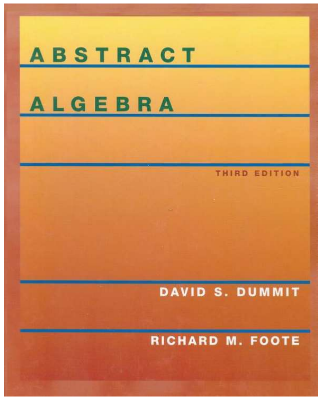
Modern Algebra

Direct Products and Semidirect Products

5.4 Recognizing Direct Products, 5.5 Semidirect Products

—Proofs of Theorems



Theorem DF.5.7

Proposition DF.5.7. Let G be a group, let $x, y \in G$, and let $H \leq G$. Then

(1) $xy = yx[x, y]$.

(2) $H \trianglelefteq G$ if and only if $[H, G] \leq H$.

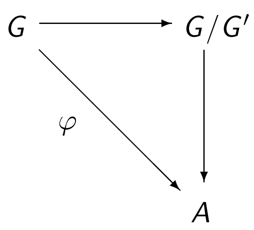
(3) For any automorphism σ of G, we have $\sigma[x, y] = [\sigma(x), \sigma(y)]$. Also, G' is a *characteristic subgroup* of G (denoted "G' char G"; this means that every automorphism of G maps G' to itself, i.e., $\sigma(G') = G'$) and G/G' is abelian.

(4) G/G' is the largest abelian quotient group of G in the sense that if $H \trianglelefteq G$ and G/H is abelian, then $G' \leq H$. Conversely, if $G' \leq H$, then $H \trianglelefteq G$ and G/H is abelian.

Theorem DF.5.7 (continued 1)

Proposition DF.5.7. Let G be a group, let $x, y \in G$, and let $H \leq G$. Then

(5) If $\varphi : G \to A$ is any homomorphism of G into an abelian group A, then φ factors through G', i.e., $G' \leq \ker(\varphi)$ and the following diagram commutes:



Theorem DF.5.7 (continued 2)

Proposition DF.5.7. Let G be a group, let $x, y \in G$, and let $H \leq G$. Then

(1) $xy = yx[x, y]$.

(2) $H \trianglelefteq G$ if and only if $[H, G] \leq H$.

Proof. (1) We have $yx[x, y] = yxx^{-1}y^{-1}xy = xy$. □

(2) We have $H \trianglelefteq G$ is and only if $g^{-1}hg \in H$ for all $g \in G$ and all $h \in H$ by Theorem I.5.1. For $h \in H$, we have $g^{-1}hg \in H$ if and only if $h^{-1}g^{-1}hg = [h, g] \in H$. So $H \trianglelefteq G$ is an only if $[h, g] \in H$ for all $h \in H$ and all $g \in G$. That is, $H \trianglelefteq G$ if and only if $[H, G] \leq H$. □

Theorem DF.5.7 (continued 3)

Proposition DF.5.7. Let G be a group, let $x, y \in G$, and let $H \leq G$. Then

(3) For any automorphism σ of G, we have $\sigma[x, y] = [\sigma(x), \sigma(y)]$. Also, G' is a *characteristic subgroup* of G (denoted "G' char G"; this means that every automorphism of G maps G' to itself, i.e., $\sigma(G') = G'$) and G/G' is abelian.

Proof (continued). (3) Let $\sigma \in \text{Aut}(G)$ be an automorphism of G and let $x, y \in G$. Then

$$\begin{aligned}\sigma([x,y]) &= \sigma(x^{-1}y^{-1}xy)\\ &= \sigma(x^{-1})\sigma(y^{-1})\sigma(x)\sigma(y) \text{ since } \sigma \text{ is an automorphism}\\ &= \sigma(x)^{-1}\sigma(y)^{-1}\sigma(x)\sigma(y) \text{ since } \sigma \text{ is an automorphism}\\ &= [\sigma(x), \sigma(y)].\end{aligned}$$

Thus for every commutator $[x, y] \in G'$, $\sigma([x, y]) \in G'$.

