THE $\rtimes$

YVAN PATRICK QUINN

Abstract. This paper is intended to introduce the semidirect product as a tool for constructing a greater variety of new groups than is possible with the direct product, which is shown to be essentially the trivial semidirect product.

1. Introduction: The $\times$

As the most basic way to construct a group from subgroups, the direct product is a straightforward method of producing a group G for which the starting subgroups H, K are normal. Mechanically, the products of two elements can be found as follows:

$$g_1, g_2 \in G : g_1 g_2 = (h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2)$$

If the commas are removed, an element $g = (h, k) = hk$, and the preceding product can still be carried out in the same way as long as h_2 and k_1 commute:

$$g_1 g_2 = (h_1 k_1)(h_2 k_2) = h_1(k_1 h_2)k_2 = h_1(h_2 k_1)k_2 = (h_1 h_2)(k_1 k_2)$$

This condition holds for all $h_2 \in H, k_1 \in K$, so

$$h_2 k_1 = k_1 h_2 = k_1 h_2 k_1^{-1} k_1 = (k_1 \cdot h_2) \Rightarrow k_1 \cdot h_2 = h_2$$

where $\cdot$ denotes the conjugation action, so $K \subseteq C_G(H)$. Therefore,

$$\forall g \in G, gHg^{-1} = (hk)H(k^{-1}h^{-1}) = h(kHk^{-1})h^{-1} = h \cdot (k \cdot H) = h \cdot H = H$$

This means $H \trianglelefteq G$, and by a symmetric argument, $H \trianglelefteq G$. We denote this group $G = H \times K$, and to ensure the distinctness of every $(h, k) \in G$, we require H, K have trivial intersection.[1] This concludes our discussion of the direct product, but definitely begs question: what if K were to act on H in a nontrivial way? While the direct product of N groups is unique (up to permutation), maybe removing this restriction would allow us to build more than one group from the same collection of smaller groups! This brings us to

Definition 1.1. The semidirect product G, denoted $H \rtimes_\varphi K$, is obtained by specifying a homomorphism

$$\varphi : K \to Aut(H)$$

which is the action of K on H by conjugation, so that $\forall k \in K : k \cdot H = \varphi(k)(H) = H$. From this, any $g \in G$ can be uniquely written as $g = hk$ for some $h \in H, k \in K$.

Theorem 1.2. *G is a group*

1991 *Mathematics Subject Classification.* Class: Groups and Rings. Topic: Semidirect Products.

[1]Otherwise, $\forall i \neq j \in H \cap K, ij = ji$, so $(i, j) = (j, i)$. Furthermore $(h, k)(i, j) = (hi, kj) = (h_i, k_j)$ but also $(h, k)(j, i) = (h_j, k_i) = (h_i, k_j)$, even though $h_i \neq h_j$ and $k_i \neq k_j$ (since $i = h^{-1}h_i$ and $j = h^{-1}h_j$), so there is more than one way to write each element of G in terms of elements of H, K.

Proof. $\forall g \in G : gg^{-1} = (hk)(hk)^{-1} = (hk)(h^{-1}k^{-1}) = h1_K h^{-1} = h1_H h^{-1} = 1$ where $g^{-1} \in G$ since $\exists h' \in H : h^{-1} = \varphi(k^{-1})(h') \Rightarrow g^{-1} = (k^{-1}h'(k^{-1})^{-1})k^{-1} = k^{-1}h' \in G$

$$g_1 g_2 = (h_1 k_1)(h_2 k_2) = h_1 k_1 h_2 (k_1^{-1} k_1) k_2 = h_1 (k_1 \cdot h_2) k_1 k_2 = h_1 h_2' k' = h' k' \in G$$

$$(g_1 g_2) g_3 = (h_1 k_1 h_2 k_2) h_3 k_3 = h_1 k_1 (h_2 k_2 h_3 k_3) = g_1 (g_2 g_3)$$

□

Corollary 1.3. *This ends up making (i) $H \trianglelefteq G$ (ii) $H \cap K = \{1\}$ (iii) $|G| = |H||K|$*

Proof.

$$(i) \forall g \in G : g \cdot H = (hk) \cdot H = h \cdot (k \cdot H) = h \cdot H = H$$

(*ii*) Let $i \neq j \in H \cap K$. Since $H \cap K$ is a group, it contains an element u for which $ij = (i \cdot j)i = ui$. This leads to duplicate elements, since $ijhk = i(j \cdot h)jk = (ih_j)(jk)$ but $ijhk = uihk = (uh_i)(ik)$. These identical elements differ in H, K components because $ik \neq jk$ and since $uh_i = uihi^{-1} = jhi^{-1} = ji^{-1} \neq ih_j$ (since the latter $\notin H \cap K$).[2]

