FINDING SEMIDIRECTION IN YOUR LIFE

ARUN DEBRAY

1. Introduction

The goal of this article is to explore the semidirect product, a generalization of the direct product for groups. First there is an overview illustrating how the semidirect product arises, and then the formal definition will be provided and the intuition behind the semidirect product will be formalized into a set of its properties. Finally, the semidirect product will be further motivated by listing some of its applications.

The direct product is given in two ways: the external direct product of groups A and B is defined by creating a group structure on the Cartesian product $A \times B$, which can be used to make smaller groups into larger ones. There is also an internal direct product, which decomposes a group into a direct product of smaller groups by writing it as isomorphic to an external direct product of two of its normal subgroups.

The semidirect product also exists in both internal and external flavors, but unlike the direct product, the external semidirect product arises from the internal one, since the internal semidirect product is easier to define and to understand. The key idea is that if H and K are subgroups of G with H normal in G, but not necessarily K, their product as subsets of G is a subgroup. This subgroup might not be isomorphic to $H \times K$, but there is a meaningful way to describe it in terms of H and K. This subgroup is known as the internal semidirect product of H and K, since it is defined as a subgroup of G, and is written $H \rtimes K$.

Then, one can generalize to arbitrary groups H and K to yield the external semidirect product. However, this requires care: the internal semidirect product is built in a way that required multiplying elements of H with elements of K. This is well-defined when H and K are both subgroups of some other group G, but for arbitrary groups, one must find a suitable analogue to multiplication.

One aspect of the direct product that will not carry over to the generalization is that one can take the direct product of any finite or countably infinite collection of groups, but the semidirect product is defined in terms of exactly two groups. This occurs because the direct product for groups is motivated by the direct product of sets, which is defined for a finite or countably infinite number of sets, but the semidirect product originates in the decomposition of a group into exactly two parts, and is both harder and less useful to generalize. One can nest semidirect products, but they are in general not associative, so this nesting doesn't operate in the same manner.

2. Review of the Direct Product

Since the semidirect product is a generalization of the direct product, it will be helpful to recall some properties of the direct product.

In the study of groups, the direct product is an important way to both understand large groups in terms of smaller ones and to build new groups from older ones. Any two groups give a direct product group by component-wise multiplication, but if one wishes to decompose a given group G into a direct product of two groups, both of these groups have to be normal in G, which limits the direct product's applicability.

The following results will also be useful, and will be presented without proof:

- If H and K are groups, then $H \times K$ (the external direct product) is also a group under component-wise application of the group operation.
- $A \times B \cong B \times A$ through the isomorphism $(a, b) \mapsto (b, a)$.
- $|A \times B| = |A||B|$.
- $H \cong \tilde{H} = \{(h, 1) \mid h \in H\}$ and $K \cong \tilde{K} = \{(1, k) \mid k \in K\}$, with $\tilde{H}, \tilde{K} \leq H \times K$. This relates the external direct product $H \times K$ with the internal direct product $\tilde{H} \times \tilde{K}$.
- If G is a group and $H, K \leq G$, then the set of products is defined to be $HK = \{hk \mid h \in H, k \in K\}$ with induced map $f : (h, k) \mapsto hk$. In general, HK is not a subgroup of G, and f is not a homomorphism.

However, there are some cases in which $HK \leq G$, so HK can be "decomposed" into $H \times K$. A sufficient condition for this is normality of H and K in G and that H and K have minimal intersection:

Theorem 1. *If $H, K \trianglelefteq G$ and $H \cap K = \{1\}$, then:*

i. $HK \leq G$,
ii. $H \times K \cong HK$, *and*
iii. the map f *given above is an isomorphism* $H \times K \to HK$.

Using this theorem, it is possible to analyze a group by viewing it as an internal direct product of smaller groups, which are better understood.

But it's possible to be more general: suppose $H \trianglelefteq G$ as before, but $K \leq G$ is not necessarily normal.