Theorem DF.5.7 (continued 4)

Proof continued. Since σ has a two-sided inverse (because Aut(G) is a group), then σ maps the set of commutators bijectively onto itself. Since the commutators are a generating set for G', then $\sigma(G') = G'$. That is, G' char G.

We now show that G/G' is abelian. Let xg' and yG' be arbitrary elements of G/G'. We have

$$\begin{aligned}(xG')(yG') &= (xy)G' \text{ by definition}\\ &= (yx[xy])G' \text{ by (1)}\\ &= (yx)G' \text{ since } [x,y] \in G'\\ &= (yG')(xG') \text{ by definition.}\end{aligned}$$

□

Theorem DF.5.7 (continued 5)

Proposition DF.5.7. Let G be a group, let $x, y \in G$, and let $H \leq G$. Then

(4) G/G' is the largest abelian quotient group of G in the sense that if $H \trianglelefteq G$ and G/H is abelian, then $G' \leq H$. Conversely, if $G' \leq H$, then $H \trianglelefteq G$ and G/H is abelian.

Proof (continued). (4) Suppose $H \trianglelefteq G$ and G/H is abelian. Then for all $x, y \in G$ we have $(xH)(yH) = (yH)(xH)$ and so

$$\begin{aligned}1H &= (xH)^{-1}(xH)(yH)^{-1}(yH) \text{ by the definition of the identity in } G/H\\ &= (xH)^{-1}(yH)^{-1}(xH)(yH) \text{ since } G/H \text{ is abelian}\\ &= (x^{-1}y^{-1}xy)H \text{ by the definition of coset mulitplication}\\ &= [x,y]H.\end{aligned}$$

So $[x, y] \in H$ for all $x, y \in G$ and hence $G' \leq H$. So G/G' is the largest abelain quotient group.

Theorem DF.5.7 (continued 6)

Proposition DF.5.7. Let G be a group, let $x, y \in G$, and let $H \leq G$. Then

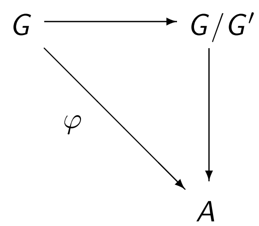
(4) G/G' is the largest abelian quotient group of G in the sense that if $H \trianglelefteq G$ and G/H is abelian, then $G' \leq H$. Conversely, if $G' \leq H$, then $H \trianglelefteq G$ and G/H is abelian.

Proof (continued). Conversely, if $G' \leq H$ then, since G/G' is abelian (by (3)), every subgroup of G/G' is normal. In particular, $H/G' \trianglelefteq G/G'$. By Corollary I.5.12, this implies that $H \trianglelefteq G$. By the Third Isomorphism Theorem (Corollary I.5.10), we have that $G/H \cong (G/G')/(H/G')$. Therefore G/H is abelian since it is a quotient group of the abelian group G/G'. □

Theorem DF.5.7 (continued 7)

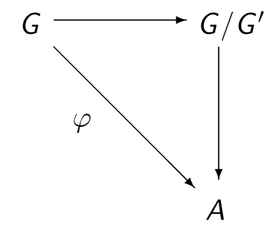
Proposition DF.5.7. Let G be a group, let $x, y \in G$, and let $H \leq G$. Then

(5) If $\varphi : G \to A$ is any homomorphism of G into an abelian group A, then φ factors through G', i.e., $G' \leq \ker(\varphi)$ and the following diagram commutes:



Theorem DF.5.7 (continued 8)

Proof (continued). (5) With ψ as the canonical homomorphism mapping $G \to G/G'$, we have $\ker(\psi) = G'$. So for any given homomorphism $\varphi : G \to A$, by Theorem I.5.6, there is a unique homomorphism θ mapping $G/G' \to A$ such that $\varphi = \theta \circ \psi$. That is, the diagram commutes:



□

Corollary DF.3.15

Corollary DF.3.15. If H and K are subgroups of G and $H \leq N_G(K) = \{g \in G \mid gKg^{-1} = K\}$, then HK is a subgroup of G. In particular, if $K \trianglelefteq G$ then $HK \leq G$ for any $H \leq G$.

