AN INTRODUCTION TO WREATH PRODUCTS

MATTHEW LUDWIG

Abstract. In this paper we will first provide an introduction to automorphism groups and inner and outer semidirect products. Then we will use these ideas to present the lamp-lighter group and introduce the restricted wreath product.

1. Introduction

Just as direct products allow us to build larger groups from smaller groups, wreath products allow us to construct larger groups with new properties from smaller groups. Since wreath products are based on the semidirect products, we will begin with an introduction to the different types of semidirect products which rely on automorphism groups. Consider the following definition of an automorphism.

Definition 1.1. An *automorphism* of a group G is an isomorphism $\phi : G \to G$. [2]

Since an isomorphism from G to G is also a group homomorphism, any automorphism from G to G must fix the identity and send all of the generators to generators while preserving the group homomorphism property. [5] Consider the following automorphisms of the cyclic group of order 5.

Example 1.2. Consider the cyclic group $\mathbb{Z}_5$ with elements $\{0, 1, 2, 3, 4\}$ with addition performed mod 5. Any automorphism must send the identity 0 to itself and generators to other generators. Since $1, 2, 3$ and 4 are all coprime with 5, they all generate $\mathbb{Z}_5$. Consider the following automorphisms ϕ given by $\phi(0) = 0$, $\phi(1) = 2$, $\phi(2) = 4$, $\phi(3) = 1$, $\phi(4) = 3$ and σ given by $\sigma(0) = 0$, $\sigma(1) = 4$, $\sigma(2) = 3$, $\sigma(3) = 2$ and $\sigma(4) = 1$. Notice that the composition $\sigma \circ \phi$ is also an automorphism as it is a group isomorphism from $\mathbb{Z}_5$ to $\mathbb{Z}_5$. This observation leads to the following definition.

Definition 1.3. The *automorphism group* of a group G, denoted by $Aut(G)$, is the set of all automorphisms of G under the operation of composition. [2]

Example 1.4. We will now find the automorphism group of $\mathbb{Z}_5$. To do this we will first find all of the automorphisms of $\mathbb{Z}_5$. We know that an automorphism

Date: 2021-04-04.

of $\mathbb{Z}_5$ is determined by where it sends the generators of $\mathbb{Z}_5$ and that an automorphism must respect the group homomorphism property that $\phi(ab) = \phi(a)\phi(b)$. Since $1, 2, 3$ and 4 are all generators we can send one of them to another and then use the group homomorphism property to determine where the other elements get mapped to. For instance, if we choose $\psi(4) = 2$, then $\psi(3) = \psi(4+4) = \psi(4) + \psi(4) = 2 + 2 = 4$ and $\psi(2) = \psi(4+4+4) = \psi(4) + \psi(4) + \psi(4) = 2 + 2 + 2 = 1$. Observe that in the automorphisms from example 1.2 that we had $\phi(4) = 3$ and $\sigma(4) = 1$. Since the identity automorphism maps 4 to itself or $e(4) = 4$, we have found all possible options of where to send the generator 4 and thus all of the other elements of the group while preserving the group homomorphism property. Therefore $Aut(\mathbb{Z}_5) = \{e, \phi, \psi, \sigma\}$ has four elements. Now recall that there are two groups of order 4; the Klein-four group and the cyclic group of order 4. [2] Since we have that $\phi = \phi$, $\phi^2 = \sigma$, $\phi^3 = \psi$ and $\phi^4 = e$ which means that ϕ generates $Aut(\mathbb{Z}_5)$, then $Aut(\mathbb{Z}_5)$ is cyclic so then $Aut(\mathbb{Z}_5) \cong \mathbb{Z}_4$.

One important application of the automorphism group for an algebraic structure such as a group, set, ring or vector space is that group actions on that structure can be defined by a homomorphism between the group G and the automorphism group of the structure. [3]. Prototypical examples of group actions include the symmetric group S_n acting on the set of n elements and the general linear group acting on a vector space. Consider the following example of a group acting on another group.