Lemma 2. *In this case,* HK *is still a subgroup of* G.

Proof. Since $1 \in H$ and $1 \in K$, then $(1)(1) = 1 \in HK$, so HK is nonempty.

Suppose $x_1, x_2 \in HK$; then, $x_1 = h_1k_1$ for some $h_1 \in H$ and $k_1 \in K$, by the construction of HK, and similarly, $x_2 = h_2k_1$ for an $h_2 \in H$ and a $k_2 \in H$. Then, $x_1x_2 = h_1k_1h_2k_2 = h_1k_1h_2k_1^{-1}k_1k_2$. Because H is normal in G, $k_1h_2k_1^{-1} \in H$, and so $h_1(k_1h_2k_1^{-1}) \in H$ as well, since subgroups are closed under multiplication. Similarly, $k_1^{-1}k_2 \in K$ since both k_1 and k_2 are.

Thus, $x_1x_2 = hk$ for some $h \in H$ and $k \in K$, so HK is closed under multiplication.

Considering inverses,

$$x^{-1} = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} = k_1^{-1}h_1^{-1}k_1k_1^{-1}.$$

$h_1^{-1} \in H$ and H is normal in G, then $k_1^{-1}h_1^{-1}k_1 \in H$, so since $k_1 \in K$, then $k_1^{-1} \in K$ as well; thus $x_1^{-1} = hk$ for some $h \in H$ and $k \in K$, so HK is closed under inverses.

Since HK is nonempty and closed under multiplication and inverses, $HK \leq G$. □

Here, the function f from Theorem 1 is again a bijection, but it isn't necessarily an isomorphism.

3. The Definition of the Semidirect Product

In this case, it isn't necessarily true that $HK \cong H \times K$, but it would be nice to be able to describe HK as some sort of internal product of H and K in G. This can be done by observing how multiplication in HK corresponds to the group operations in H and K: in some sense, the product should be given by $(h_1, k_1)(h_2, k_2) = (h_1(k_1h_2k_1^{-1}), k_1k_2)$. But if one also wants the semidirect product to be useful abstractly, then it must be possible to define what conjugation means in the external case, where multiplication between elements of H and K is not necessarily defined.

Since conjugation is a group action of K on H, the definition builds this "twist" into the multiplication by using such a group action, so that $(h_1, k_1)(h_2, k_2) = (h_1(k_1 \cdot h_2), k_1k_2)$ in this general case. In order for this action to be well-behaved, it must come from $\mathrm{Aut}(H)$, so the external semidirect product can be defined more compactly by specifying the homomorphism from K into $\mathrm{Aut}(H)$, which then defines a group action naturally:

Definition. Suppose H and K are groups, and let $\varphi : K \to \mathrm{Aut}(H)$ be a homomorphism. Let $\cdot$ be the left action of K on H given by G as above (i.e. $k \cdot h = \varphi(k)(h)$). Then, the semidirect product of H and K, denoted $H \rtimes_\varphi K$ (or $H \rtimes K$ if φ is clear from context), is the set $H \times K$ with multiplication given by

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

for $h_1, h_2 \in H$ and $k_1, k_2 \in K$, so that (h_1, k_1) and (h_2, k_2) are in $H \rtimes K$.

Theorem 3. $H \rtimes K$ *is a group under the group operation defined above.*

Proof. The key to this proof is that multiplication in $H \rtimes K$ is defined using a group action; its nice properties will lead to the group axioms.