Proof. Let $h \in H$, $k \in K$. Since $H \leq N_G(K)$ then $hkh^{-1} \in K$ and so $hk = hk(h^{-1}h) = (hkh^{-1})h \in KH$ and so $HK \subset KH$. Similarly $kh = (hh^{-1})kh = h(h^{-1}kh) \in HK$. Therefore $KH = HK$ and by the previous not, HK is a subgroup of G. □

Theorem DF.5.10

Theorem DF.5.10. Let H and K be groups and let φ be a homomorphism from K into $\mathrm{Aut}(H)$. Let $\cdot$ denote action of K on H determined by φ. Let G be the set of ordered pairs (h, k) with $h \in H$ and $k \in K$ and define the binary operation $(h_1, k_1)(h_2, k_2) = (h_1\ k_1 \cdot h_2, k_1, k_2)$.

(1) The binary operation makes G a group of order $|G| = |H||K|$.

(2) The sets $\tilde{H} = \{(h, 1) \mid h \in H\}$ and $\tilde{K} = \{(1, k) \mid k \in K\}$ are subgroups of G and the maps $h \mapsto (h, 1)$ for $h \in H$ and $k \mapsto (1, k)$ for $k \in K$ are isomorphisms of these subgroups with groups H and K.

(3) $H \trianglelefteq G$ (associating H with its isomorphic copy of ordered pairs).

(4) $H \cap K = \{1\}$.

(5) For all $h \in H$ and $k \in K$, we have $khk^{-1} = k \cdot h = \varphi(k)(h)$.

Theorem DF.5.10 (continued 1)

Theorem DF.5.10. Let H and K be groups and let φ be a homomorphism from K into $\text{Aut}(H)$. Let $\cdot$ denote action of K on H determined by φ. Let G be the set of ordered pairs (h,k) with $h \in H$ and $k \in K$ and define the binary operation $(h_1,k_1)(h_2,k_2) = (h_1\ k_1 \cdot h_2, k_1, k_2)$.

(1) The binary operation makes G a group of order $|G| = |H||K|$.

Proof. (1) For $1 \in K$ and φ a homomorphism from K into $\text{Aut}(H)$, we have that $\varphi(1)$ is the identity automorphism of H since a homomorphism maps an identity to an identity. So for $h \in H$ the action is $1 \cdot h = h$. We use this to show that the identity is $(1,1)$:

$$\begin{aligned}(1,1)(h,k) &= (1\ 1 \cdot h, 1k)\\ &= (1h, 1k) \text{ by above}\\ &= (h,k).\end{aligned}$$

Now for any $\varphi(k) \in \text{Aut}(H)$, since $\varphi(k)$ is an automorphism then $k \cdot h = \varphi(k)(h)$ is the inverse of $k \cdot h^{-1} = \varphi(k)(h^{-1})$.

Theorem DF.5.10

Theorem DF.5.10 (continued 2)

Proof (continued). We use this to show that the the inverse of (h,k) is $(k^{-1} \cdot h^{-1}, k^{-1})$:

$$\begin{aligned}(k^{-1} \cdot h^{-1}, k^{-1})(h,k) &= ((k^{-1} \cdot k^{-1})(k^{-1} \cdot h), k^{-1}k)\\ &= (1,1) \text{ by above.}\end{aligned}$$

Since we have established a left identity and left inverses, by Theorem I.1.3, we have a two sided identity and two sided inverses.

For associativity (using Dummit and Foote's notation):

$$\begin{aligned}((a,x),(b,y))(c,z) &= (ax \cdot b, xy)(cz)\\ &= ((ax \cdot b)((xy.c), xyz)\\ &= ((a\ x \cdot b)(x \cdot (y \cdot x)), xyz)\\ &= (a((x \cdot b)(x \cdot (y \cdot c))), xyz)\\ &= (a(x \cdot (b(y \cdot c))), xyz) \text{ since the action}\\ &\quad \text{of } x \text{ is an automorphism and so}\\ &\quad (x \cdot b)(x \cdot (y \cdot c)) = x \cdot (b(y \cdot c))\end{aligned}$$

Theorem DF.5.10

Theorem DF.5.10 (continued 3)

Theorem DF.5.10. Let H and K be groups and let φ be a homomorphism from K into $\text{Aut}(H)$. Let $\cdot$ denote action of K on H determined by φ. Let G be the set of ordered pairs (h,k) with $h \in H$ and $k \in K$ and define the binary operation $(h_1,k_1)(h_2,k_2) = (h_1\ k_1 \cdot h_2, k_1, k_2)$.

