Converses to the Splitting Lemma in the Category of Groups

William Cabell

May 02, 2018

1 Introduction

The splitting lemma is an important result in category theory that states that for a category $\mathcal{C}$, objects $A, B, C \in \text{obj}(\mathcal{C})$, morphisms $\theta \in \text{Hom}(A, B)$, $\varphi \in \text{Hom}(B, C)$, and $1_{\mathcal{C}}$, the unity element in $\mathcal{C}$ such that the sequence

$$1_{\mathcal{C}} \to A \xrightarrow{\theta} B \xrightarrow{\varphi} C \to 1_{\mathcal{C}}$$

is short exact, then $B \cong A \oplus C$ if the sequence is split; that is, if there exists a morphism $\varphi^{-1} \in \text{Hom}(C, B)$ such that $\varphi^{-1}\varphi = \text{id}_C$, the identity on C. In summary, the lemma asserts that if one object injects into a second object, and that second object projects onto a third object, then the second object is a direct sum of the first and third objects.

The converse of the lemma does not hold in general. We will explore a few cases in which the converse does hold in the category of groups, with the hope that such exploration might illuminate future research on the subject. We will show, specifically, that if a group can be partially decomposed into smaller groups, we may be able to work with the decomposition to find split exact sequences.

A quick word on notation: $\mathbb{Z}_n$ refers to the cyclic group of order n and D_{2n} refers to the dihedral group of order $2n$. All other notation is introduced as necessary or is standard enough to be unambiguous.

I would like to thank Dr. Linnell for suggesting this topic, for overseeing my research, and for guiding me along the way towards a final result.

1.1 Group Extensions

In group theory, short exact sequences are known as extensions. Extensions are fairly well-studied in group theory as they are closely related to the classification of groups. The problem of classifying groups based on simple components by group extensions is referred to as the extension problem. The extension problem is the subject of much current research in group theory [4].

Definition 1. If N and Q are groups, then a group G is called an extension of N by Q if there exists a short exact sequence

$$1 \to N \to G \to Q \to 1$$

where 1 is the trivial group.

From this definition, it follows that N must be a normal subgroup of G and $G/N \cong Q$, and given any normal subgroup N of a group G, we can construct such a sequence. However, it is not generally true that $G = N \times G/N$ for any $N \lhd G$; an easy counterexample is that $\mathbb{Z}_4 \neq \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Thus we cannot trivially generate extensions by normal subgroups, and, equivalently, we cannot trivially form converses to the splitting lemma in the category of groups.

1.2 Finitely Generated Abelian Groups

The converse of the splitting lemma is generally true for finitely generated Abelian groups; that is, any finitely generated Abelian group of the form $H \oplus K$ will form a split exact sequence. We can easily form such groups, since any finitely generated Abelian group has a primary decomposition into a direct sum of primary cyclic subgroups and infinite cyclic subgroups.

2 Decomposition of Groups

The simplest way to decompose a group into components is the direct product. If a group is of the form $G \cong H \times K$ for some groups H and K, we have formed the trivial extension

$$1 \to H \xrightarrow{f} H \times K \xrightarrow{g} K \to 1$$

where f is the natural injection $f : h \mapsto (h, e)$ and g is the natural projection $g : (h, k) \mapsto k$. This sequence is obviously exact, and splits by the function $K \to H \times K$ where $k \mapsto (0, k)$.

We can write an isomorphic sequence

$$1 \to H \xrightarrow{f^*} G \xrightarrow{g^*} K \to 1$$

where f^* and g^* are the appropriate induced maps by functions mapping an element in $H \times K$ to G and G to $H \times K$, respectively. Throughout the rest of this paper, sequences with a group and the composition of a group will be used interchangeably, with the understanding that once such compositions are known, such functions are trivial to create.

2.1 Examples

Group theorists may classify extensions by direct product as trivial, but they are not so unimportant in the context of the splitting lemma, especially in the non-Abelian case. We will list some easy corollaries to the fact that any direct product forms a split exact sequence.

- **Nilpotent Groups:** Any nilpotent group can be written as a direct product of its Sylow subgroups, so any Sylow subgroup or direct product of Sylow subgroups of a nilpotent group will split the group.
- **Chain Conditions:** Any group having only finite-length ascending chains or only finite-length descending chains of normal subgroups can be expressed as a direct product of finitely many of its normal subgroups. [2] Equivalently, any direct factor of a group meeting either chain condition splits the group.

The direct product is useful because of the great body of knowledge we have built up behind it. There are many fairly strong statements we can make with it, as shown. To form a split extension, however, only one subgroup must be normal. In the direct product, both must be. So, clearly, we can generalize.