Suppose $(h_1, k_1), (h_2, k_2), (h_3, k_3) \in H \rtimes K$. Then,

$$\begin{aligned}((h_1, k_1)(h_2, k_2))(h_3, k_3) &= (h_1(k_1 \cdot h_2), k_1k_2)(h_3, k_3)\\ &= (h_1(k_1 \cdot h_2)((k_1k_2) \cdot h_3), k_1k_2k_3)\\ &= (h_1(k_1 \cdot h_2)(k_1 \cdot (k_2 \cdot h_3)), k_1k_2k_3)\\ &= (h_1(k_1 \cdot (h_2(k_2 \cdot h_3))), k_1k_2k_3)\\ &= (h_1, k_1)(h_2(k_2 \cdot h_3), k_2k_3)\\ &= (h_1, k_1)((h_2, k_2)(h_3, k_3)),\end{aligned}$$

so multiplication in $H \rtimes K$ is associative.

The element $(1, 1) \in H \rtimes K$ is the identity: for any $(h, k) \in H \rtimes K$,

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

and similarly,

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

The inverse of (h,k) is $(k^{-1}\cdot h^{-1}, k^{-1})$:

$$\begin{aligned}(k^{-1}\cdot h^{-1}, k^{-1})(h,k) &= ((k^{-1}\cdot h^{-1})(k^{-1}\cdot h), k^{-1}k)\\ &= (k^{-1}\cdot(h^{-1}h),1)\\ &= (k^{-1}\cdot 1, 1) = (1,1),\end{aligned}$$

and similarly,

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

□

Example 1. The simplest interesting example of the semidirect product is when $H = \mathbb{Z}/n\mathbb{Z}$ and $K = \mathbb{Z}/2\mathbb{Z}$. Here, φ gives the group action $k\cdot h = h^{-1}$ for all $h\in H$ and $k\in K$.

Let $\tilde{h} = (h,1)$ and $\tilde{k} = (1,k)$ for some $h\in H$ and $k\in K$. Then, $\tilde{h}^2 = (h(1\cdot h),1) = (h^2,1)$, and thus for any $a\in\mathbb{Z}$, $\tilde{h}^a = (h^a,1)$. In particular, $\tilde{h}^n = (h^n,1) = (1,1) = 1$. Similarly, $\tilde{k}^2 = (1(k\cdot 1),k^2) = (1(1^{-1}),1) = (1,1) = 1$. Additionally,

$$\begin{aligned}\tilde{k}\tilde{h}\tilde{k}^{-1} &= (1,k)(h^{-1},1)(1,k)\\ &= (1(k\cdot h),k)(1,k) = (h^{-1},k)(1,k)\\ &= (h^{-1}(k\cdot 1),k^2)\\ &= (h^{-1}1^{-1},1) = (h^{-1},1) = \tilde{h}^{-1}.\end{aligned}$$

Thus, $\langle\tilde{h},\tilde{k}\rangle \le H\rtimes K$ is isomorphic to D_{2n}, since it is given by the same generators and relations:

$$\left\langle r,s \mid r^n = s^1 = 1, srs = r^{-1}\right\rangle.$$

However, since $|H\rtimes K| = |H||K| = 2n$ (by Corollary 4, below), then $\langle\tilde{h},\tilde{k}\rangle$ is in fact all of $H\rtimes K$ — so $H\rtimes K\cong D_{2n}$.

Interestingly, since $H\rtimes K$ and $H\times K$ are the same set of elements and differ only in their group operation, this means that $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ and D_{2n} can be thought of as two different multiplications defined on the same set. This is particularly noteworthy given that their definitions were in no way related.

4. Corollaries to the Definition

There are several immediate consequences of Theorem 3:

Corollary 4. $|A\rtimes B| = |A||B|$.

Proof. Since $A\rtimes B$ and $A\times B$ are identical as sets, then they have the same number of elements, so $|A\rtimes B| = |A\times B| = |A||B|$. □

Like the direct product, the semidirect product contains subgroups isomorphic to each of the groups in the product:

Corollary 5. *Let $\tilde{H} = \{(h,1) \mid h\in H\}$ and $\tilde{K} = \{(1,k)\mid k\in K\}$. Then, $\tilde{H}$ and $\tilde{K}$ are subgroups of $H\rtimes K$, $H\cong\tilde{H}$, and $K\cong\tilde{K}$.*

Proof. Neither $\tilde{H}$ nor $\tilde{K}$ is nonempty, since $(1,1)$ is in both.