(1) The binary operation makes G a group of order $|G| = |H||K|$.

Proof (continued).

$$\begin{aligned}((a,x),(b,y))(c,z) &= (a(x \cdot (b(y \cdot c))), xyz)\\ &= (a,x)(b\ y \cdot c, yz) \text{ by the definition}\\ &\quad \text{of the binary operation}\\ &= (z,x)((b,y)(c,z)) \text{ by the definition}\\ &\quad \text{of the binary operation.}\end{aligned}$$

So G is a group under the binary operation.

Theorem DF.5.10

Theorem DF.5.10 (continued 4)

Theorem DF.5.10.

(2) The sets $\tilde{H} = \{(h,1) \mid h \in H\}$ and $\tilde{K} = \{(1,k) \mid k \in K\}$ are subgroups of G and the maps $h \mapsto (h,1)$ for $h \in H$ and $k \mapsto (1,k)$ for $k \in K$ are isomorphisms of these subgroups with groups H and K.

Proof (continued). (2) Let $\theta : H \to \tilde{H}$ and $\psi : K \to \tilde{K}$ be defined as $\theta(h) = (h,1)$ and $\psi(k) = (1,k)$. Then "clearly" θ and ψ are one to one and onto. Now

$$\theta(h_1h_2) = (h_1h_2, 1) = (h_1\ 1 \cdot h_2, 11) = (h_1,1)(h_2,1) = \theta(h_1)\theta(h_2), \text{ and}$$

$$\begin{aligned}\psi(k_1k_2) &= (1, k_1k_2) = (1\ 1, k_1k_2)\\ &= (1\ k_1 \cdot 1, k_1k_2) \text{ since action on 1}\\ &\quad \text{by an automorphism yields 1 } (*)\\ &= (1,k_1)(1,k_2) = \psi(k_1)\psi(k_2).\end{aligned}$$

Theorem DF.5.10 (continued 5)

Theorem DF.5.10.

(4) $H \cap K = \{1\}$.

(5) For all $h \in H$ and $k \in K$, we have $khk^{-1} = k \cdot h = \varphi(k)(h)$.

Proof (continued). (4) "Clearly" $\tilde{H} \cap \tilde{K} = \{(1,1)\}$. Identifying H and K with $\tilde{H}$ and $\tilde{K}$ (as hypothesized) yields $H \cap K = \{1\}$.
(5) We now show that when k acts on h, the action is actually conjugation: $k \cdot h = khk^{-1}$. Notice that, in the notation of $\tilde{H}$ and $\tilde{K}$,

$$\begin{aligned}(1,k)(h,1)(1,k)^{-1} &= ((1,k)(h,1))(1,k^{-1}) \\ &= (1\ k \cdot h, k)(1,k^{-1}) \\ &= (k \cdot h\ k \cdot 1, kk^{-1}) \\ &= (k \cdot h, 1) \text{ since } k \cdot 1 = 1 \text{ as in (1); see } (*).\end{aligned}$$

"Identifying" H and K with $\tilde{H}$ and $\tilde{K}$ gives $khk^{-1} = k \cdot h = \varphi(k)(h)$.

Theorem DF.5.10 (continued 6)

Theorem DF.5.10. Let H and K be groups and let φ be a homomorphism from K into $\mathrm{Aut}(H)$. Let $\cdot$ denote action of K on H determined by φ. Let G be the set of ordered pairs (h,k) with $h \in H$ and $k \in K$ and define the binary operation $(h_1,k_1)(h_2,k_2) = (h_1\ k_1 \cdot h_2, k_1,k_2)$.

(3) $H \trianglelefteq G$ (associating H with its isomorphic copy of ordered pairs).