(*iii*) Since the intersection is trivial, all $|K|$ cosets kH are distinct, and of size $|H|$. □

2. Motivation: Recomposing D_{2n}

Consider the dihedral group for odd n, and the abelian group generated by $\langle r \rangle$, which is isomorphic to Z_n. This group is normal in D_{2n}, which can be seen by conjugating r^i by arbitrary elements:

$$r^j r^i r^{-j} = r^i \in \langle r \rangle$$

$$s r^j r^i r^{-j} s = s r^i s = r^{-i} \in \langle r \rangle$$

By defining a homomorphism $\varphi : D_{2n} \to \langle s \rangle$ as $\varphi(x) = x^n$, it might be thought that since $Im(\varphi) \cong Z_2$, we could recover the original group D_{2n} from Z_n and Z_2. This would be impossible with the direct product, because $\langle s \rangle \ntrianglelefteq D_{2n}$, but since $Z_n \trianglelefteq D_{2n}$, the semidirect product may be exactly what we need to produce the correct group! Let $\psi : Z_2 \to Aut(Z_n)$ map x to the automorphism of the inversion on Z_n, so that

$$\forall y \in Z_n : \psi(x)(y) = x \cdot y = y^{-1}$$

Proposition 2.1. $Z_n \rtimes_\psi Z_2 \cong D_{2n}$

Proof. Identifying x with s and y with r, it should be apparent that since all elements of $Z_n \rtimes_\psi Z_2$ can be written as yx, and since the new rule defined by the homomorphism ψ acts in the same way as the the rule in D_{2n},

$$s \cdot r^i = s r^i s^{-1} = (r^i)^{-1} = r^{-i} \Rightarrow s r^i = r^{-i} s$$

and since the s and r specific rules still apply within Z_2 and Z_n, the newly composed group is isomorphic to D_{2n}. □

Remark 2.2. It is worth noting that even though both Z_2 and Z_n are abelian, their semidirect product is not.

Lemma 2.3. *For any H, K which are both abelian, the direct product $G = H \times K$ must also be abelian.*

[2] See footnote 1.

Proof. We showed in the introduction that the elements of H and K must commute, so $\forall g_1, g_2 \in G : g_1g_2 = (h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2 = h_1(h_2k_1)k_2 = (h_1h_2)(k_1k_2)$

$$= (h_2h_1)(k_2k_1) = h_2(h_1k_2)k_1 = (h_2k_2)(h_1k_1) = g_2g_1$$

□

3. Implications: Classifying all groups of certain orders

Seeing as direct products allowed for the classification of all finitely generated abelian groups (see the namesake Fundamental Theorem for how to do this), it might be hoped that the semidirect product allows for a similar classification of groups with some more general property.

Theorem 3.1. *Suppose $H, K \leq G$ satisfy (i) $H \trianglelefteq G$, and (ii) $H \cap K = \{1\}$ Then $HK \cong H \rtimes K$.*

Proof. Since any element of $H \rtimes K$ can be written as hk for some $h \in H, k \in K$ (proven in Theorem 1.2), the elements of $H \rtimes K$ are exactly those of HK. So, define a bijection $\phi : H \rtimes K \to HK$ as $\phi((h, k)) = hk$. This is a homomorphism because

$$\phi((h_1, k_1)(h_2, k_2)) = \phi((h_1(k_1 \cdot h_2), k_1k_2)) = [h_1(k_1 \cdot h_2)][k_1k_2] = [h_1(k_1h_2k_1^{-1})][k_1k_2]$$
$$= h_1k_1h_2k_1^{-1}k_1k_2 = (h_1k_1)[h_2(k_1^{-1}k_1)k_2] = (h_1k_1)(h_2k_2) = \phi((h_1, k_1))\phi((h_2, k_2))$$

□

If we can show that any group of order n must have proper subgroups H, K (for which $|H||K| = n$) satisfying Theorem 3.1, then any $G = HK \cong H \rtimes_\varphi K$, for some choice of H, K and φ. Thus, all groups of order n can be explicitly constructed.

Remark 3.2. While this condition does not hold for arbitrary n, it is nonetheless possible to classify groups of some very general orders.

Example 3.3. There are either exactly one or two groups of order pq, where p, q are distinct primes. If $p \mid q - 1$, there is a unique non-abelian group of order pq.

Proof. (Dummit 181-2) Without loss of generality, assume $p < q$, and let G be some group of order pq. By Sylow's Theorems, for $P \in Syl_p(G), Q \in Syl_q(G) : G = QP \cong Q \rtimes P$.[3] Since q prime, Q is cyclic, and $Aut(Q)$ is a cyclic group of order $q - 1$ (Any nonidentity element can generate G, so can be mapped to the generating element.)