Suppose $(h_1,1),(h_2,1)\in\tilde{H}$. Then, $(h_1,1)(h_2,1) = (h_1(1\cdot h_2),1) = (h_1h_2,1)\in\tilde{H}$, and $(h_1,1)^{-1} = (h_1^{-1},1)\in\tilde{H}$ as well, so $\tilde{H}\le H\rtimes K$.

Similarly, if $(1,k_1),(1,k_2)\in\tilde{K}$, then $(1,k_1)(1,k_2) = (1(k_1\cdot 1),k_1k_2) = (1,k_1k_2)\in\tilde{K}$, and $(1,k_1)^{-1} = (1,k_1^{-1})\in\tilde{K}$, so $\tilde{K}\le H\rtimes K$ as well.

The map $f: H\to\tilde{H}$ given by $f(h) = (h,1)$ is a bijection since it has a well-defined inverse $(h,1)\mapsto h$. It is also a group homomorphism: if $h_1,h_2\in H$, then $f(h_1)f(h_2) = (h_1,1)(h_2,1) = (h_1h_2,1) = f(h_1h_2)$. Thus, f is an isomorphism, so $H\cong\tilde{H}$.

Similarly, $g: K\to\tilde{K}$ given by $g(k) = (1,k)$ is a bijection, since it has a well-defined inverse $(1,k)\mapsto k$, and it is a homomorphism: if $k_1,k_2\in K$, then $g(k_1)g(k_2) = (1,k_1)(1,k_2) = (1,k_1k_2) = g(k_1k_2)$. Thus, g is an isomorphism, and $K\cong\tilde{K}$. □

Often, the tildes are dropped, identifying H and K with their subgroups in $H \rtimes K$, though this is only true up to isomorphism.

These subgroups of $H \rtimes K$ illustrate that the definitions of the internal and external semidirect product agree. Specifically, the internal semidirect product of $\tilde{H}$ and $\tilde{K}$ given in Corollary 5 and the external semidirect product of H and K share the properties that motivated their definitions:

Corollary 6. *With $\tilde{H}$ and $\tilde{K}$ as in Corollary 5,*

(1) $\tilde{H} \trianglelefteq H \rtimes K$,
(2) $\tilde{H} \cap \tilde{K} = \{1\}$, and
(3) If $\tilde{h} = (h, 1) \in \tilde{H}$ and $\tilde{k} = (1, k) \in \tilde{K}$, then $\tilde{k}\tilde{h}\tilde{k}^{-1} = k \cdot h$.

Proof. Part 2 is clear: if $(h, 1) = (1, k)$, then $h = k = 1$, so $\tilde{H} \cap \tilde{K} = \{1\}$.

Suppose $\tilde{h} = (h, 1)$ and $\tilde{k} = (1, k)$. Then,

$$\begin{aligned}(1,k)(h,1)(1,k)^{-1} &= (1,k)(h,1)(1,k^{-1}) \\ &= (k \cdot h, k)(1, k^{-1}) \\ &= ((k \cdot h)(k \cdot 1), kk^{-1}) \\ &= (k \cdot h, 1).\end{aligned}$$

This proves Part 3, and since K acts on H, then $k \cdot h \in H$, so $\tilde{k}\tilde{h}\tilde{k}^{-1} = (k \cdot h, 1) \in \tilde{H}$, which implies Part 1. □

These last two corollaries flesh out the properties of the semidirect product: though the definition of the external semidirect product gives a group, the properties shown in the corollaries are the desired ones given the motivation in the internal case. Since these properties follow from the definition, then the definition can be used as desired in both the external and the internal case. The corollaries themselves are also very useful independently of motivation, since they provide quite a lot of useful information on subgroups of a given semidirect product.