Proof (continued). (3) Recall that $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$ is the normalizer of H in G. By (5), since $khk^{-1} = k \cdot h = \varphi(k)(h)$ and $\varphi(k)$ is an automorphism of H, then $khk^{-1} \in H$ for all $h \in H$ and for all $k \in K$, and so $kHk^{-1} = k \cdot H = \varphi(k)(H) = H$. So $K < N_G(H)$. Also, of course, $H \leq N_G(H)$. Since $G = HK$ (though technically G consists of ordered pairs instead of products, but we "identity" these). So $G \leq N_G(H)$ and hence $G = N_G(H)$. That is, $H \trianglelefteq G$. □

Proposition DF.5.11

Proposition DF.5.11. Let H and K be groups and let $\varphi : K \to \mathrm{Aut}(H)$ be a homomorphism. The following are equivalent.

(1) The identity set map between $H \rtimes K$ and $H \times K$ (both consisting of ordered pairs) is a group homomorphism (and hence $H \rtimes K \cong H \times K$).

(2) φ is the trivial homomorphism from K into $\mathrm{Aut}(H)$ (which maps all $k \in K$ to the identity automorphism).

(3) $K \trianglelefteq H \rtimes K$.

Proof. (1) implies (2) Suppose the identity map is an isomorphism between $H \rtimes K$ and $N \times K$. In $H \times K$, $(h_1,k_1)(h_2,k_2) = (h_1h_2, k_1k_2)$ and in $H \rtimes K$, $(h_1,h_2)(k_1,k_2) = (h_1\ k_1 \cdot h_2, k_1k_2)$. So it must be that $h_1h_2 = h_1\ k_1 \cdot h_2$, or $h_2 = k_1 \cdot h_2$. This must hold for all $h_2 \in H$, so $\varphi(k_1)$ must be the identity automorphism. Also, this holds for all $k_1 \in K$ and so it must be that $\varphi(k)$ is the identity automorphism for all $k \in K$. That is, φ is the trivial homomorphism from K to $\mathrm{Aut}(H)$.

Proposition DF.5.11 (continued 1)

Proposition DF.5.11. Let H and K be groups and let $\varphi : K \to \mathrm{Aut}(H)$ be a homomorphism. The following are equivalent.

(2) φ is the trivial homomorphism from K into $\mathrm{Aut}(H)$ (which maps all $k \in K$ to the identity automorphism).

(3) $K \trianglelefteq H \rtimes K$.

Proof (continued). (2) implies (3) If φ is the trivial homomorphism, then $\varphi(k)$ is the identity automorphism of H and $k \cdot h = h$ for all $h \in H$ and for all $k \in K$. By Theorem DF.10(5), $k \cdot h = khk^{-1}$, so $khk^{-1} = h$ for all $h \in H$, $k \in K$. So $kh = hk$ and the elements of H commute with the elements of K. Also H normalizes K (since $kh = hk$ for all $h \in H$, $k \in K$ implies $k = hkh^{-1}$ for all $h \in H$, $k \in K$ and hence $hKh^{-1} = K$ for all $h \in H$), and of course K normalizes itself. Let $g \in H \rtimes K$ and consider gkg^{-1}. We translate this into ordered pairs where, say, $g = (h_1, k_1)$ and $k = (1,k)$.

Proposition DF.5.11 (continued 2)

Proposition DF.5.11. Let H and K be groups and let $\varphi : K \to \mathrm{Aut}(H)$ be a homomorphism. The following are equivalent.

(2) φ is the trivial homomorphism from K into $\mathrm{Aut}(H)$ (which maps all $k \in K$ to the identity automorphism).

(3) $K \trianglelefteq H \rtimes K$.

Proof (continued). (2) implies (3) Then

$$\begin{aligned} gkg^{-1} &= (h_1, k_1)(1, k)(h_1, k_1)^{-1} \\ &= ((h_1, k_1)(1, k))(h_1, k_1)^{-1} \\ &= (h_1\ k_1 \cdot 1, k_1 k)(k_1^{-1} \cdot h_1, k_1^{-1}) \text{ by the definition of product} \\ &\quad \text{in } H \rtimes K \text{ and the formula for an inverse of } (h_1, k_1) \\ &\qquad \text{(see the proof of Theorem DF.10)} \\ &= (h_1\ 1, k_1 k)(h - 1^{-1}, k_1^{-1}) \text{ since the group action yields} \\ &\qquad \text{the identity automorphism} \\ &= (h_1\ (k_1 k) \cdot h_1^{-1}, k_1, k, k_1^{-1}) \text{ by the definition of product} \end{aligned}$$

Proposition DF.5.11 (continued 3)

Proposition DF.5.11. Let H and K be groups and let $\varphi : K \to \mathrm{Aut}(H)$ be a homomorphism. The following are equivalent.

