Semidirect Products

Alexander Reynolds
abreynolds@asu.edu

ARIZONA STATE UNIVERSITY

MAT 444: Abstract Algebra
Dr. John Jones
Spring 2016

1 Direct Products

Definition 1.1 (Direct Product)**.** Let I be any nonempty indexing set and let $(G_i, *_i)$ be a group for each $i \in I$. The *direct product* of an arbitrary collection of groups $\{G_i : i \in I\}$ is the set $G = \prod_{i \in I} G_i$ (the Cartesian product of all G_i) with a componentwise binary operation defined as follows: if $\prod a_i$ and $\prod b_i$ are elements of G, then their product in G is given by

$$\left(\prod_{i \in I} a_i\right) * \left(\prod_{i \in I} b_i\right) = \prod_{i \in I} (a_i *_i b_i)$$

where $*_i$ is the operation in the group G_i.

Proposition 1.1. *The direct product of groups is a group.*

Note from the definition that the operation in the constructed group relies only on the operations already given from the initial groups. This property makes the direct product quite intuitive and simple to work with in terms of computation. Recognizing direct products inside of another group is hardly more involved, so long as the normal subgroups are known. A few simple facts regarding subgroups will be recalled to understand how to recognize direct products.

Proposition 1.2. *If H is a normal subgroup of G, then for any subgroup K of G, HK is a subgroup of G.*

Proposition 1.3. *Let H and K be subgroups of the group G. The number of distinct ways of writing each element of the set HK in the form hk for some $h \in H$ and $k \in K$ is $|H \cap K|$. In particular, if $H \cap K = \langle e \rangle$, then each element of HK can be written uniquely as a product hk for some $h \in H$ and $k \in K$.*

Theorem 1.4 (Recognition Theorem)**.** *Suppose G is a group with normal subgroups H and K with trivial intersection. Then $HK \cong H \times K$.*

It is quite intuitive then both to recognize and construct direct products of groups.

2 Semidirect Products

Notice that the direct product of groups gives a set which is the Cartesian product of the groups. Though defining the operation in the direct product to be the component-wise product in each group is instinctive, there seems no reason to expect it should be the only way to combine elements over a Cartesian product of sets.

Consider the possibility that H and K are subgroups of a group G with trivial intersection and H is normal in G. From Proposition 1.2, HK is a subgroup of G. The group HK then combines elements $hk, h'k' \in HK$ by $(hk)(h'k') = h(kh'k^{-1})kk'$ where $h(kh'k^{-1}) \in H$ since H is normal and $kk' \in K$. Since the intersection of H and K are trivial, the representation $(hkh'k^{-1})(kk')$ is unique from Proposition 1.3. In other words, this is the group operation.

Since K is a group and $kk' \in K$, the operation to combine k and k' in G is the same as the operation in K. Similarly, the operation to combine the two elements h and $(kh'k^{-1})$ producing an element in H is the same as in G. However, the operations inside H and K are closed binary operations on the sets, and so the operation which conjugates h' by k is an operation that must occur outside of H and K. Notice that if $kh'k^{-1} = h'$, then K would be normal in G and the operation to combine elements in HK would only require the operations in H and K; and thus $HK \cong H \times K$ with the component-wise operations. So, if a different operation is to be considered over the Cartesian product of sets to form a group, there needs to be a way to define the conjugation $kh'k^{-1}$ in terms of H and K only.

Group actions allow for such a definition, since if H is normal in G, conjugation is an action of K on H. That is, viewing H as a left K-set, if $k \in K$ and $h \in H$ then

$$^{k}h = khk^{-1}$$

so that for any $hk, h', k' \in HK$,

$$(hk)(h'k') = (h\,{}^{k}h', kk').$$

The action of conjugation gives an homomorphism $\varphi : K \to \mathrm{Aut}(H)$ (as stated in the following proposition), and thus this operation is fully defined in terms of H and K, as required.

Proposition 2.1. *Let H and K be groups. The map*

$$\begin{aligned} \varphi : K &\longrightarrow \mathrm{Aut}(H) \\ k &\longmapsto \varphi(k) \end{aligned} \tag{1}$$

is an homomorphism, where $\varphi(k)$ is an action of k on H by conjugation, viz.,

$$\begin{aligned} \varphi(k) : H &\longrightarrow H \\ h &\longmapsto {}^{k}h = khk^{-1}. \end{aligned} \tag{2}$$