It is also worth noting two distinct differences between $H \rtimes K$ and $H \times K$: first, it is not true in the general case that $H \rtimes K \cong K \rtimes H$, and second, $H \rtimes K$ is not necessarily abelian, even if H and K are (as in $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \cong D_{2n}$).

As might be expected, the semidirect product reduces to the direct product when $K \trianglelefteq G$. The following proposition formalizes this by considering the three aspects of the differences between the semidirect and the direct products: their definitions, their rules of multiplication (i.e. Part 2, since the homomorphism determines multiplication in $H \rtimes K$), and whether K is normal in the product. These three criteria, which all arose at different points of the motivation, are equivalent, which further anchors the abstract definition into the intuition it was designed to follow.

Proposition 7. *Suppose H and K are groups and $\varphi : K \to \mathrm{Aut}(H)$ is a group homomorphism. Then, the following are equivalent:*

(1) $H \rtimes K = H \times K$.
(2) $\varphi(k) = 1$ for every $k \in K$.
(3) $\tilde{K} \trianglelefteq H \rtimes K$.

Proof. It will be shown that (1) $\implies$ (2) $\implies$ (3) $\implies$ (1).

By (1), for any $h_1, h_2 \in H$ and $k_1, k_2 \in K$, $(h_1, k_1)(h_2, k_2) = (h_1(k_1 \cdot h_2), k_1k_2) = (h_1h_2, k_1k_2)$, so $k_1 \cdot h_2 = h_2$ for all $k_1 \in K$ and $h_2 \in H$. Thus, $\cdot$ is the trivial action, so $\varphi(k_2) = 1$, which proves (2).

Thus, by Part 3 of Corollary 6, $hkh^{-1} = k \cdot h = h$ for all $h \in H$ and $k \in K$, then $hk = kh$, so $\tilde{H} \subseteq N_{H \rtimes K}(\tilde{K})$. Since the normalizer is a subgroup and K is in its own normalizer, then $HK = H \rtimes K \subseteq N_{H \rtimes K}(\tilde{K})$, so the normalizer of K is the entire group,which implies that K is normal, which satisfies (3).

Then, since $hk = kh$ for all $h \in H$ and $k \in K$, $h_1(k_1 \cdot h_2) = h_2(k_2 \cdot h_1)$, so the action of K on H is the trivial action, so both of these are equal to h_1h_2. Thus, $(h_1, k_1)(h_2, k_2) = (h_1h_2, k_1k_2)$, so multiplication in $H \rtimes K$ is identical to the rule in $H \times K$. Since these sets contain the same elements, then $H \rtimes K = H \times K$, which implies (1). □

5. Some uses of the Semidirect Product

In addition to analyzing a large group in terms of smaller ones, the semidirect product can be used to create entirely novel groups. For example, the dihedral group D_{2n} can be built from finite cyclic groups, as above. However, the construction given can be generalized to the infinite case, where $H = \mathbb{Z}$, leading to a group with the following generators and relations:

$$\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} = \left\langle r, s \mid s^2 = 1, srs = r^{-1} \right\rangle.$$

This group is called the infinite dihedral group and denoted D_∞ or Dih_∞. Intuitively, since D_{2n} is the set of symmetries of the n-gon, D_∞ should correspond to some analogous infinite object. One's first guess might be a circle, which is the limit of successive n-gons as $n \to \infty$, but D_∞ is not the group of symmetries of a circle: for every angle $0 \leq \theta < 2\pi$, there is a distinct symmetry of the circle that is given by rotation through the angle θ. However, there are an uncountable number of such θ, while D_∞ is countable.

