, s), (r, 1), (r, s), (r^2, 1), (r^2, s)\} \cong D_6$ , where multiplication in  $G$  is defined by Theorem 2.1. More generally, if  $H = \mathbb{Z}/\mathbb{Z}_n$ , the cyclic group of order  $n$ , then  $H \rtimes_{\phi} K$  is  $D_{2n}$ .

## 5 Classification: Groups of Order 12

There are many applications of the semidirect product to classifications of groups. In order to recognize semidirect products similarly to how we recognized direct products, we will use the following theorem, which we state without proof.

**Theorem 5.1** (Recognition Theorem). *Suppose  $G$  is group with subgroups  $H$  and  $K$  such that*

(a)  $H \trianglelefteq G$  and

(b)  $H \cap K = 1$ .

*If  $\phi$  is a homomorphism from  $K$  into  $\text{Aut}(H)$  defined by mapping  $k \in K$  to the automorphism of left conjugation by  $k$  on  $H$ , then  $HK \cong H \rtimes_{\phi} K$ . Further, if  $G = HK$ , with  $H$  and  $K$  satisfying (a) and (b), then  $G$  is the semidirect product of  $H$  and  $K$ .*

In general the process of classifying all possible groups of order  $n$  is as follows. We first find proper subgroups  $H$  and  $K$  of  $G$  satisfying the above *Recognition Theorem* to determine when a group is a semidirect product, and subsequently find all triples  $H, K$ , and  $\phi$ , where  $\phi$  is a homomorphism from  $K$  into  $\text{Aut}(H)$ . We then compute the semidirect product for each of these triples and then verify which results are isomorphic, resulting in a list of groups of order  $n$ .

As an example, we will investigate the classification of groups of order 12.

Consider a group  $G$  such that  $|G| = 12$ , and let  $H \in Syl_2(G)$  and  $K \in Syl_3(G)$ , the sets of  $Sylow_2$  and  $Sylow_3$  subgroups respectively. We know by *Sylow's Theorem* and prior analysis that either  $H$  or  $K$  is normal in  $G$ . By *Lagrange's Theorem*, both  $|H|$  and  $|K|$  must divide  $|G|$ , and since they are relatively prime, they must also have trivial intersection i.e.  $H \cap K = 1$ . By the *Recognition Theorem*,  $G$  is a semidirect product. Since  $|H| = 4$   $H \cong Z_4$  or  $Z_2 \times Z_2$  (the two groups of order 4) and  $K \cong Z_3$ . We consider the cases in which  $H \trianglelefteq G$  and  $K \trianglelefteq G$  separately.

*Case:  $H \trianglelefteq G$ :*

We start by determining all the possible homomorphisms from  $K$  into  $Aut(H)$ . Considering the case that  $H \cong Z_4$ , we see that  $Aut(H) \cong Z_2$ , so only the trivial homomorphism from  $K$  into  $Aut(H)$  exists. This means that the semidirect product reduces to the direct product, and the  $G \cong Z_3 \times Z_4 = Z_{12}$ , which is the only group of order 12 with a normal cyclic Sylow 2-subgroup.

Therefore, we now consider the case in which  $H \cong Z_2 \times Z_2$ , in which case  $Aut(H) \cong S_3$ . There must be a unique order 3 subgroup of  $Aut(V)$ , which must be cyclic so we denote it  $\langle x \rangle$ . Since  $K$  is isomorphic to  $Z_3$ , we consider  $K = \langle y \rangle$ , which gives the following possible homomorphisms from  $K$  into  $Aut(H)$ , each of which we consider separately:

$$\phi_i(y) = x^i, \quad i = 0, 1, 2. \quad (29)$$

The trivial case is when the homomorphism is  $\phi_0$ , which gives again reduces to the familiar direct product  $Z_2 \times Z_2 \times Z_3$ . In the case of both  $\phi_1$  and  $\phi_2$ , the semidirect products computed will be isomorphic, since  $y^2$  is another possible generator for  $K$  and  $\phi_2(y^2) = x = \phi_1(y)$ . In these cases, the semidirect product yields groups isomorphic to the alternating group of order 12,  $A_4$ . We have so far determined 3 unique groups of order 12. We now consider the case in which  $K \trianglelefteq G$ .

*Case :  $K \trianglelefteq G$  :*

We now start by determining all the homomorphisms from  $H$  into  $Aut(K)$ . Since  $|K| = 3$  is a prime, the order of the automorphism group of  $K$  must be 2, so it must be that  $Aut(K) \cong Z_2$ . We consider the two possible cases for  $H$ . If  $H \cong Z_4$ , then there is the trivial homomorphism from  $H$  into  $Aut(K)$  and that which sends the generator of  $H$  to the generator of  $Aut(K)$ . The trivial homomorphism gives us the direct product of  $Z_3 \times Z_4 \cong Z_{12}$ , which we have already obtained. The nontrivial homomorphism, which in this case inverts elements, gives  $Z_3 \rtimes_{\phi} Z_4$ , a unique non-abelian group of order 12. In particular, we know that it is not  $D_{12}$  or  $A_4$  since it has a cyclic  $Sylow_2$  subgroup of order 4.

Finally, we consider the case in which  $H \cong Z_2 \times Z_2 = \langle x \rangle \times \langle y \rangle$ , since both groups are cyclic. The homomorphisms from  $H$  into  $Aut(K)$  are specified by making their kernels one of the three order 2 subgroups of  $H$ . All three of these semidirect products (one for each homomorphism) are easily seen to be isomorphic to  $S_3 \times Z_2$ .

We conclude that there are total of 5 groups of order 12.

## 6 Conclusion

We have therefore defined a product between groups  $H$  and  $K$  possessing a homomorphism from  $K$  into  $\text{Aut}(H)$ , that allows us to construct a larger group  $G$  satisfying Theorem 2.1. We have also shown how we can use the *Recognition Theorem* to determine when a group is a semidirect product, allowing us to classify all groups of certain orders. Among the numerous other examples are the classification of groups of order 30 and  $p^3$  (for  $p$  an odd prime). In the example considered above, the procedure works well because  $H$  and  $K$  often have prime or prime squared order, making it easier to determine their automorphism groups.