Semidirect Products
WiM: MATH 120

Kenneth G. Chang

November 21, 2017

1 Definition of Semidirect Product

Definition 1.1. Let H and K be any two subgroups and $\varphi : K \to \mathrm{Aut}(H)$ be a homomorphism. We say that G is the *semidirect product* of H and K if:

$$G = \{(h, k) \mid h \in H, k \in K\} \tag{1}$$

$$(h_1, k_1)(h_2, k_2) = (h_1\varphi(k_1)(h_2), k_1k_2) \tag{2}$$

The semidirect product of H and K is commonly denoted as $H \rtimes_\varphi K$ (or $H \rtimes K$ when φ is clear). Before proving that $H \rtimes K$ is a group, it is useful to show that $\varphi(k)(h)$ amounts to a group action of K on H.

Lemma 1.1. *$\varphi(k)(h)$, rewritten as $k \cdot h$, is a group action of K on H.*

Proof. The compatibility property holds since $k_1 \cdot (k_2 \cdot h) = \varphi(k_1)(\varphi(k_2)(h)) = \varphi(k_1) \circ \varphi(k_2)(h) = \varphi(k_1k_2)(h) = (k_1k_2) \cdot h$.

The identity property holds since $1 \cdot h = \varphi(1)(h) \overset{(1)}{=} id(h) = h$. $^{(1)}$ is since the identity automorphism is the identity in the field $\mathrm{Aut}(H)$. □

Thus, we can rewrite the multiplication relation above as $(h_1, k_1)(h_2, k_2) = (h_1\ k_1 \cdot h_2, k_1k_2)$.

Theorem 1.1. *For any H, K, and $\varphi : K \to \mathrm{Aut}(H)$, $H \rtimes_\varphi K$ is a group.*

Proof. The three properties are easy to verify based on the properties of group action. Note that since $k \cdot h$ is equivalent to a homomorphism $\varphi(k)(h)$, the usual homomorphism properties hold, namely that $(k \cdot h_1)(k \cdot h_2) = k \cdot (h_1h_2)$ and $k \cdot 1 = 1$.

(1) Associativity

$$\begin{aligned}
((h_1, k_1)(h_2, k_2))(h_3, k_3) &= (h_1\ k_1 \cdot h_2, k_1k_2)(h_3, k_3) \\
&= (h_1\ k_1 \cdot h_2\ (k_1k_2) \cdot h_3, k_1k_2k_3) \\
&= (h_1\ k_1 \cdot h_2\ k_1 \cdot (k_2 \cdot h_3), k_1k_2k_3) \\
&= (h_1\ k_1 \cdot (h_2\ k_2 \cdot h_3), k_1k_2k_3) \\
&= (h_1\, k_1)(h_2\ k_2 \cdot h_3, k_2k_3) \\
&= (h_1, k_1)((h_2, k_2)(h_3, k_3))
\end{aligned} \tag{3}$$

(2) Identity

$$(1,1)(h,k) = (1(1 \cdot h), (1)(k)) = (1(h), k) = (h,k) \tag{4}$$

$$(h,k)(1,1) = (h(k \cdot 1), k(1)) = (h(1), k) = (h,k) \tag{5}$$

From this, we can conclude that $(1,1)$ is the identity.
(3) Inverse

$$\begin{aligned}(h,k)(k^{-1} \cdot h^{-1}, k^{-1}) &= (h\ k \cdot (k^{-1} \cdot h^{-1}), kk^{-1}) = (h\ kk^{-1} \cdot h^{-1}, 1) \\ &= (h\ 1 \cdot h^{-1}, 1) = (hh^{-1}, 1) = (1,1)\end{aligned} \tag{6}$$

$$\begin{aligned}(k^{-1} \cdot h^{-1}, k^{-1})(h,k) &= (k^{-1} \cdot h^{-1}\ k \cdot h, k^{-1}k) \\ &= ((k \cdot h)^{-1}(k \cdot h), 1) = (1,1)\end{aligned} \tag{7}$$

From this, we conclude that $(h,k)^{-1} = (k^{-1} \cdot h^{-1}, k^{-1})$.
Since all three conditions are satisfied, the proof is complete.