If one instead considers an n-gon to have sides of unit length, their limit is the real line, with a vertex at each integer. Thus, D_∞ can be considered to be the set of symmetries of the integers: r sends each vertex to the right, so that $r(x) = x+1$ for any $x \in \mathbb{Z}$, and s flips the number line: $s(x) = -x$. Then, $rsr^{-1}(x) = rs(x-1) = r(-x+1) = -x = s(x)$, satisfying the generators and relations. (Intuitively if one flips the integers, shifts them to the right, and then flips them back, the result is the same as if they had been shifted to the left.)

In a similar process, one can take the semidirect product of $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ when $n \neq 2$, letting φ again give the group action $k \cdot h = h^{-1}$. Thus, one obtains the generators and relations

$$\mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/n\mathbb{Z} = \left\langle x, y \mid x^m = y^n = 1, yxy^{-1} = x^{-1} \right\rangle.$$

This is a nonabelian group of order mn (unless one of m or n equals 1), and is often something new: for example, when $m = 3$ and $n = 4$, the group $G = \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ is a nonabelian group of order 12 with $\langle(\bar{0}, \bar{1})\rangle$ a cyclic subgroup of order 4. Thus, G is isomorphic to neither A_4 nor D_{12}, since neither has a cyclic subgroup of order 4. A list of small nonabelian groups contains many such semidirect products of small cyclic groups.

Another useful construction involving the semidirect product is the holomorph of a group:

Definition. If H is any group, then the holomorph of H is $\mathrm{Hol}(H) = H \rtimes \mathrm{Aut}(H)$, where φ is the identity map.

This construction is useful both to generate new examples of groups and to treat group elements and group automorphisms in a unified manner.

Example 2. If φ is an automorphism of $\mathbb{Z}/3\mathbb{Z}$, then $\varphi : \bar{0} \mapsto \bar{0}$, and either $\bar{1} \mapsto \bar{2}$ and $\bar{2} \mapsto \bar{1}$ or φ is the identity; thus, $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$ has 2 elements, since they were both explicitly listed, and is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

Thus, $\mathrm{Hol}(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} = D_6$.

Semidirect products are also useful for classifying groups of a given order. The key to this is the decomposition of a group into a semidirect product, analogous to Theorem 1:

Theorem 8. *Suppose G is a group and H and K are subgroups of G such that H is normal in G and $H \cap K = \{1\}$. If $\varphi : K \to \mathrm{Aut}(H)$ is given by $\varphi(k)(h) = khk^{-1}$, then $HK \cong H \rtimes K$. In particular, if $G = HK$, then $G \cong H \rtimes K$.*

Proof. By Lemma 2, HK is a subgroup of G, since H is normal.

Since every element of HK can be written uniquely as a product hk, with $h \in H$ and $k \in K$, then $(h, k) \mapsto hk$ is a bijection.

It can be computed that this is a homomorphism, and in fact this is the same calculation as in Lemma 2, so the map is an isomorphism. □

This theorem is a useful tool for classifying groups of a given order, and provides some more information about the structure of such groups. The general algorithm is as follows:

(1) Prove that every group G of a given order n has subgroups $H \trianglelefteq G$ and $K \leq G$ such that $H \cap K = 1$ and $HK = G$.
(2) Then, list all of the isomorphism classes of H and K meeting the above conditions.
(3) For each pair of H and K found in the previous step, identify all homomorphisms $\varphi : K \to \mathrm{Aut}(H)$.
(4) For each triple H, K, φ, write down $H \rtimes_\varphi K$, and eliminate those groups that are isomorphic to something already on the list.

This approach can be tedious, but it produces a complete list of groups of order n up to isomorphism. Sometimes, Sylow's Theorem can be helpful, in order to enumerate subgroups of a given order or to show H is normal, and Lagrange's Theorem can be used to show that $H \cap K = \{1\}$ if $|H|$ and $|K|$ are relatively prime.

This approach is not comprehensive, however. Q_8, the quarternion group, cannot be written as a semidirect product, since no two of its subgroups H and K satisfy both $H \cap K = \{1\}$ and $HK = Q_8$. In general, this process works better when the order of the group doesn't divide a large power of a prime, because many such groups cannot be written as semidirect products. These groups may be more approachable from the perspective of Sylow's Theorem.

