

Frank Moore  
 Algebra 901 Notes  
 Professor: Tom Marley

**Semidirect Products:**

**Definition:** Let  $H, K$  be groups and let  $\phi : K \rightarrow \text{Aut}(H)$  be a group homomorphism. Define the (external) **semidirect product** of  $H$  and  $K$  (wrt  $\phi$ ) to be  $H \rtimes_{\phi} K = \{(h, k) | h \in H, k \in K\}$  with the following operation:

$$(h_1, k_1)(h_2, k_2) := (h_1\phi(k_1)(h_2), k_1k_2)$$

**Claim:** This set under the operation listed above forms a group.

**Proof:**

**Closed:** The operation is clearly closed.

**Associativity:** Exercise.

**Identity:**  $(1, 1)(h, k) = (1\phi(1)(h), k)$  and because homomorphisms take identity to identity (the identity map), we get  $(1(h), k) = (h, k)$ . For the other side, we see  $(h, k)(1, 1) = (h\phi(k)(1), k) = (h \cdot 1, k) = (h, k)$  since  $\phi(k)(1) = 1$  because automorphisms take identity to identity.

**Inverse of  $(h, k)$ :** Consider  $(h, k)^{-1} = (\phi(k^{-1})(h^{-1}), k^{-1})$ . Lets check if this works:

**Right side:**  $(h, k)(\phi(k^{-1})(h^{-1}), k^{-1}) = (h\phi(k)[\phi(k^{-1})(h^{-1})], 1)$  by definition of the operation, and then we have  $(h\phi(kk^{-1})(h^{-1}), 1)$  because  $\phi$  was a homomorphism, and this gives  $(h \cdot h^{-1}, 1) = (1, 1)$  because  $\phi(kk^{-1}) = \text{identity on } H$ .

**Left side:**  $(\phi(k^{-1})(h^{-1}), k^{-1})(h, k) = (\phi(k^{-1})(h^{-1})\phi(k^{-1})(h), 1)$  by definition, which gives  $(\phi(k^{-1})(h^{-1}h), 1)$  because  $\phi(k^{-1})$  is an automorphism, which gives  $\phi(k^{-1})(1), 1) = (1, 1)$ .

**Remark:** Let  $G = H \rtimes_{\phi} K$ . Then the following hold:

- Let  $H' = \{(h, 1) | h \in H\}$  and  $K' = \{(1, k) | k \in K\}$ . Then  $H'$  and  $K'$  are subgroups of  $G$ , and  $H' \cong H, K' \cong K$ . Also note that the funkiness of the semidirect product's operation goes away when either component is 1 in both of the elements in  $G$ .
- $G = H'K'$ .  $(h, k) = (h, 1)(1, k) \neq (1, k)(h, 1)$ .
- $H' \cap K' = \{1\}$ .
- $H' \triangleleft G$ .

**Proof:** Let  $(h', 1) \in H'$ , and  $(h, k) \in G$ . Then  $(h, k)(h', 1)(h, k)^{-1} = (h, k)(h', 1)(\phi(k^{-1})(h^{-1}), k^{-1}) = (*, 1) \in H'$ .

**Theorem:** Let  $G = H \rtimes_{\phi} K$ . Then the following conditions are equivalent:

- $\phi$  is the trivial map ( $\phi : k \mapsto 1_H \ \forall k \in K$ ).

- $G = H \times K$ .
- $K' \triangleleft G$ .

**Proof:** (1)  $\Rightarrow$  (2).  $(h_1, k_1)(h_2, k_2) = (h_1h_2, k_1k_2)$  if  $\phi$  is trivial, so  $G = H \times K$ . (2)  $\Rightarrow$  (3) is easy, since by definition, if you have  $G$  is a direct product of groups,  $K' \triangleleft G$ . (3)  $\Rightarrow$  (1): We know that  $H' \triangleleft G$  and  $H' \cap K' = \{1\}$ . As  $K'$  is normal, we have  $h'k' = k'h'$  for all  $h' \in H$  and  $k' \in K$ , so the conjugation is trivial.

**Corollary:**  $H \rtimes_{\phi} K$  is abelian  $\Leftrightarrow \phi$  is trivial and  $H, K$  are abelian.

**Example:** Find the smallest odd integer  $n$  such that  $\exists$  a non-abelian group of order  $n$ . Smallest  $n$  that would work is 21, because  $3|7-1$ . So, try  $C_7 \rtimes_{\phi} C_3$  where  $\phi : C_3 \rightarrow \text{Aut}(C_7)$  with  $\phi$  non-trivial. Note that  $\text{Aut}(C_7) \cong Z_7^* \cong Z_6$ . Say  $C_3 = \langle a \rangle$  and  $C_7 = \langle b \rangle$ . To define  $\phi$  with  $\phi$  being nontrivial, we want  $\phi(a)$  to be an automorphism of  $C_7$  with order dividing 3 that is not 1, so the order of  $\phi$  must be 3. So, we define  $\phi$  as follows:

$$\begin{aligned} \phi : C_3 &\rightarrow \text{Aut}(C_7) \\ a &\mapsto \left[ \begin{array}{c} \psi : C_7 \rightarrow C_7 \\ b \mapsto b^2 \end{array} \right] \end{aligned}$$

Note that the order of  $\phi(a) = |\psi| = 3$  in the group of automorphisms of  $C_7$ , so we have succeeded. So, we have  $C_7 \rtimes_{\phi} C_3$  is a nonabelian group of order 21.