Example 1.5. Consider the following example of a group action of $\mathbb{Z}_2$ on $\mathbb{Z}_5$. We found that $Aut(\mathbb{Z}_5) \cong \mathbb{Z}_4$. Therefore a group action of $\mathbb{Z}_2$ on $\mathbb{Z}_5$ is defined by a homomorphism $\alpha : \mathbb{Z}_2 \to Aut(\mathbb{Z}_5) \cong \mathbb{Z}_4$. Consider the homomorphism given by $\alpha(0) = 0$ and $\alpha(1) = 2$. Since 2 is the only element of order 2 in $\mathbb{Z}_4$, then it corresponds to the order 2 element σ in $Aut(\mathbb{Z}_5)$. Therefore the element 1 in $\mathbb{Z}_2$ acts on the elements of $\mathbb{Z}_5$ by mapping them according to σ and 0 in $\mathbb{Z}_2$ acts on the elements of $\mathbb{Z}_5$ according to the automorphism e, that is by not permuting them.

2. Semidirect Products

2.1. **Outer Semi-Direct Products.** Now that we have introduced automorphism groups and how group actions can be thought of as homomorphisms between one group and the automorphism group of an algebraic structure, we can introduce the outer semidirect product of two groups. Consider the following definition.

Definition 2.1. Let K and H be two groups with an action of K on H, i.e. a homomorphism $\alpha : K \to Aut(H)$. Then the outer semidirect product $K \ltimes_\alpha H$ is a group whose elements are $\{(k, h) | k \in K, h \in H\}$ and whose multiplication

is given by $(k_1, h_1)(k_2, h_2) = (k_1k_2, h_1 \cdot \alpha(k_1)(h_2))$ where $\alpha(k_1)(h_2)$ is the result of applying the automorphism $\alpha(k_1)$ to the element h_2. [1]

Example 2.2. Consider the groups $\mathbb{Z}_2$ and $\mathbb{Z}_5$ and their semidirect product $\mathbb{Z}_2 \ltimes_\alpha \mathbb{Z}_5$. First we know that elements in the group are $\{(0,0), (0,1), (0,2), (0,3), (0,4), (0,5), (1,0), (1,1), (1,2), (1,3), (1,4), (1,5))\}$. Now the composition of elements depends on a homomorphism $\alpha : \mathbb{Z}_2 \to Aut(\mathbb{Z}_5) \cong \mathbb{Z}_4$. Observe that if $\alpha(0) = e$, $\alpha(1) = e$, then the composition formula from definition 1.6 becomes (k_1k_2, h_1h_2) which is the composition for a direct product, which tells us that $\mathbb{Z}_2 \ltimes_\alpha \mathbb{Z}_5 = \mathbb{Z}_2 \times \mathbb{Z}_5$. However, we could also have the homomorphism given in example 1.5 which was given by $\alpha(0) = e$ and $\alpha(1) = \sigma$ where σ is the automorphism of order 2 in $Aut(\mathbb{Z}_5)$ from example 1.2. This results in an entirely different definition of composition. Consider the following example of the composition of elements resulting from the two choices of homomorphisms:

$$(1,2)(1,1) = (1+1, 2+\alpha(1)(1)) = (0, 2+e(1)) = (0, 2+1) = (0,3)$$

$$(1,2)(1,1) = (1+1, 2+\alpha(1)(1)) = (0, 2+\sigma(1)) = (0, 2+4) = (0,1)$$

Now we can rewrite the elements of $\mathbb{Z}_5$ as e_5, r, r^2, r^3 and r^4 and the elements of $\mathbb{Z}_2$ as e_2 and f and get the following:

$$(f, r^2)(f, r) = (f \cdot f, r^2 \cdot \alpha(f)(r)) = (f \cdot f, r^2 \cdot e(r)) = (e_2, r^2 \cdot r) = (e_2, r^3)$$

$$(f, r^2)(f, r) = (f \cdot f, r^2 \cdot \alpha(f)(r)) = (f \cdot f, r^2 \cdot \sigma(r)) = (e_2, r^2 \cdot r^4) = (e_2, r)$$

The first composition is exactly the same as the composition in the direct product of $\mathbb{Z}_2 \times \mathbb{Z}_5$. Now let's try to account for what is going on in the second composition. Applying the map $\phi(f^a, r^b) = r^b f^a$ to each element in the second composition and to the resulting element gives the following:

$$(f, r^2)(f, r) = r^2 frf \stackrel{?}{=} r = (e_2, r)$$

Notice that the second equality only holds when $rf = fr^{-1}$ and that this is the final relation in the relators of the group presentation of D_5 as in rewriting the elements we already know that $r^5 = f^2 = e$. Therefore if we can show that ϕ is a bijective homomorphism or that the above equality holds then the compositions of elements in $\mathbb{Z}_2 \ltimes \mathbb{Z}_5$ would behave exactly like the composition of elements the dihedral group D_5. This observation leads us to the following theorem.