Decomposing groups is aided by a result called the Splitting Lemma, which allows another way to check if a group B is isomorphic to some semidirect product of two of its subgroups. It occurs in the context of the following definition:

Definition. A short exact sequence of groups is a collection of groups and homomorphisms between them $A \xrightarrow{f} B \xrightarrow{g} C$, such that f is injective, g is surjective, and $\mathrm{Im}(f) = \mathrm{Ker}(g)$. Such a sequence of groups is often denoted $1 \to A \to B \to C \to 1$ (or with 0 instead of 1 if the groups are written additively).

The lemma is usually stated in more generality, but the version for groups is as follows:

Lemma 9 (Splitting Lemma for Groups)**.** *Suppose $1 \to A \xrightarrow{f} B \xrightarrow{g} C \to 1$ is a short exact sequence, and suppose there exists a homomorphism $\varphi : C \to B$ such that $g \circ \varphi$ is the identity map on C. Then, $B \cong A \rtimes C$.*

Proof. By the First Isomorphism Theorem, $A \cong \mathrm{Ker}(g) = \mathrm{Im}(f) \trianglelefteq B$. Denote $\mathrm{Ker}(g)$ by $\tilde{A}$, since it is isomorphic to A. Similarly, since g is surjective and $g \circ \varphi$ is the identity, then $\mathrm{Ker}(\varphi) = 1$ (since otherwise one would obtain non-identity elements of C which map to the identity by $g \circ \varphi$). Thus, φ is injective, so $C \cong \mathrm{Im}(\varphi) \leq B$, again by the First Isomorphism Theorem. Denote $\tilde{C} = \mathrm{Im}(\varphi)$.

If $x \in \tilde{A} \cap \tilde{C}$, then $x \in \mathrm{Ker}(g) \cap \mathrm{Im}(\varphi)$, which means that x must map to 1, since $g \circ \varphi$ is the identity. Thus, $\tilde{A} \cap \tilde{C} = \{1\}$.

Additionally, by the First Isomorphism Theorem, $B/\tilde{A} \cong \tilde{C}$ (using g as the homomorphism), so since every element in B can be written uniquely as a product of an $a \in \tilde{A}$ and an element of its identity coset, then every element in B can correspondingly be written as a product of an element of $\tilde{A}$ and an element of $\tilde{C}$. Thus, $B = \tilde{A}\tilde{C}$, since $\tilde{A}\tilde{C} \subseteq B$.

Thus, $\tilde{A}$ and $\tilde{C}$ meet all the conditions for Theorem 8, so $B \cong \tilde{A} \rtimes \tilde{C}$. Since $A \cong \tilde{A}$ and $C \cong \tilde{C}$, then $A \rtimes C \cong \tilde{A} \rtimes \tilde{C}$, so $B \cong A \rtimes C$ as well. □

This can make some proofs considerably shorter: for example, consider the short exact sequence $0 \to \mathbb{Z}/n\mathbb{Z} \xrightarrow{f} D_{2n} \xrightarrow{g} \mathbb{Z}/2\mathbb{Z} \to 0$ with $f : \bar{a} \mapsto r^a$ and $g : r^a s^b \mapsto \bar{b}$. It is straightforward to show these are group homomorphisms, and that $\mathrm{Im}(f) = \mathrm{Ker}(g) = \langle r \rangle$. φ can be given explicitly by $\varphi(\bar{0}) = 1$ and $\varphi(\bar{1}) = s$, so that $g \circ \varphi$ is the identity. Then, the Splitting Lemma's requirements are met, so $D_{2n} \cong \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

The Splitting Lemma can be defined on many structures other than groups; for example, the analogous statement in which A, B, and C are vector spaces implies the Rank-Nullity Theorem from linear algebra, an unexpected connection.