3 Semidirect Product

The important distinction from the direct product is that for $G \cong N \times H$, both N and H must be normal, while in the semidirect product only N must be normal.

Definition 2. The semidirect product of normal subgroup N and subgroup Q of group G is isomorphic to G, written

$$G \cong N \rtimes Q$$

if and only if there exists a split short exact sequence $1 \to N \to G \to Q \to 1$.

The characterization of a combination of groups as a semidirect product has a separate derivation, which is that $G \cong N \rtimes H$ if and only if $N \cap H = 1$ and there exist unique $n \in N, h \in H$ such that for any $g \in G$, $g = nh$. We will use these definitions interchangeably.

In the context of Abelian groups, the semidirect product is redundant, since it is isomorphic to the direct product. In the context of non-Abelian groups, though, the semidirect product is very useful – though we must consider a few subtleties.

First, unlike the direct product, the semidirect product is not necessarily unique. A quick example is $\mathbb{Z}_4 \rtimes \mathbb{Z}_2$, which is isomorphic to three groups: $\mathbb{Z}_4 \times \mathbb{Z}_2$, D_8, and the quaternion group of order 8. Second, if $G \cong H \rtimes K$ and $H, K \lhd G$, then $G \cong H \times K$. The first fact shows why it is difficult to construct groups from simple groups (why the extension problem is difficult), and the second fact allows us to deconstruct some groups more easily.

3.1 The Schur-Zassenhaus Theorem

The Schur-Zassenhaus Theorem is by far the most general theorem dealing with the existence of semidirect products. It states that if a normal subgroup of a group is a Hall subgroup, that is, the order of the subgroup is coprime to the order of its quotient group, then it splits the group by its quotient group. We will extend the Schur-Zassenhaus Theorem.

3.2 The Dihedral Group

The dihedral group is perhaps the easiest-to-consider non-Abelian group, so our analysis shall begin with it. We will refer to the elements of D_{2n} as r for the first rotation and h as an arbitrary involution. For example, $D_8 = \{e, r, r^2, r^3, h_0, h_1, h_2, h_3\}$.

We consider first the simple case D_8, in particular, its cyclic subgroups. D_8 has precisely two cyclic normal subgroups: $\langle r \rangle$ and $\langle r^2 \rangle$. To form semidirect products, we must consider whether either of these normal subgroups together with another subgroup of D_8 forms the entire group D_8 subject to the conditions previously specified. In fact, one such pair jumps out immediately – the pair $\langle r \rangle$ and $\langle h \rangle$. Any element in $d \in D_8$ can be represented uniquely as $d = r^a h^b$ for some $0 \leq a \leq 3, 0 \leq b \leq 1$, and $\langle r \rangle \cap \langle h \rangle = 1$, so $D_8 \cong \langle r \rangle \rtimes \langle h \rangle$. It is worth noting for generality's sake that $\langle r \rangle \cong \mathbb{Z}_4$ and $\langle h \rangle \cong \mathbb{Z}_2$. Examining the underlying Cartesian product, we can see that a very natural definition of the general group D_{2n} is as the group defined similarly for n: $\mathbb{Z}_n \rtimes \mathbb{Z}_2$.

3.3 The Chinese Remainder Theorem

The emergence of the cyclic group as a component of D_{2n} facilitates the use of even smaller components, in particular, primary cyclic subgroups of $\mathbb{Z}_n$ (equivalently, Sylow subgroups of $\mathbb{Z}_n$). We could make a statement about such subgroups for D_{2n}, but actually we can make an even more general statement with the following definition.

Definition 3. A Hall divisor is a positive integer d dividing positive integer n if $(d, \frac{n}{d}) = 1$, where the tuplet denotes the greatest common denominator of the two numbers. Note that by this definition, $\frac{n}{d}$ is also a Hall divisor.

Theorem 1. Let b be a Hall divisor of n such that $n = ab$. Given a group G and a subgroup $H \leq G$ such that $G \cong \mathbb{Z}_n \rtimes H$, the cyclic group of order b splits G such that

$$G \cong \mathbb{Z}_b \rtimes (\mathbb{Z}_a \rtimes H).$$

Proof. Let $G \cong \mathbb{Z}_n \rtimes H$ for $H \leq G$, let r be a generator for the cyclic group $\mathbb{Z}_n$, and let $h \in H$. Let $n = ab$ such that $(a, b) = 1$ (equivalently, let a be a Hall divisor of n with $n = ab$).