Theorem 2.3. *(Exercise 5)* $\mathbb{Z}_2 \ltimes_\alpha \mathbb{Z}_n \cong D_n$ *via the map* $\phi : \mathbb{Z}_2 \ltimes_\alpha \mathbb{Z}_n \to D_n$ *given by* $\phi(f^a, r^b) = r^b f^a$ *where* $\alpha : \mathbb{Z}^2 \to Aut(\mathbb{Z}_n)$ *by* $\alpha(e) = e$ *and* $\alpha(f) = (r \to r^{-1})$*[1]*

Proof. First we show that this map ϕ is a homomorphism. $\phi((f^a, r^b)(f^c, r^d)) = \phi(f^{a+c}, r^b \cdot \alpha(f^a)(r^d)) = r^{b-d} f^{a+c} = r^b r^{-d} f^a f^c = r^b f^a r^d f^c = \phi(f^a, r^b)\phi(f^c, r^d)$. In the fourth equality we used the fact that $rf = fr^{-1}$ in a dihedral group.

In the second equality, we assume that $f^a = f$ which means that $\alpha(f) = (r \to r^{-1})$. Now if we assume that $f^a = e$, then $\alpha(e) = e$ and then $\phi((f^a, r^b)(f^c, r^d)) = \phi(f^{a+c}, r^b \cdot \alpha(e)(r^d)) = \phi(f^{a+c}, r^{b+d}) = r^{b+d}f^{a+c} = r^b r^d f^a f^c = r^b f^a r^d f^c = \phi(f^a, r^b)\phi(f^c, r^d)$. The penultimate equality follows from the fact that $f^a = e$. Therefore we have shown that ϕ is a homomorphism. Now we show that ϕ is one-to-one. Suppose $\phi((f^a, r^b)) = \phi((f^c, r^d))$, then $r^b f^a = r^d f^c$. This is only true when $b \equiv d \mod 2$ and when $a \equiv c \mod n$ which implies that $(f^a, r^b) = (f^c, r^d)$ in $\mathbb{Z}_2 \ltimes_\alpha \mathbb{Z}_n$. Now ϕ is onto as every element in D_n can be written as some combination of the generators r and f, so then there exists some element (f^a, r^b) for some a and b. Since ϕ is a bijective homomorphism it is a group isomorphism.

□

2.2. **Inner Semidirect Products.** Outer semidirect product allowed us to construct a new group, $N \ltimes_\alpha H$, from two groups H and K by defining an action of K on H which we showed was equivalent to providing a homomorphism $\alpha : K \to Aut(H)$. The previous example illustrated how any dihedral group can be decomposed into the semidirect product of two cyclic groups. A natural question to ask is if any group G can be written as the semidirect product of two groups. This leads us to the definition of the inner semidirect product.

Proposition 2.4. *Let G be a group with H and K subgroups such that*

(1) $H \trianglelefteq G$
(2) $H \cap K = \{e\}$
(3) $HK = G$

Then $G \cong K \ltimes_\alpha H$, where $\alpha : H \to Aut(K)$ is given by $\alpha(h)(k) = hkh^{-1}$.[1]