□

2 Basic Properties of the Semidirect Product

Immediately, we can observe the following properties of the semidirect product $H \rtimes K$. Here we define $\widetilde{H} = \{(h,1) \mid h \in H\}$ and $\widetilde{K} = \{(1,k) \mid k \in K\}$ to be subsets of $H \rtimes K$.

Theorem 2.1. *$\widetilde{H}$ and $\widetilde{K}$ are subgroups of $H \rtimes K$, with $\widetilde{H} \cong H$ and $\widetilde{K} \cong K$.*

Proof. Let $g : K \to \widetilde{K}$ and $f : H \to \widetilde{H}$ be defined as $f(k) = (1,k)$ and $g(h) = (h,1)$.

$$g(k_1)g(k_2) = (1,k_1)(1,k_2) = (1\ k_2 \cdot 1, k_1k_2) = (1, k_1k_2) = g(k_1k_2) \tag{8}$$

$$f(h_1)f(h_2) = (h_1,1)(h_2,1) = (h_1\ 1 \cdot h_2, (1)(1)) = (h_1h_2, 1) = f(h_1h_2) \tag{9}$$

The above demonstrates that $\widetilde{K}$ and $\widetilde{H}$ are closed under multiplication and are therefore subgroups, and that f and g are homomorphisms. Since

$f(h) = (h, 1) = (1, 1) \Rightarrow h = 1$ and $g(k) = (k, 1) = (1, 1) \Rightarrow k = 1$, it follows that $\ker f = \ker g = 1$. Therefore, since $|H| = |\widetilde{H}|$ and $|K| = |\widetilde{K}|$, f and g represent isomorphisms.

□

Theorem 2.2. $\widetilde{H} \trianglelefteq H \rtimes K$.

Proof.

$$\begin{aligned}(h_c, k_c)^{-1}(h, 1)(h_c, k_c) &= (k_c^{-1} \cdot h_c^{-1}, k_c^{-1})(k_c \cdot h, k_c) \\ &= (k_c^{-1} \cdot h_c^{-1}\ k_c^{-1} \cdot (k_c \cdot h), k_c^{-1}k_c) \\ &= (k_c^{-1} \cdot h_c^{-1}\ (k_c^{-1}k_c) \cdot h, 1) \\ &= (k_c^{-1} \cdot h_c^{-1}\ 1 \cdot h, 1) \\ &= (k_c^{-1} \cdot h_c^{-1}\ h, 1) \in \widetilde{H}\end{aligned} \tag{10}$$

The above shows that $(h_c, k_c)^{-1}\widetilde{H}(h_c, k_c) \subseteq \widetilde{H}$ for all $(h_c, k_c) \in H \rtimes K$. Thus, $\widetilde{H} \trianglelefteq H \rtimes K$. □

Theorem 2.3. $\widetilde{H} \cap \widetilde{K} = 1$.

Proof. Say that some $(h, k) \in \widetilde{H} \cap \widetilde{K}$. Then $(h, k) = (h', 1)$ for some $(h', 1) \in \widetilde{H}$ and $(h, k) = (1, k')$ for some $(1, k') \in \widetilde{K}$. Thus, $k = 1$ and $h = 1$, so $(h, k) = 1$. Hence, $\widetilde{H} \cap \widetilde{K} = 1$. □

3 The Inner Semidirect Product

We saw in the previous section that the semidirect product $H \rtimes K$ satisfies $\widetilde{H} \trianglelefteq H \rtimes K$ and $\widetilde{H} \cap \widetilde{K} = 1$. In this section, we show that the semidirect product is the most general class of groups that satisfy these properties. We need one result before beginning the proof.

Lemma 3.1. *The function $\varphi : K \to (H \to H)$ defined by $\varphi(k)(h) = khk^{-1}$ maps into $\mathrm{Aut}(H)$, the space of automorphisms of H.*

Proof. Let $k \in K$. $\varphi(k)(h_1)\varphi(k)(h_2) = kh_1k^{-1}kh_2k^{-1} = kh_1h_2k^{-1} = \varphi(k)(h_1h_2)$, so $\varphi(k)$ must be a homomorphism. Moreover, $\ker \varphi(k) = \{h|\varphi(k)(h) = 1\} = \{h|khk^{-1} = 1\} = \{h|k^{-1}khk^{-1}k = k^{-1}k\} = \{h|h = 1\} = 1$. Thus, $\varphi(k)$ is an automorphism.