Proof. To show that φ is an homomorphism is to show that for all $k, k' \in K$, $\varphi(kk') = \varphi(k)\varphi(k')$. Since $\varphi(k)$ is a function, the equality is given by demonstrating that both $\varphi(kk')$ and $\varphi(k)\varphi(k')$ affect an element $h \in H$ identically. Let $h \in H$ be arbitrary. Then

$$\varphi(kk')(h) = (kk')h(kk')^{-1} = k(k'hk'^{-1})k^{-1} = \varphi(k)(k'hk'^{-1}) = \varphi(k)(\varphi(k')(h)) = \varphi(k)\varphi(k')(h).$$

Therefore, φ is an homomorphism. □

The presentation of the left action as a left superscript allows for easier reading in most cases, as ${}^{k}h$ is more compact than $\varphi(k)(h)$ and emphasizes that ${}^{k}h$ is an element of H. In some cases, for clarity of notation $\varphi(k)(h)$ will be used interchangeably with ${}^{k}h$, but keep in mind that $\varphi(k)(h) \in H$.

A group operation can be developed using the map from Proposition 2.1 allowing to connect two groups H and K into a group. More specifically, two groups H and K along with an homomorphism $\varphi : K \to \mathrm{Aut}(H)$ uniquely yield a larger group. The statements in the introduction to this section are summarized in the following recognition theorem for specific reference and proof.

Proposition 2.2. *Suppose H is a normal subgroup of a group G and K is a subgroup so that $H \cap K = \{e\}$. Then HK is a subgroup of G, and if $h, h' \in H$ and $k, k' \in K$ then $(hk)(h'k') = h''k''$ where*

$$h'' = h\,{}^{k}h',$$
$$k'' = kk'$$

and for any $hk \in HK$,

$$(hk)^{-1} = {}^{k^{-1}}h^{-1}k^{-1}.$$

Proof. From Proposition 1.2, HK is a subgroup of G. Let $hk, h'k' \in HK$. Then

$$(hk)(h'k') = hkh^{-1}(k^{-1}k)k' = h(kh'k^{-1}) = h\,{}^{k}h'kk'.$$

Now, let $hk \in HK$. Then

$$(hk)^{-1} = k^{-1}h^{-1} = k^{-1}h^{-1}kk^{-1} = {}^{k^{-1}}h^{-1}k^{-1}.$$ □

Proposition 1.3 suggests unique representations of elements in HK and Proposition 2.2 suggests an operation which is closed under inversion and multiplication. That is, the elements with the operation have a group structure. Further, since the elements can be represented uniquely as hk, they can be associated to pairs (h, k). As mentioned earlier, for direct products, these pairs are combined under a canonical map from element-wise group operations. However, this is not the operation defined in 2.2. Under this operation, the group HK is termed a *semidirect product*. A constructive theorem will give the necessary formality.

Theorem 2.3. *Let H and K be groups, and $\varphi : K \to \mathrm{Aut}(H)$ be an homomorphism. Then $(G, *) = (\{(h, k) : h \in H, k \in K\}, *)$ is a group with*

- *identity* $(e_H, e_K) = (e, e)$*,*
- *operation* $(h,k) * (h',k') = (h\,{}^{k}h', kk')$ *for all* $(h,k),(h',k') \in G$*,*
- *inversion* $(h,k)^{-1} = ({}^{k^{-1}}h^{-1}, k^{-1})$ *for all* $(h,k) \in G$*.*

Proof. To show G is a group, the associative, identity, and inverse laws must be obeyed under the operation.

- (Associativity) Let $(h,k),(h',k'),(h'',k'') \in G$. Then

$$\begin{aligned}((h,k)*(h',k'))*(h'',k'') &= (h\,{}^{k}h', kk')*(h'',k'')\\ &= (h\,{}^{k}h'\,{}^{kk'}h'', kk'k'')\\ &= (h\,{}^{k}h'\,{}^{k}({}^{k'}h''), kk'k'')\\ &= (h\,{}^{k}h'\,{}^{k'}h''), kk'k'')\\ &= (h,k)*(h'\,{}^{k'}h''), k'k'')\\ &= (h,k)*((h',k')*(h'',k'')).\end{aligned}$$

- (Identity) Let $(h,k) \in G$, and consider $(e,e) \in G$. Left and right multiplication yield

$$\begin{aligned}(h,k)*(e,e) &= (h\,{}^{k}e, k) = (h,k),\\ (e,e)*(h,k) &= (e\,{}^{e}h, k) = (h,k).\end{aligned}$$

- (Inversion) Let $(h,k) \in G$. Then

$$(h,k)*({}^{k^{-1}}h^{-1}, k^{-1}) = (h\,{}^{k}({}^{k^{-1}}h^{-1}), kk^{-1}) = (hh^{-1}, kk^{-1}) = (e,e).$$

Thus, $(G,*)$ is a group. □

Definition 2.1 (Semidirect Product)**.** A group G satisfying the properties in Theorem 2.3 is denoted the *semidirect product* of H and K with homomorphism φ, notated $G = H \rtimes_\varphi K$. In the typical case where the homomorphism is understood, it is written

$$G = H \rtimes K. \tag{3}$$

Many interesting properties of the semidirect product fall from the prior constructions. These are enumerated in a single corollary.