Proof. Consider the map $\phi : K \ltimes_\alpha H \to G$ via $\phi(k, h) \to hk$.[1] We would like to show that this is a group isomorphism or a bijective group homomorphism. To first show that ϕ is a homomorphism we must show that $\phi((k_1, h_1)(k_2, h_2)) = \phi((k_1, h_1))\phi((k_2, h_2))$. Notice that $\phi((k_1, h_1)(k_2, h_2)) = \phi((k_1k_2, h_1\alpha(k_1)(h_2))) = \phi((k_1k_2, h_1k_1h_2k_1^{-1})) = h_1k_1h_2k_1^{-1}k_1k_2 = h_1k_1h_2k_2 = \phi(k_1, h_1)\phi(k_2, h_2)$. Now to show that ϕ is injective we must show that if $\phi((k_1, h_1)) = \phi((k_2, h_2))$, then $(k_1, h_1) = (k_2, h_2)$. If $\phi((k_1, h_1)) = \phi((k_2, h_2))$, then $h_1k_1 = h_2k_2$. Now we can multiply by h_1^{-1} and k_2^{-1} to get $k_1k_2^{-1} = h_1^{-1}h_2$. Since H and K are closed under composition of elements, then we know that $k_1k_2^{-1} \in K$ and $h_1^{-1}h_2 \in H$. Since these elements are equal, then we know that they must be in both H and K or in $H \cap K$. Now by assumption (2) we know that this element $k_1k_2^{-1} = h_1^{-1}h_2 = e$. Therefore $k_1k_2^{-1} = e$ and $h_1h_2^{-1} = e$ which means that $k_1 = k_2$ and $h_1 = h_2$. Therefore we have that $(k_1, h_1) = (k_2, h_2)$ which means that ϕ is injective. Now in order for ϕ to be surjective, every element in G must have at least one element in $K \ltimes_\alpha H$ that the map ϕ sends to it. This means every element in G must be able to

be written in the form hk for some $h \in H$ and $k \in K$. Now observe that this is satisfied as assumption (3) tells us that $HK = G$ and we know that $H \cap K = \{e\}$. Therefore ϕ is a group isomorphism. □

Example 2.5. Consider the group of symmetries of the tetrahedron or the alternating group $A_4 = \{e, (12)(34), (13)(24), (14)(23), (123), (132), (134), (143), (124), (142), (234), (243)\}$ which is the subgroup of even permutations of S_4 of all the permutations that can be obtained from a product of an even number of transpositions. Recall that $H = \{e, (12)(34), (13)(24), (14)(23)\}$ is the Klein-4 group and that it is a normal subgroup of A_4.[4] Now we want to find a subgroup K that satisfies the properties listed above. Consider the subgroup $K = \{e, (123)(132)\}$. It can be verified that $HK = A_4$ as the composition of elements in H with elements in K results in all of the permutations in A_4 and that $H \cap K = \{e\}$. Therefore $A_4 = K \ltimes_\alpha H$ where $\alpha : H \to Aut(K)$ is given by $\alpha(h)(k) = hkh^{-1}$.

3. Wreath Products

Now that we have shown that we can use outer semidirect products to construct new larger groups from two smaller groups and inner semidirect products to break down a group into the semidirect products of two smaller groups we will now introduce wreath products which use these products to create new larger groups. Consider the following example.

Example 3.1. There is an infinitely long street on which the real line lies and at every integer there is a lamppost that can be switched on or off. There is also a group that acts on this space in the following way. An element of the group is a set of instructions for a lamplighter (who is starting at the origin) to turn on or off a set of lamps and then walk to some integer or endpoint. We define composition of group elements a and b by telling the lamplighter to start at 0, do the instruction of a and then start to do the instructions of b starting from the endpoint a specified. We can formalize this by saying the instructions are given by the pair $(m, p(x))$ where $p(x) \in \mathbb{Z}_2[x, \frac{1}{x}]$ is the list of which lamps to switch and where $m \in \mathbb{Z}$ is the endpoint. For instance, the element $(34, \frac{1}{x^{52}} + \frac{1}{x^3} + x^7 + x^9)$ tells the lamplighter to first flip on the lamps at the integers $-52, -3, 7$ and 9 and then go to the integer 34. The composition of elements is defined by $(m_1, p_1(x))(m_2, p_2(x)) = (m_1 + m_2, p_1(x) + x^{m_1} p_2(x))$. Observe that this looks like the formula for composition of a semidirect product given in definition 2.1. Now we know that $m \in K = \mathbb{Z}$ and that $p(x) \in H = \bigoplus_{i \in \mathbb{Z}} (\mathbb{Z}_2) = \{\text{polynomials in } \mathbb{Z}_2[x\frac{1}{x}], \text{under addition}\}$. This is the direct sum of $\mathbb{Z}_2$ indexed by $\mathbb{Z}$ where elements are infinitely long tuples such as $(...0, 0, 1, 0, 1, 0...)$. In order to define a semidirect product, we need define a homomorphism $\alpha : K \to Aut(H)$. Consider the homomorphism α given by $\alpha(m)(p(x)) = x^m p(x)$ and notice that $\alpha(m)(p(x))$ is an automorphism of H as it is an isomorphism from H to H

as $\alpha(m)(p(x)) = x^m p(x)$ takes every polynomial in H to another polynomial in H with power m higher. Therefore by definition 2.1 we can write $G = \mathbb{Z} \ltimes_\alpha H$. [1]