□

Theorem 3.1. *If H, K are subgroups of a group G where $H \trianglelefteq G$ and $H \cap K = 1$, then $HK \cong H \rtimes_\varphi K$ for some φ.*

Proof. Because of Lemma 3.1, $\varphi : K \to \mathrm{Aut}(H)$ and hence the group action $\cdot$ can be defined by the function $\varphi(k)(h) = khk^{-1}$.

Let us define $\psi : H \rtimes_\varphi K \to HK$ as $\psi((h,k)) = hk$.

$$\begin{aligned}
\psi((h_1,k_1))\psi((h_2,k_2)) &= h_1k_1h_2k_2 \\
&= h_1k_1h_2k_1^{-1}k_1k_2 \\
&= h_1(k_1h_2k_1^{-1})k_1k_2 \\
&\overset{(1)}{=} \psi((h_1(k_1h_2k_1^{-1}),k_1k_2)) \\
&= \psi((h_1\ k_1 \cdot h_2, k_1k_2)) \\
&= \psi((h_1,k_1)(h_2,k_2))
\end{aligned} \tag{11}$$

(1) is since $H \trianglelefteq G$ implies $k_1h_2k_1^{-1} \in H$. Thus, ψ is a homomorphism.

Say $(h,k) \in \ker\psi$, i.e. $\psi((h,k)) = hk = 1$. Note that this implies $h = k^{-1}$ and $k = h^{-1}$. Since K and H are subgroups, they are closed under inversion, so $h \in K$ and $k \in H$. Thus, $h, k \in H \cap K$, so $h = k = 1$. Thus $(h,k) = (1,1)$. Therefore, $\ker\psi = (1,1)$, the identity. Note that $|HK| = \frac{|H||K|}{|H\cap K|} = \frac{|\widetilde{H}||\widetilde{K}|}{|\widetilde{H}\cap\widetilde{K}|} = |H \rtimes K|$, Thus, ψ is an isomorphism. □

When classifying groups G that satisfy $H \trianglelefteq G$ and $H \cap K = 1$ for some H, K, this result allows us to enumerate all possibilities by iterating over all possible functions $\varphi : K \to \mathrm{Aut}(H)$.

4 Classification of Groups of Order 12

The results we have proved above along with what we have learned over the previous chapters can be used to classify all possible groups of order 12. Here, we define G to be any group of order 12. Let A be a Sylow-2 subgroup of G, and B be a Sylow-3 subgroup of G.

Lemma 4.1. *$AB = G$.*

Proof. By Lagrange's theorem, $|A| = 4$ divides $|AB|$ and $|B| = 3$ divides $|AB|$. Thus $\mathrm{LCM}(|A|,|B|) = 12$ divides $|AB|$. Moreover, since $AB \leq G$, $|AB|$ divides $|G| = 12$. Thus, $|AB| = |G| = 12$, and since $AB \subseteq G$, $AB = G$. □

Lemma 4.2. *Either $A \trianglelefteq G$ or $B \trianglelefteq G$.*

Proof. Say for the purpose of contradiction that A, B are not normal subgroups in G.

Then $n_2, n_3 \neq 1$. Since $n_3 \mid 4$ and $n_3 \equiv 1 \pmod 3$. Thus, $n_3 = 4$. Say for the purpose of contradiction that two distinct Sylow-3 subgroups B_1 and B_2 of G share a non-identity element b. Since $|B_1| = |B_2| = 3$ is prime, $B_1 = B_2 = \langle b \rangle$. This contradicts that B_1 and B_2 are distinct. Hence, every non-identity element in a given Sylow-3 subgroup is not found in any other Sylow-3 subgroup. Since $|B_1| = |B_2| = 3$ is prime, each non-identity element has order 3. Thus, since there are 4 Sylow-3 subgroups, each with 2 non-overlapping elements of order 3, G has at least $2 \times 4 = 8$ elements of order 3.