Case 1: If $p \nmid q - 1$, there is no subgroup order p of $Aut(G)$, and so the only homomorphism $\varphi : P \to Aut(Q)$ is trivial (i.e. $\mathrm{Im}(\varphi) = \{1\}$). Therefore, since $G = Q \rtimes_\varphi P$, for any $p \in P, q \in Q, p \cdot q = \phi(p)(q) = p$. Thus, the only semidirect product produces the direct product $Q \times P$. Since P, Q are cyclic, G must be also be cyclic, and is thus $\cong Z_{pq}$.

Case 2: If $p \mid q - 1$, let y be any nonidentity $\in P$, (which must generate P because it is a cyclic group of prime order). Let $\varphi_1 : P \to Aut(Q)$ be a homomorphism that takes $\varphi_1(y) = \gamma$, where γ generates the unique order p subgroup of $Aut(G)$. Since p is prime, this subgroup can be generated by any nonzero element, so there is such a homomorphism for each of the $p-1$ powers of γ in P. That is, $\varphi_i(y) = \gamma^i, 0 \leq i \leq p-1$, where φ_0 is trivial, so makes $G = Q \rtimes_{\varphi_0} P = Q \times P$ as discussed in *Case 1.* Naïvely, every φ_i gives a different semidirect product, making

[3]For a proof of this, see the first example of (Dummit 143).

p distinct groups $G_i = Q \rtimes_{\varphi_i} P$ of order pq.[4] But since p is prime, $\forall i \geq 1$, Euclid's Algorithm can be used to find a $b < p$ such that $ib = 1 \pmod{p}$. Now, let $x = y^b \in P$, which makes $\varphi_i(x) = (\varphi_i(y))^b = (\gamma^i)^b = \gamma^{ib} = \gamma$. Since any element of P can generate P, there is a bijective automorphism $\phi : P \to P$ for which $\phi(y) = y^b = x$, so $\varphi_i \circ \phi(y) = \varphi_i(x) = \gamma = \varphi_1(y)$. Since ϕ is a bijection, $\varphi_i \cong \varphi_1$, which means $G_i \cong G_1, \forall i \geq 1$. Since φ_1 is nontrivial, $G_1 \ncong Z_q \times Z_p$, so by the Fundamental Theorem of Finitely Generated Abelian Groups, G_1 (which is of finite order pq) is non-abelian. Therefore, in the case where $p \mid q - 1$, there are exactly two groups of order pq (one cyclic $\cong Z_{pq} \cong Z_q \times Z_p$, and one non-abelian $\cong Z_q \rtimes_\varphi Z_p$, for $\mathrm{Im}(\varphi) \neq \{1\}$).

□

Generally, the procedure for finding classifying the groups of a certain order n consists in first showing that any group G of this order must have proper subgroups H, K of trivial intersection such that $H \trianglerighteq G$ and $G = HK$. Then, all possible groups H, K must be found, up to isomorphism. (Most likely, you will have the orders of the groups H, K, and need to find all possible groups of the given orders.) Next, for every pair of groups H, K, all homomorphisms $\varphi : K \to Aut(H)$ must be found. Finally, every such unique homomorphism gives a distinct group $G = H \rtimes_\varphi K$ of order n.

4. Conclusion

In the mission of classifying groups, the ability to construct larger groups from known groups is crucial. Although useful, the direct product is inherently limiting because it is only able to produce a single group from a choice of two smaller groups. While there are only single groups of order 2 and 3, (which cannot be broken down into subgroups, and thus, cannot even be constructed from a direct product), already there are two nonisomorphic groups of order 4 (Z_4 and $V_4 = Z_2 \times Z_2$), only one of which can be found using a direct product. This is especially disconcerting considering the fact that Z_4 has the same proper subgroups as V_4, so it seems logical that another procedure should be able to take these subgroups and give Z_4. This paper was an attempt to provide the necessary exposition for and proper development of the semidirect product as a method of constructing a greater variety of groups from smaller known groups, and went so far as to outline a general procedure for finding all possible groups of a given order, as long as the order is tractable. In the process, the direct product was shown to be the special case of a semidirect product in which the choice of homomorphism defining the action of one group on the other is trivial.

References

[1] Péter Csikvári: *Sample paper*, `math.mit.edu/~csikvari/sample_paper.tex/`

[2] David S. Dummit, Richard M. Foote: *Abstract Algebra, 3rd Ed.*, John Wiley and Sons, Inc. (2004) 175-184.

Stanford University, Department of Mathematics, Stanford, CA 94305
Email address: `yvan@stanford.edu`

[4] See Corollary 1.3