Theorem 3.2. *(Exercise 9) With subgroups of G, $K = \{(m, p(x))|p(x) = 0\}$ and $H = \{(m, p(x))|m = 0\}$, H is a normal subgroup of G, and that for $m \in K$ and $p(x) \in H$, $\alpha(m)(p(x)) = (m, 0)(0, p(x))(m, 0)^{-1}$. [1]*

Proof. In order to show that H is a normal subgroup of G, we must show that for all $h \in H$ and $g \in G$ we have that $ghg^{-1} \in H$. Therefore consider the product $(m_1, p_1(x))(0, p_h(x))(-m_1, \frac{1}{p(x)})$. Now we know that $(m_1, p_1(x))(0, p_h(x))$ $(-m_1, \frac{1}{p(x)}) = (m_1, p_1(x))(-m_1, p_h(x) + x^0 \frac{1}{p_1(x)}) = (m_1, p_1(x))(-m_1, p_h(x) + \frac{1}{p_1(x)}) = (m_1 - m_1, p_1(x) \cdot x^{m_1} \cdot (p_h(x) + \frac{1}{p_1(x)})) = (0, p'(x)) \in H$. Observe that we have that H is a normal subgroup of G, $HK = G$ and $H \cap K = \{(0, 0)\}$. Now by proposition 2.4, $G = K \ltimes_\alpha H = \mathbb{Z} \ltimes_\alpha \bigoplus_{i \in \mathbb{Z}} (\mathbb{Z}_2)$ and that for $m \in K$ and $p(x) \in H$, $\alpha(m)(p(x)) = (m, 0)(0, p(x))(m, 0)^{-1}$. □

This semidirect produce is a little different from the previous ones that we have seen as we have infinitely many copies of $\mathbb{Z}_2$. Also, this seems a little redundant to write as the $\mathbb{Z}$ which keeps track of the endpoint location m for the lamplighter already appears in the index for the lampposts. [1] This leads us to the definition of a wreath product.

Definition 3.3. Let H and K be groups. Let A be the direct sum given by

$$A = \bigoplus_{w \in K} H_w,$$

where each H_w is an identical copy of H, indexed by the elements of K. Then K acts on A via

$$k(a_w) = a_{k^{-1}w}$$

The restricted wreath product $H \wr K$ is the group $H \wr K = K \ltimes A$. [1]

Using this definition we can express the lamplighter group as $\mathbb{Z}_2 \wr \mathbb{Z}$ as we know that $K \ltimes_\alpha H = \mathbb{Z} \ltimes_\alpha \bigoplus_{i \in \mathbb{Z}} (\mathbb{Z}_2)$ where $A = \bigoplus_{i \in \mathbb{Z}} (\mathbb{Z}_2)$. [1]

4. Conclusion

Ultimately, wreath products provide a more succinct way of expressing the semidirect product of two groups. This change in notation is useful as wreath products arise in many applications and their succinct notation for representing the semidirect of two groups is convenient. Besides the lamplighter group, wreath products are used in the construction of the generalized symmetric group, the Rubik's cube group, the Sudoku symmetry group, the musical group of uniform triad transformations and in many other applications.

References

[1] Vivian Kuperberg. *Wreath Products*. http://web.stanford.edu/ viviank/wreath.pdf.
[2] Joseph J. Rotman. "An introduction to the Theory of Groups". In: 1995.
[3] Todd Rowland. *Group Action*. https://mathworld.wolfram.com/GroupAction.html.
[4] Eric Weisstein. *Alternating Group*. https://mathworld.wolfram.com/AlternatingGroup.html.
[5] Ada Zhang. *The Framework of Music Theory as Represented with Groups*. 2009.

5. Reference Notes

- The structure of this paper is based on the structure of [1]
- Example 2.2 is loosely based on the example on pg. 8 in [5]
- Example 3.1 is based on the example on pg. 2 in [1]