

## 5.5 SEMIDIRECT PRODUCTS

In this section we study the “semidirect product” of two groups  $H$  and  $K$ , which is a generalization of the notion of the direct product of  $H$  and  $K$  obtained by relaxing the requirement that both  $H$  and  $K$  be normal. This construction will enable us (in certain circumstances) to build a “larger” group from the groups  $H$  and  $K$  in such a way that  $G$  contains subgroups isomorphic to  $H$  and  $K$ , respectively, as in the case of direct products. In this case the subgroup  $H$  will be normal in  $G$  but the subgroup  $K$  will not necessarily be normal (as it is for direct products). Thus, for instance, we shall be able to construct non-abelian groups even if  $H$  and  $K$  are abelian. This construction will allow us to enlarge considerably the set of examples of groups at our disposal. As in the preceding section, we shall then prove a recognition theorem that will enable us to decompose some familiar groups into smaller “factors,” from which we shall be able to derive some classification theorems.

By way of motivation suppose we already have a group  $G$  containing subgroups  $H$  and  $K$  such that

- (a)  $H \trianglelefteq G$  (but  $K$  is not necessarily normal in  $G$ ), and
- (b)  $H \cap K = 1$ .

It is still true that  $HK$  is a subgroup of  $G$  (Corollary 3.15) and, by Proposition 8, every element of  $HK$  can be written uniquely as a product  $hk$ , for some  $h \in H$  and  $k \in K$ , i.e., there is a bijection between  $HK$  and the collection of ordered pairs  $(h, k)$ , given by  $hk \mapsto (h, k)$  (so the group  $H$  appears as the set of elements  $(h, 1)$  and  $K$  appears as the set of elements  $(1, k)$ ). Given two elements  $h_1k_1$  and  $h_2k_2$  of  $HK$ , we first see how to write their product (in  $G$ ) in the same form:

$$\begin{aligned}(h_1k_1)(h_2k_2) &= h_1k_1h_2(k_1^{-1}k_1)k_2 \\&= h_1(k_1h_2k_1^{-1})k_1k_2 \\&= h_3k_3,\end{aligned}\tag{5.1}$$

where  $h_3 = h_1(k_1h_2k_1^{-1})$  and  $k_3 = k_1k_2$ . Note that since  $H \trianglelefteq G$ ,  $k_1h_2k_1^{-1} \in H$ , so  $h_3 \in H$  and  $k_3 \in K$ .

These calculations were predicated on the assumption that there *already existed* a group  $G$  containing subgroups  $H$  and  $K$  with  $H \trianglelefteq G$  and  $H \cap K = 1$ . The basic idea of the semidirect product is to turn this construction around, namely start with two (abstract) groups  $H$  and  $K$  and try to *define* a group containing (an isomorphic copy of) them in such a way that (a) and (b) above hold. To do this, we write equation (1), which defines the multiplication of elements in our group, in a way that makes sense even if we do not already know there is a group containing  $H$  and  $K$  as above. The point is that  $k_3$  in equation (1) is obtained only from multiplication in  $K$  (namely  $k_1k_2$ ) and  $h_3$  is obtained from multiplying  $h_1$  and  $k_1h_2k_1^{-1}$  in  $H$ . If we can understand where the element  $k_1h_2k_1^{-1}$  arises (in terms of  $H$  and  $K$  and without reference to  $G$ ), then the group  $HK$  will have been described entirely in terms of  $H$  and  $K$ . We can then use this description to *define* the group  $HK$  using equation (1) to define the multiplication.

Since  $H$  is normal in  $G$ , the group  $K$  acts on  $H$  by conjugation:

$$k \cdot h = khk^{-1} \quad \text{for } h \in H, k \in K$$

(we use the symbol  $\cdot$  to emphasize the action) so that (1) can be written

$$(h_1 k_1)(h_2 k_2) = (h_1 k_1 \cdot h_2)(k_1 k_2). \quad (5.2)$$

The action of  $K$  on  $H$  by conjugation gives a homomorphism  $\varphi$  of  $K$  into  $\text{Aut}(H)$ , so (2) shows that the multiplication in  $HK$  depends only on the multiplication in  $H$ , the multiplication in  $K$  and the homomorphism  $\varphi$ , hence is defined intrinsically in terms of  $H$  and  $K$ .

We now use this interpretation to define a group given two groups  $H$  and  $K$  and a homomorphism  $\varphi$  from  $K$  to  $\text{Aut}(H)$  (which will turn out to define conjugation in the resulting group).