**Note:** Consider  $C_p \rtimes_{\phi} C_q$ , where  $\phi : C_q \rightarrow \text{Aut}(C_p)$ . Then there exists a nontrivial  $\phi \Leftrightarrow q \nmid p-1$ .

**Theorem:** Let  $p < q$  be primes. Then  $\exists$  a non-abelian group of order  $pq \Leftrightarrow q \equiv 1 \pmod{p}$ .

**Proof:** “ $\Rightarrow$ ”: If  $q \not\equiv 1 \pmod{p}$ , then any group of order  $pq$  is cyclic by the lemma. “*Leftarrow*”: Suppose  $q \equiv 1 \pmod{p}$ . Then  $p|q-1 = |\text{Aut}(C_q)|$ . Therefore,  $\exists$  an automorphism  $\psi \in \text{Aut}(C_q)$  of order  $p$ . Define  $\phi : C_p = \langle a \rangle \rightarrow \text{Aut}(C_q)$  which sends  $a \mapsto \psi$ , which is a nontrivial homomorphism and therefore  $C_q \rtimes_{\phi} C_p$  is a nonabelian group of order  $pq$ .

**Presentations:** A way of describing groups and relations which define the group. If there are no relations, the group is said to be free. What follows is a loose description of presentations. A formal definition involves a look into free groups, and normal subgroups containing the relations.

**Notation:**

$$\langle x_1, \dots, x_n | w_1 = 1, \dots, w_n = 1 \rangle$$

where the  $w_i$  are ‘words’:  $w_i = x_{i_1}^{\alpha_1}$  where  $x_{i_j} \in \{x_1, \dots, x_n\}$ . For example:  $\langle x, y, z | x^2y = 1, xy^{-1}z^3 = 1 \rangle$  would be a presentation of some group.

**Examples:**

1.  $\langle x | \emptyset \rangle$  is a presentation of the integers.
2.  $\langle x | x^n = 1 \rangle = C_n$
3.  $\langle x, y | \emptyset \rangle$  is a presentation of the free group on 2 elements.
4.  $\langle x, y | xy = yx \rangle = \mathbb{Z} \times \mathbb{Z}$  which is the free abelian group on 2 elements.

5.  $\langle a, b | a^2 = 1, b^2 = 1, ab = ba \rangle$  is  $Z_2 \times Z_2$ , also known as the Klein 4-group.

6.  $D_8 = \langle x, y | x^4 = 1, y^2 = 1, yx = x^{-1}y \rangle$

7.  $Q_8 = \langle x, y | x^4 = 1, x^2 = y^2, yx = x^{-1}y \rangle$ .

**Example:** Create a presentation for the nonabelian group of order 21 we constructed last time: Let  $G = C_7 \rtimes C_3$ ,  $C_7 = \langle b \rangle$ ,  $C_3 = \langle a \rangle$ ,  $\phi$  is such that:

$$\begin{aligned} \phi : C_3 &\rightarrow \text{Aut}(C_7) \\ a &\mapsto \left[ \begin{array}{l} \psi : C_7 \rightarrow C_7 \\ b \mapsto b^2 \end{array} \right] \end{aligned}$$

Let  $x = (b, 1)$ ,  $y = (1, a)$ . Notice that  $o(x) = 7$  and  $o(y) = 3$ , and by the counting theorem, we have that  $G = \langle x \rangle \langle y \rangle$ . So,  $G = \langle x, y \rangle$ , and we investigate what relations define  $G$ . Obviously, we have  $x^7 = 1$  and  $y^3 = 1$ . Consider:

$$\begin{aligned} yx &= (1, a)(b, 1) \\ &= (1\phi(a)(b), a) \\ &= (b^2, a) \end{aligned}$$

So, we see that  $G = \langle x, y | x^7 = 1, y^3 = 1, yx = x^2y \rangle$ .

**Definition:** Let  $G$  be an abelian group. Define  $f : G \rightarrow G$  to send  $a \in G$  to  $a^{-1} \in G$ . Since  $f^2 = f \circ f = \text{Id}_G$ ,  $f$  is an automorphism of  $G$ .  $f$  is called the inversion map.  $o(f) = 2$  unless  $a^2 = 1 \forall a \in G$ .

**Example:** Let  $n > 2$  be an integer,  $C_2 = \langle a \rangle$  be a cyclic group of order 2, and  $C_n = \langle b \rangle$  be a cyclic group of order  $n$ . Define

$$\begin{aligned} \phi : C_2 &\rightarrow \text{Aut}(C_n) \\ a &\mapsto f \end{aligned}$$

where  $f$  is the inversion map defined above. So,  $\phi$  is non-trivial, and therefore  $C_n \rtimes_{\phi} C_2$  is a nonabelian group of order  $2n$  called the dihedral group. We now find a presentation for  $D_{2n}$ .

Let  $x = (b, 1)$ ,  $y = (1, a)$ . As before,  $G = \langle x, y \rangle = \{x^i y^j | 0 \leq i \leq n-1, 0 \leq j \leq 1\}$  since any power of  $x$  looks like  $(b^n, 1)$  and any power of  $y$  looks like  $(1, a)$ . We know that  $x^n = 1$ ,  $y^2 = 1$  and considering  $yx$ , we see that  $(1, a)(b, 1) = (b^{-1}, a) = x^{-1}y$ . So, a presentation for  $D_{2n}$  is as follows:

$$D_{2n} = \langle x, y | x^n = 1, y^2 = 1, yx = x^{-1}y \rangle$$