By the definition of G, $\mathbb{Z}_n \lhd G$ so $grg^{-1} \in \mathbb{Z}_n$ for all $g \in G$ and $r \in \mathbb{Z}_n$. We note here that there exists a normal subgroup of both G and $\mathbb{Z}_n$ isomorphic to $\mathbb{Z}_b$. Consider the elements of order b in $\mathbb{Z}_n$. Under conjugation, such elements will still be in $\mathbb{Z}_n$ since $\mathbb{Z}_n$ is normal by construction, and they will also be in $\mathbb{Z}_b$ since they will have order divisible by b. Conjugation by the identity ensures that conjugation is surjective onto $\mathbb{Z}_b$, so an entire cyclic subgroup is formed.

Thus, by the definition of a semidirect product, there exists a unique representation for all elements $g \in G$ of the form

$$g = r^k \cdot h$$

for some $h \in H$, $k \in \mathbb{Z}$ where $0 \leq k < n$. By the Chinese remainder theorem, $r^k = r^{as} \cdot r^{bt}$ for some integers s and t. Then each element has a unique representation of the form

$$g = r^{as} \cdot r^{bt} \cdot h.$$

Because $\langle r^a \rangle \cong \mathbb{Z}_b$, $\langle r^b \rangle \cong \mathbb{Z}_a$, and $\mathbb{Z}_b \lhd G$, we have that

$$G \cong \mathbb{Z}_b \rtimes (\mathbb{Z}_a \rtimes H).$$

□

Theorem 1 is an extension of the Schur-Zassenhaus Theorem since there is no restriction on the order of H, so $\mathbb{Z}_b$ is not necessarily a Hall subgroup of G.

3.4 Nilpotent Groups

The idea of convolving across direct factors of a partially decomposed group seems appealing. Indeed, it worked very cleanly for D_{2n}; we were able to find many split extensions of D_{2n} and, in fact, any group isomorphic to $\mathbb{Z}_n \rtimes H$. It turns out that we can take the same idea and generalize it beyond decomposition of cyclic groups to decomposition of nilpotent groups.

To intuit Theorem 2, recall that a nilpotent group can be written as a direct product of its Sylow subgroups

$$K \cong S_{p_1} \times S_{p_2} \times \cdots \times S_{p_k}$$

where S_{p_i} denotes a Sylow p_i-subgroup.

Theorem 2. Let $G \cong K \rtimes H$ for some nilpotent group K. Any Sylow subgroup S_{p_i} of K will split G.

Proof. The idea of this proof is similar to the proof of Theorem 1. We have the decomposition of K already, as $K \cong S_{p_1} \times S_{p_2} \times \cdots \times S_{p_k}$.

We claim S_{p_i} is normal in G. By the definition of G, $K \lhd G$. As before, there exists a normal subgroup of both G and K isomorphic to S_{p_i} (the one from the direct factor expansion). Consider the elements of S_{p_i} in K. Under conjugation in G, such elements will still be in K since K is normal by construction, and they will also be in S_{p_i} since there is a unique Sylow p_i-subgroup of K. Therefore our claim that $S_{p_i} \lhd G$ is true.

Since $S_{p_i} \lhd G$ and S_{p_i} has a complement T in G, $G \cong S_{p_i} \rtimes (T \rtimes H)$. $\square$

We note that it is trivial to extend the theorem to direct products of Sylow subgroups; that is, a direct product of some Sylow subgroups of any nilpotent group K will split a group $G \cong K \rtimes H$ for any group H.

4 Conclusion

We have shown that given a partial decomposition of a group into a semidirect product with a nilpotent group as the normal factor, we can convolve across normal subgroups of the nilpotent group to generate nontrivial converses to the splitting lemma (converses which may not be guaranteed by the Schur-Zassenhaus Theorem).

It would be interesting to investigate how this idea of convolution could be extended further, perhaps beyond convolving across direct factors, which is all that we did in this paper, to convolving across factors of a semidirect product. It seems likely that there is a more general result, although it is not obvious (at least to the author) what that might be. However, it should probably not be true in general that we may convolve across any partially decomposed group, since normality is not transitive, which is the primary issue.

References

[1] Steven Roman. *Fundamentals of Group Theory.* Birkhäuser, 2012.

[2] Joseph J. Rotman. *An Introduction to the Theory of Groups.* Springer, fourth edition, 1995.

[3] Joseph J. Rotman. *An Introduction to Homological Algebra.* Springer, second edition, 2009.

[4] Joseph J. Rotman. *Advanced Modern Algebra*, volume 114 of *Graduate Studies in Mathematics.* American Mathematical Society, second edition, 2010.