Since any Sylow-2 subgroup of G has order 4, its elements must have order 1, 2, or 4. Hence, each Sylow-2 subgroup A' must be a subset of $G_3^C = \{g \in G \mid |g| = 3\}^C$. Thus, since $4 = |A'| \leq |G_3^C| \leq 4$, so $G_3^C = 4$. Thus, since $|A'| = G_3^C$ and $A' \subseteq G_3^C$, it follows that $A' = G_3^C$. Thus, G_3^C is the unique Sylow-2 subgroup, so $n_2 = 1$. Thus, A is a normal subgroup in G, a contradiction. □

Lemma 4.3. *$B \cong Z_3$ and either $A \cong Z_4$ or $A \cong Z_2 \times Z_2$.*

Proof. Since $|B| = 3$ is prime, B is cyclic of order 3, therefore $B \cong Z_3$, proving the first part of the lemma.

Observe that all non-identity elements of A must have order 2 or 4. First, suppose that some element a has order 4. Thus, clearly $A = \langle a \rangle$, so A is cyclic of order 4, and therefore $A \cong Z_4$.

Now suppose that instead all elements of A have order 2. Thus, all elements are their own inverse. Thus, for all $x, y \in A$, $xy = x^{-1}y^{-1} = (x^{-1}y^{-1})^{-1} = (y^{-1})^{-1}(x^{-1})^{-1} = yx$, so A is abelian. Thus, A can be decomposed cyclically as Z_4 or $Z_2 \times Z_2$. Since no element of A has order 4, isomorphism with Z_4 is impossible, so $A \cong Z_2 \times Z_2$.

□

Lemma 4.4. $\mathrm{Aut}(Z_4) \cong \mathrm{Aut}(Z_3) \cong Z_2$ *and* $\mathrm{Aut}(Z_2 \times Z_2) \cong S_3$.

Proof. $\mathrm{Aut}(Z_4) \cong (\mathbb{Z}/4\mathbb{Z})_\times \overset{(2)}{\cong} Z_2$, with $^{(2)}$ true since $(\mathbb{Z}/4\mathbb{Z})_\times = \{\bar{1}, \bar{3}\}_\times$ is a group of prime order and therefore isomorphic to the corresponding cyclic group. Likewise $\mathrm{Aut}(Z_3) \cong (\mathbb{Z}/3\mathbb{Z})_\times \cong \{\bar{1}, \bar{2}\}_\times \cong Z_2$.

Since $x^2 = 1\ \forall x \in Z_2 \times Z_2$ and $Z_2 \times Z_2$ is abelian, we have $\mathrm{Aut}(Z_2 \times Z_2) \cong GL_2(\mathbb{F}_2) \cong S_3$.

□

Lemma 4.5. *If $A \trianglelefteq G$, then $G \cong Z_{12}$, $G \cong Z_2 \times Z_6$, or $G \cong A_4$.*

Proof. We can determine all possible isomorphism classes by generating semidirect products based on all possible homomorphisms $\varphi : B \to \mathrm{Aut}(A)$. Observe that since the only normal subgroups of B are 1 and B, it follows that $\ker\varphi = 1$ or $\ker\varphi = B$.

Suppose $A \cong Z_4$. Then $\mathrm{Aut}(A) \cong Z_2$. $\ker\varphi = 1$ is impossible since we are mapping into a smaller space. Thus, $\ker\varphi = B$ is the trivial homomorphism, implying that $b \cdot a = \varphi(b)(a) = id(a) = a\ \forall a \in A, b \in B$, so the semidirect product is equivalent to the direct product $A \times B \cong Z_4 \times Z_3 \cong Z_{12}$.

Now suppose $A \cong Z_2 \times Z_2$ and $\ker\varphi = B$. Again, $A \rtimes_\varphi B$ is just the direct product $A \times B$, and $A \times B \cong Z_2 \times Z_2 \times Z_3 \cong Z_2 \times Z_6$.