(2) φ is the trivial homomorphism from K into $\mathrm{Aut}(H)$ (which maps all $k \in K$ to the identity automorphism).

(3) $K \trianglelefteq H \rtimes K$.

Proof (continued). (2) implies (3) Then

$$\begin{aligned} gkg^{-1} &= (h_1\ (k_1 k) \cdot h_1^{-1}, k_1, k, k_1^{-1}) \text{ by the definition of product} \\ &= (h_1 h_1^{-1}, k_1 k k_1^{-1}) \text{ since group action yields the} \\ &\qquad \text{identity automorphism} \\ &= (1, k_1 k k_1^{-1}) \in K. \end{aligned}$$

So $K \trianglelefteq H \rtimes K$ (again, we "identity" K and $\tilde{K}$) by Theorem I.5.1(iv).

Proposition DF.5.11 (continued 4)

Proposition DF.5.11. Let H and K be groups and let $\varphi : K \to \mathrm{Aut}(H)$ be a homomorphism. The following are equivalent.

(1) The identity set map between $H \rtimes K$ and $H \times K$ (both consisting of ordered pairs) is a group homomorphism (and hence $H \rtimes K \cong H \times K$).

(3) $K \trianglelefteq H \rtimes K$.

Proof. (3) implies (1) [The text, DF, uses a simplified notation when considering h, k, hk, etc. We use the ordered pair notation throughout this proof.] Notice that the commutator satisfies:

$$\begin{aligned} [h, k] &= [(h, 1), (1.k)] \text{ "identifying" as in Theorem DF.10} \\ &= (h, 1)^{-1}(1, k)^{-1}(h, 1)(1, k) \\ &= (1 \cdot h^{-1}, 1)(k^{-1} \cdot 1, k^{-1})(h, 1)(1, k) \\ &= (h^1, 1)(1, k)(h, 1)(1, k). \end{aligned}$$

Since $H \trianglelefteq H \rtimes K$ by Theorem DF.10(3), $(1, k)^{-1}(h, 1)(1, k) \in H$ and so $(h, 1)^{-1}(1, k)^{-1}(h, 1)(1, k) \in H$. That is, $[h, k] = [(h, 1), (1, k)] \in H$.

Proposition DF.5.11 (continued 5)

Proposition DF.5.11. Let H and K be groups and let $\varphi : K \to \mathrm{Aut}(H)$ be a homomorphism. The following are equivalent.

(1) The identity set map between $H \rtimes K$ and $H \times K$ (both consisting of ordered pairs) is a group homomorphism (and hence $H \rtimes K \cong H \times K$).

(3) $K \trianglelefteq H \rtimes K$.

Proof (continued). (3) implies (1) (continued) Similarly, since $K \trianglelefteq H \rtimes K$ by hypothesis, then $(h, 1)^{-1}(1, k)^{-1}(h, 1) \in K$ and so $(h, 1)^{-1}(1, k)^{-1}(h, 1)(1, k) \in K$. That is $[h, k] = [(h, 1)(1, k)] \in K$. Since $H \cap K = 1 = (1, 1)$ ("identifying") by Theorem DF.10(4), then

$$[h, k] = [(h, 1)(1, k)] = (h^{-1}, 1)(1, k^{-1})(h, 1)(1, k) = (1, 1).$$

This implies $(h, 1)(1, k) = (1, k)(h, 1)$ (or "identifying," $hk = kh$). Now $(h, 1)(1, k) = (h\ 1 \cdot 1, k) = (h, k)$ and $(1, k)(h, 1) = (1\ k \cdot h, k)$, since these are equal, we must have $k \cdot h = h$ for all $h \in H$, $k \in K$. That is, the action of K on H is the identity ($\varphi(k)(h) = h$).