Corollary 2.4. *Let* $G = H \rtimes_\varphi K$*. Then*

(1) $|G| = |H||K|$*,*

(2) $\{(h,e) : h \in H\}$ *and* $\{(e,k) : k \in K\}$ *are subgroups of* G *isomorphic to* H *and* K *respectively,*

(3) H is normal in G,

(4) $H \cap K = \langle e \rangle$,

(5) $khk^{-1} = {}^k h$ for all $h \in H, k \in K$.

Proof. First, note that $|G| = |H \times K| = |H||K|$, yielding (1).

Define the bijections $H \to G$ by $h \mapsto (h, e)$ and $K \to G$ by $k \mapsto (e, k)$. Let $h, h' \in H$ and $k, k' \in K$. Then

$$(h, e)(h', e) = (h\, {}^e h') = (hh', e),$$
$$(e, k)(e, k') = (e\, {}^k e, kk') = (e, kk'),$$

so these maps are homomorphisms, and thus $\{(h, e) : h \in H\} \cong H$ and $\{(e, k) : k \in K\} \cong K$, giving the necessary isomorphisms for (2).

From the isomorphism in (2), (4) follows:

$$H \cap K = \{(h, e) : h \in H\} \cap \{(e, k) : k \in K\} = \{(e, e)\}.$$

Let $h, k \in G$. Then

$$\begin{aligned}(e, k)(h, e)(e, k)^{-1} &= ((e, k)(h, e))(e, k)^{-1} \\ &= ({}^k h, k)(e, k^{-1}) \\ &= ({}^k h\, {}^k e, kk^{-1}) \\ &= ({}^k h, 1).\end{aligned}$$

It follows that $khk^{-1} = {}^k h$ for all $h \in H, k \in K$, so that (5) holds under the mappings from the isomorphisms in (2). Additionally, since ${}^k h \in H$ and k was arbitrary, H is normal in G, which is (3). This completes the proof. □

Note that the semidirect product symbol $\rtimes$ is a superimposition of the direct product symbol $\times$ with the symbol $\triangleleft$ indicating normal subgroup inclusion. The normal subgroup is placed on the left so that $G = H \rtimes_\varphi K$ refers to the group with elements from $H \times K$ with multiplication given by φ and where H is normal in G (but K is not necessarily normal).

Theorem 2.5 (Recognition Theorem)**.** *Suppose G is a group with subgroups H and K, so that H is normal in G and the intersection $H \cap K$ is trivial. If $\varphi : K \to \mathrm{Aut}(H)$ is the automorphism given by left conjugation by k, then $HK \cong H \rtimes K$. If $G = HK$ then $G = H \rtimes K$.*

Proof. This is simply a restatement of Proposition 2.2 with more formality relating to semidirect products. □

It seems relatively clear that under some particular homomorphism, the semidirect product will yield the direct product. In fact, it was already mentioned earlier that if conjugation by k did not affect h, then K would be normal; since the additional requirement from direct products is that K should also be normal, the homomorphism $\varphi : K \to \mathrm{Aut}(H)$ should be trivial, so that φ does not permute of the elements in H.

Proposition 2.6. *Let H and K be groups and let $\varphi : K \to \mathrm{Aut}(H)$ be an homomorphism. Then the following are equivalent:*

(1) the identity map between $H \rtimes K$ and $H \times K$ is an isomorphism

(2) $\varphi : K \to \mathrm{Aut}(H)$ is the trivial homomorphism

(3) K is normal in $H \rtimes K$.

Proof. (1) $\implies$ (2). Suppose $h, h' \in H$ and $k, k' \in K$ and there exists an isomorphism from $H \rtimes K$ to $H \times K$. Then

$$(h\,{}^k h', kk') = (h,k)(h',k') = (hh', kk')$$

where the first equality follows from the group operation in $H \rtimes K$ and the second follows from the group operation in $H \times K$. This shows $h' = {}^k h'$ for all k and h', that is, $\varphi(k)$ is the trivial (identity) automorphism.

(2) $\implies$ (3). Suppose φ is trivial. Then for all $k \in K, h \in H$, ${}^k h = h$, so K is normal in H. Since K is normal in K and H and K make up all elements of $H \rtimes K$, then K is normal in $H \rtimes K$.