Now suppose $A \cong Z_2 \times Z_2$ and $\ker\varphi = 1$. Thus, $\varphi(B) \leq \mathrm{Aut}(A)$ has order 3. The only subgroup of S_3 of order 3 is $\langle(1\ 2\ 3)\rangle \cong Z_3$, which corresponds to a cyclic permutation of the three non-identity elements in $\mathrm{Aut}(A)$. Hence, we have three automorphisms $\varphi_0((x,1)) = (x,1), \varphi_0((1,x)) = (1,x)$ which is just the trivial automorphism, and therefore reduces to $A \times B \cong Z_2 \times Z_6$. The remaining automorphisms are $\varphi_1((x,1)) = (1,x), \varphi_1((1,x)) = (x,x)$ and $\varphi_2((x,1)) = (x,x), \varphi_2((1,x)) = (x,1)$. It can be easily demonstrated that for $\varphi = \varphi_1$ or $\varphi = \varphi_2$, $(Z_2 \times Z_2) \rtimes_\varphi Z_3 \cong A_4$ through the isomorphism $\psi((x^m, x^n, y^\ell)) = ((1\ 2)(3\ 4))^m((1\ 3)(2\ 4))^n(1\ 2\ 3)^\ell$. Thus $A \rtimes_\varphi B \cong A_4$.

□

Lemma 4.6. *If $B \trianglelefteq G$, then $G \cong Z_{12}$, $G \cong Z_2 \times Z_6$, $G \cong S_3 \times Z_2$, or $G \cong Z_3 \rtimes_\varphi Z_4$ for $\varphi(x^m)(x^n) = x^{n(-1)^m}$.*

Proof. We can determine all possible isomorphism classes by generating semidirect products based on all possible homomorphisms $\varphi : A \to \mathrm{Aut}(B)$. Observe that since $\mathrm{Aut}(B) \cong Z_2$, there is one non-identity element, which we denote λ. Since B is cyclic, it is therefore abelian, so the inverter $\psi(b) = b^{-1}\ \forall b \in B$ is an automorphism, and it is nontrivial since there exist elements of order 3 in B. Thus, this inverter is λ.

Suppose $A \cong Z_4$. The normal subgroups of Z_4 are 1, Z_4, and $\langle x^2\rangle$. $\ker\varphi = 1$ is impossible since we are mapping onto a smaller space. If $\ker\varphi = Z_4$, the semidirect product is equivalent to the direct product $A \times B \cong Z_4 \times Z_3 \cong Z_{12}$.

If $\ker\varphi = \langle x^2\rangle$, then $\varphi(1) = \varphi(x^2) = 1$ and $\varphi(x) = \varphi(x^3) = \lambda$. This is equivalent to $G \cong Z_3 \rtimes_\varphi Z_4$ for $\varphi(x^m)(x^n) = x^{n(-1)^m}$.

Suppose $A \cong Z_2 \times Z_2$. Again, $\ker\varphi = 1$ is impossible since we are mapping to a smaller space. If $\ker\varphi = Z_2 \times Z_2$, the homomorphism is trivial so $G \cong Z_2 \times Z_6$. The remaining subgroups of $Z_2 \times Z_2$ are $\langle(x,1)\rangle$, $\langle(1,x)\rangle$, and $\langle(x,x)\rangle$. We can easily verify that these result in semidirect products isomorphic to $S_3 \times Z_2$. For example, in the case that $\ker\varphi = \langle(x,1)\rangle$, we have the isomorphism $\psi((x^m, x^n, y^\ell)) = ((12)^n(123)^\ell, x^m)$. □

Theorem 4.1. *If $|G| = 12$, one of the following holds: $G \cong Z_{12}$, $G \cong Z_2 \times Z_6$, $G \cong A_4$, $G \cong S_3 \times Z_2$, or $G \cong Z_3 \rtimes_\varphi Z_4$ for $\varphi(x^m)(x^n) = x^{n(-1)^m}$.*

Proof. Lemma 4.2 states that for some G with $|G| = 12$, where a Sylow-2 group $A \leq G$ and a Sylow-3 group $B \leq G$, either A or B is normal in G. Lemmas 4.5 and 4.6 state that our proposition is not violated in either case. □

While it is beyond the scope of this section to show that none of the isomorphism groups described are equivalent, one can be sure that no isomorphism groups have been missed.