**Theorem 10.** Let  $H$  and  $K$  be groups and let  $\varphi$  be a homomorphism from  $K$  into  $\text{Aut}(H)$ . Let  $\cdot$  denote the (left) action of  $K$  on  $H$  determined by  $\varphi$ . Let  $G$  be the set of ordered pairs  $(h, k)$  with  $h \in H$  and  $k \in K$  and define the following multiplication on  $G$ :

$$(h_1, k_1)(h_2, k_2) = (h_1 k_1 \cdot h_2, k_1 k_2).$$

- (1) This multiplication makes  $G$  into a group of order  $|G| = |H||K|$ .
- (2) The sets  $\{(h, 1) \mid h \in H\}$  and  $\{(1, k) \mid k \in K\}$  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 the groups  $H$  and  $K$  respectively:

$$H \cong \{(h, 1) \mid h \in H\} \quad \text{and} \quad K \cong \{(1, k) \mid k \in K\}.$$

Identifying  $H$  and  $K$  with their isomorphic copies in  $G$  described in (2) we have

- (3)  $H \trianglelefteq G$
- (4)  $H \cap K = 1$
- (5) for all  $h \in H$  and  $k \in K$ ,  $khk^{-1} = k \cdot h = \varphi(k)(h)$ .

*Proof:* It is straightforward to check that  $G$  is a group under this multiplication using the fact that  $\cdot$  is an action of  $K$  on  $H$ . For example, the associative law is verified as follows:

$$\begin{aligned} ((a, x)(b, y))(c, z) &= (a x \cdot b, xy)(c, z) \\ &= (a x \cdot b (xy) \cdot c, xyz) \\ &= (a x \cdot b x \cdot (y \cdot c), xyz) \\ &= (a x \cdot (b y \cdot c), xyz) \\ &= (a, x)(b y \cdot c, yz) \\ &= (a, x)((b, y)(c, z)) \end{aligned}$$

for all  $(a, x), (b, y), (c, z) \in G$ . We leave as an exercise the verification that (1,1) is the identity of  $G$  and that

$$(h, k)^{-1} = (k^{-1} \cdot h^{-1}, k^{-1})$$

for each  $(h, k) \in G$ . The order of the group  $G$  is clearly the product of the orders of  $H$  and  $K$ , which proves (1).

Let  $\tilde{H} = \{(h, 1) \mid h \in H\}$  and  $\tilde{K} = \{(1, k) \mid k \in K\}$ . We have

$$(a, 1)(b, 1) = (a \cdot b, 1) = (ab, 1)$$

for all  $a, b \in H$  and

$$(1, x)(1, y) = (1, xy)$$

for all  $x, y \in K$ , which show that  $\tilde{H}$  and  $\tilde{K}$  are subgroups of  $G$  and that the maps in (2) are isomorphisms.

It is clear that  $\tilde{H} \cap \tilde{K} = 1$ , which is (4). Now,

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

so that identifying  $(h, 1)$  with  $h$  and  $(1, k)$  with  $k$  by the isomorphisms in (2) we have  $khk^{-1} = k \cdot h$ , which is (5).

Finally, we have just seen that (under the identifications in (2))  $K \leq N_G(H)$ . Since  $G = HK$  and certainly  $H \leq N_G(H)$ , we have  $N_G(H) = G$ , i.e.,  $H \trianglelefteq G$ , which proves (3) and completes the proof.

**Definition.** Let  $H$  and  $K$  be groups and let  $\varphi$  be a homomorphism from  $K$  into  $\text{Aut}(H)$ . The group described in Theorem 10 is called the *semidirect product* of  $H$  and  $K$  with respect to  $\varphi$  and will be denoted by  $H \rtimes_{\varphi} K$  (when there is no danger of confusion we shall simply write  $H \rtimes K$ ).

The notation is chosen to remind us that the copy of  $H$  in  $H \rtimes K$  is the normal “factor” and that the construction of a semidirect product is not symmetric in  $H$  and  $K$  (unlike that of a direct product). Before giving some examples we clarify exactly when the semidirect product of  $H$  and  $K$  is their direct product (in particular, we see that direct products are a special case of semidirect products). See also Exercise 1.

**Proposition 11.** Let  $H$  and  $K$  be groups and let  $\varphi : K \rightarrow \text{Aut}(H)$  be a homomorphism. Then the following are equivalent:

- (1) the identity (set) map between  $H \rtimes K$  and  $H \times K$  is a group homomorphism (hence an isomorphism)
- (2)  $\varphi$  is the trivial homomorphism from  $K$  into  $\text{Aut}(H)$
- (3)  $K \trianglelefteq H \rtimes K$ .

*Proof:* (1)  $\Rightarrow$  (2) By definition of the group operation in  $H \rtimes K$

$$(h_1, k_1)(h_2, k_2) = (h_1 k_1 \cdot h_2, k_1 k_2)$$

for all  $h_1, h_2 \in H$  and  $k_1, k_2 \in K$ . By assumption (1),  $(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2)$ . Equating the first factors of these ordered pairs gives  $k_1 \cdot h_2 = h_2$  for all  $h_2 \in H$  and all  $k_1 \in K$ , i.e.,  $K$  acts trivially on  $H$ . This is (2).

(2)  $\Rightarrow$  (3) If  $\varphi$  is trivial, then the action of  $K$  on  $H$  is trivial, so that the elements of  $H$  commute with those of  $K$  by Theorem 10(5). In particular,  $H$  normalizes  $K$ . Since  $K$  normalizes itself,  $G = HK$  normalizes  $K$ , which is (3).