(3) $\implies$ (1). Suppose that K is normal in $H \rtimes K$. Then $hk = kh$ for all $h \in H, k \in K$ and the action is trivial, so that

$$(h,k)(h',k') = (h\,{}^k h', kk') = (hh', kk')$$

for all $h, h' \in H$ and $k, k' \in K$. □

Semidirect products are determined by the given homomorphisms, but no statements so far have suggested the uniqueness of semidirect products from distinct homomorphisms. This is because it is indeed possible for two different maps to yield isomorphic semidirect products.

Theorem 2.7. *Suppose that K, J and H are groups, $\sigma : K \to J$ is an isomorphism, and $\psi : J \to \mathrm{Aut}(H)$ is an homomorphism, so that $\varphi = \psi \circ \sigma : K \to \mathrm{Aut}(H)$ is also an homomorphism. Then $H \rtimes_\varphi K \cong H \rtimes_\psi J$.*

Proof. To construct a isomorphism between the two semidirect products, consider the map

$$\begin{aligned} \Phi : H \rtimes_\varphi K &\longrightarrow H \rtimes_\psi J \\ (h,k) &\longmapsto (h, \sigma(k)). \end{aligned}$$

Since σ is an isomorphism, $\sigma(e) = e$ so that $(h, \sigma(e)) = (h, e)$ for all $h \in H$. If $(h, j) \in H \rtimes_\psi J$, then $j \in J$ and since σ is onto, $\sigma(k) = j$ for some $k \in K$. So $\Phi(h,k) = (h, j)$ so φ is onto. If $\Phi(h,k) = \Phi(h',k')$ then $(h, \sigma(k)) = (h', \sigma(k'))$, so $h = h'$ and $\sigma(k) = \sigma(k')$. Since σ is bijective, the inverse map σ^{-1} exists and $k = \sigma^{-1}(\sigma(k)) = \sigma^{-1}(\sigma(k')) = k'$. So, Φ is a bijection.

The function σ is an homomorphism, so

$$\Phi(h,k)\Phi(h',k') = (h, \sigma(k))(h', \sigma(k') = (hh', \sigma(k)\sigma(k')) = (hh', \sigma(kk')) = \Phi(hh', kk')$$

as required. Therefore Φ is an isomorphism. □

Corollary 2.8. *Suppose that K and H are groups. If $\psi : K \to \mathrm{Aut}(H)$ is an homomorphism, then for any $\sigma \in \mathrm{Aut}(K)$, $\varphi = \psi \circ \sigma : K \to \mathrm{Aut}(H)$ is also an homomorphism giving $H \rtimes_\varphi K \cong H \rtimes_\psi K$.*

Proof. Apply Theorem 2.7 with $J = K$. □

Corollary 2.9. *Suppose that H and K are groups, K is cyclic, and $\varphi, \psi : K \to \mathrm{Aut}(H)$ are monomorphisms with the same image in $\mathrm{Aut}(H)$. Then there exists $\sigma \in \mathrm{Aut}(K)$ so that $\varphi = \psi \circ \sigma$.*

Proof. This follows from Corollary 2.8 as if K is cyclic then any automorphism σ preserves the generators of K. □

Lemma 2.10. $\mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^*$ *for all positive integers n.*

Proof. Note that the elements of $\mathbb{Z}_n^*$ are the generators of $\mathbb{Z}_n$. If $\sigma \in \mathrm{Aut}(\mathbb{Z}_n)$, then $\sigma(1)$ generates $\mathbb{Z}_n$ since 1 generates $\mathbb{Z}_n$; thus the evaluation homomorphism

$$\begin{aligned} \varphi : \mathrm{Aut}(\mathbb{Z}_n) &\longrightarrow \mathbb{Z}_n^* \\ \sigma_1 &\longmapsto \sigma(1) \end{aligned}$$

is an isomorphism of groups. □

Theorem 2.11. *Suppose G is a group of order pq where $p < q$ are primes. Then either*

- $q \not\equiv 1 \pmod{p}$ *and $G \cong \mathbb{Z}_{pq}$, or*
- $q \equiv 1 \pmod{p}$ *and either $G \cong \mathbb{Z}_{pq}$ or G is non-abelian and $G \cong \mathbb{Z}_p \rtimes \mathbb{Z}_q$.*

Proof. Suppose P is a Sylow p-subgroup and Q is a Sylow q-subgroup of a group G. Then $n_p \mid p$ and $n_q \equiv 1 \pmod{q}$. Since $p < q$, this forces $n_q = 1$ so Q is normal in G. The subgroup $P \cap Q = \langle e \rangle$ since the order divides p and q, which are prime. Thus PQ is a subgroup of G containing P and Q. Further, p and q divide $|PQ|$, so $G = PQ$. This yields a semidirect product since all elements can be written uniquely as elements from the Cartesian product $P \times Q$.