(3)  $\Rightarrow$  (1) If  $K$  is normal in  $H \rtimes K$  then (as in the proof of Theorem 9) for all  $h \in H$  and  $k \in K$ ,  $[h, k] \in H \cap K = 1$ . Thus  $hk = kh$  and the action of  $K$  on  $H$  is trivial. The multiplication in the semidirect product is then the same as that in the direct product:

$$(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2)$$

for all  $h_1, h_2 \in H$  and  $k_1, k_2 \in K$ . This gives (1) and completes the proof.

## Examples

In all examples  $H$  and  $K$  are groups and  $\varphi$  is a homomorphism from  $K$  into  $\text{Aut}(H)$  with associated action of  $K$  on  $H$  denoted by a dot. Let  $G = H \rtimes K$  and as in Theorem 10 we identify  $H$  and  $K$  as subgroups of  $G$ . We shall use Propositions 4.16 and 4.17 to determine homomorphisms  $\varphi$  for some specific groups  $H$ . In each of the following examples the proof that  $\varphi$  is a homomorphism is easy (since  $K$  will often be cyclic) so the details are omitted.

- (1) Let  $H$  be any abelian group (even of infinite order) and let  $K = \langle x \rangle \cong \mathbb{Z}_2$  be the group of order 2. Define  $\varphi : K \rightarrow \text{Aut}(H)$  by mapping  $x$  to the automorphism of inversion on  $H$  so that the associated action is  $x \cdot h = h^{-1}$ , for all  $h \in H$ . Then  $G$  contains the subgroup  $H$  of index 2 and

$$xhx^{-1} = h^{-1} \quad \text{for all } h \in H.$$

Of particular interest is the case when  $H$  is cyclic: if  $H = \mathbb{Z}_n$ , one recognizes  $G$  as  $D_{2n}$  and if  $H = \mathbb{Z}$  we denote  $G$  by  $D_\infty$ .

- (2) We can generalize the preceding example in a number of ways. One way is to let  $H$  be any abelian group and to let  $K = \langle x \rangle \cong \mathbb{Z}_{2n}$  be cyclic of order  $2n$ . Define  $\varphi$  again by mapping  $x$  to inversion, so that  $x^2$  acts as the identity on  $H$ . In  $G$ ,  $xhx^{-1} = h^{-1}$  and  $x^2hx^{-2} = h$  for all  $h \in H$ . Thus  $x^2 \in Z(G)$ . In particular, if  $H = \mathbb{Z}_3$  and  $K = \mathbb{Z}_4$ ,  $G$  is a non-abelian group of order 12 which is not isomorphic to  $A_4$  or  $D_{12}$  (since its Sylow 2-subgroup,  $K$ , is cyclic of order 4).
- (3) Following up on the preceding example let  $H = \langle h \rangle \cong \mathbb{Z}_{2^n}$  and let  $K = \langle x \rangle \cong \mathbb{Z}_4$  with  $xhx^{-1} = h^{-1}$  in  $G$ . As noted above,  $x^2 \in Z(G)$ . Since  $x$  inverts  $h$  (i.e., inverts  $H$ ),  $x$  inverts the unique subgroup  $\langle z \rangle$  of order 2 in  $H$ , where  $z = h^{2^{n-1}}$ . Thus  $xzx^{-1} = z^{-1} = z$ , so  $x$  centralizes  $z$ . It follows that  $z \in Z(G)$ . Thus  $x^2z \in Z(G)$  hence  $\langle x^2z \rangle \trianglelefteq G$ . Let  $\bar{G} = G/\langle x^2z \rangle$ . Since  $x^2$  and  $z$  are distinct commuting elements of order 2, the order of  $x^2z$  is 2, so  $|\bar{G}| = \frac{1}{2}|G| = 2^{n+1}$ . By factoring out the product  $x^2z$  to form  $\bar{G}$  we identify  $x^2$  and  $h^{2^{n-1}}$  in the quotient. In particular, when  $n = 2$ , both  $\bar{x}$  and  $\bar{h}$  have order 4,  $\bar{x}$  inverts  $\bar{h}$  and  $\bar{h}^2 = \bar{x}^2$ . It follows that  $\bar{G} \cong Q_8$  in this case. In general, one can check that  $\bar{G}$  has a unique subgroup of order 2 (namely  $\langle \bar{x}^2 \rangle$ ) which equals the center of  $\bar{G}$ . The group  $\bar{G}$  is called the *generalized quaternion group* of order  $2^{n+1}$  and is denoted by  $Q_{2^{n+1}}$ :

$$Q_{2^{n+1}} = \langle h, x \mid h^{2^n} = x^4 = 1, x^{-1}hx = h^{-1}, h^{2^{n-1}} = x^2 \rangle.$$

- (4) Let  $H = \mathbb{Q}$  (under addition) and let  $K = \langle x \rangle \cong \mathbb{Z}$ . Define  $\varphi$  by mapping  $x$  to the map “multiplication by 2” on  $H$ , so that  $x$  acts on  $h \in H$  by  $x \cdot h = 2h$ . Note that multiplication by 2 is an automorphism of  $H$  because it has a 2-sided inverse, namely