The direct product $P \times Q$ always exists for groups P and Q, so it could be that $G \cong P \times Q \cong \mathbb{Z}_{pq}$ whence $\varphi : Q \to \mathrm{Aut}(P)$ is trivial.

By Lemma 2.10, $\mathrm{Aut}(Q)$ has order $q-1$ since $\mathbb{Z}_{q-1}^*$ has order $q-1$. Thus a nontrivial homomorphism $\varphi : Q \to \mathrm{Aut}(P)$ exists if and only if $p \mid (q-1)$. If nontrivial homomorphisms do exist, then by Proposition 2.9 they all give isomorphic semidirect products.

Therefore if $p \mid (q-1)$, there are two isomorphisms, $\varphi, \psi : Q \to \mathrm{Aut}(P)$ where φ is trivial, and otherwise there is only the trivial homomorphism φ. The result follows. □

Example 2.1. Classification of groups of order 15.

Let G be a group with $|G| = 15 = 3 \cdot 5$. Since $5 \not\equiv 1 \pmod{3}$, by Theorem 2.11, $G = \mathbb{Z}_{15}$.

Example 2.2. Classification of groups of order 12.

Let G be a group with $|G| = 12 = 2^2 \cdot 3$. Let H be a Sylow 2-subgroup of order 4 and K be a Sylow 3-subgroup, so that $H \cong V_4$ or $H \cong \mathbb{Z}_4$ and $K \cong \mathbb{Z}_3$. One of H or K (or both) are normal since $HK = G$, following from the fact that $H \cap K = \langle e \rangle$ since $\gcd(|H|, |K|) = 1$. This yields the following possibilities for the group G represented as a semidirect product:

(1) $\mathbb{Z}_4$ and $\mathbb{Z}_3$ are both normal

(2) $\mathbb{Z}_4$ is normal, $\mathbb{Z}_3$ is not normal

(3) $\mathbb{Z}_4$ is not normal, $\mathbb{Z}_3$ is normal

(4) V_4 and $\mathbb{Z}_3$ are both normal

(5) V_4 is normal, $\mathbb{Z}_3$ is not normal

(6) V_4 is not normal, $\mathbb{Z}_3$ is normal

For cases (1) and (4), these correspond to the direct products so that in (1) $G \cong \mathbb{Z}_{12}$ and in (4) $G \cong \mathbb{Z}_2 \times \mathbb{Z}_6$.

For (2), $\mathrm{Aut}(\mathbb{Z}_4) \cong \mathbb{Z}_2$ by Lemma 2.10, and any homomorphism $\varphi : \mathbb{Z}_3 \to \mathbb{Z}_2$ is trivial.

In case (3), $\mathrm{Aut}(\mathbb{Z}_4) \cong \mathbb{Z}_2$ by Lemma 2.10, and there is one non-trivial homomorphism $\varphi : \mathbb{Z}_4 \to \mathbb{Z}_2$, yielding a non-abelian semidirect product $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$. This is not isomorphic to A_4 nor D_6, it is the *dicyclic* group of order $4 \cdot 3$, written $G = \mathrm{Dic}_3$.

The automorphisms of the Klein 4-group $\mathrm{Aut}(V_4) \cong S_3$, so in case (5) the images of the homomorphisms $\varphi, \psi : V_4 \to S_3$ are the same so they are simply related by an automorphism of S_3. Since A_4 is the only non-abelian group of order 12 with a single 2-subgroup, $G = A_4$.

Again by Lemma 2.10, $\mathrm{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_2$, so with the assumptions in (6) the maps $\varphi : V_4 \to \mathbb{Z}_2$ which have kernels as (proper, nontrivial) subgroups in V_4 give rise to three distinct homomorphisms. However, by Corollary 2.9 these are all equivalent up to some automorphism of V_4, yielding identical semidirect products: $G = D_6$

No other representations of G are possible, since by Lagrange's theorem, $|H \cap K| = 1$; G must then be one of the five semidirect products:

(1) $G = \mathbb{Z}_{12}$ and is abelian

(2) $G = \mathbb{Z}_2 \times \mathbb{Z}_6$ and is abelian

(3) $G = D_6$ and is non-abelian

(4) $G = A_4$ and is non-abelian

(5) $G = \mathrm{Dic}_3$ and is non-abelian