

Dr. H. Joseph Straight  
SUNY Fredonia

*Smokin' Joe's Catalog of Groups: Direct Products and Semi-direct Products*

One of the fundamental problems in group theory is to catalog all the groups of some given order  $n$ . For example, suppose  $n = 12$ . How many different groups of order 12 are there? And what do we mean by “different.”

One way to attack the problem is to generate examples of groups of order  $n$ , decide which ones are “different” and which are the “same,” and then show that all the different examples form a complete collection of the groups of order  $n$ . In this regard, it is useful to have a way to generate groups of larger order from known groups of smaller order.

The *direct product* and the *semi-direct product* are operations on groups. Each provides a way to construct a “new” group  $G$  from two given groups  $G_1$  and  $G_2$ . In fact, if  $G_1$  and  $G_2$  are finite, then the order of  $G$  is the product of the orders of  $G_1$  and  $G_2$ . Thus, if we are interested in producing groups of order 12, for example, we might try forming the direct product of a group of order 6 with a group of order 2, or we might form the semi-direct product of a group of order 4 with a group of order 3.

**Definition 1:** Let  $(G_1, *)$  and  $(G_2, \bullet)$  be two groups. The (*external*) *direct product* of  $G_1$  with  $G_2$  is the group  $G = G_1 \times G_2$ , with the operation on  $G$  defined by

$$(x_1, x_2)(y_1, y_2) = (x_1 * y_1, x_2 \bullet y_2) \quad \clubsuit$$



So the idea is this. To find the direct product of group  $G_1$  with group  $G_2$ , we form the set of all ordered pairs  $(x_1, x_2)$ , with  $x_1 \in G_1$  and  $x_2 \in G_2$ . Then, to “multiply” the two ordered pairs  $(x_1, x_2)$  and  $(y_1, y_2)$ , we form the ordered pair  $(x_1 y_1, x_2 y_2)$ , with the first coordinate  $x_1 y_1$  being the “product” of the first coordinates  $x_1$  and  $y_1$  in  $G_1$ , and the second coordinate  $x_2 y_2$  being the “product” of the second coordinates  $x_2$  and  $y_2$  in  $G_2$ .

When the operations in  $G_1$  and  $G_2$  are considered to be “addition,” some texts denote  $G_1 \times G_2$  by  $G_1 \oplus G_2$ , and call  $G_1 \oplus G_2$  the *direct sum* of  $G_1$  with  $G_2$ . We'll stick with the “direct product” terminology and the notation  $G_1 \times G_2$ . However, when the operations in  $G_1$  and  $G_2$  are considered to be “addition,” we will write  $\clubsuit$  above as

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$$

**Example 1:** Find the direct product of

(a)  $\mathbb{Z}_6$  with  $\mathbb{Z}_2$

(b)  $D_3$  with  $\mathbb{Z}_2$

**Solution:** Recall that:

$$\mathbb{Z}_2 = \{0, 1\}, \text{ with the operation being addition modulo 2}$$

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}, \text{ with the operation being addition modulo 6}$$

$$D_3 = \langle r, s \mid |r| = 3, |s| = 2, sr = r^2s \rangle$$

(a) Thus,

$$\mathbb{Z}_6 \times \mathbb{Z}_2 = \{(0, 0), (0, 1), (1, 0), (1, 1), (2, 0), (2, 1), (3, 0), (3, 1), (4, 0), (4, 1), (5, 0), (5, 1)\}$$

The operation table for  $\mathbb{Z}_6 \times \mathbb{Z}_2$  is shown below. To “add” two ordered pairs, we add the first coordinates using addition modulo 6, and we add the second coordinates using addition modulo 2. For example,

$$(3, 1) + (5, 1) = ((3 + 5) \bmod 6, (1 + 1) \bmod 2) = (2, 0)$$

Note that the group  $\mathbb{Z}_6 \times \mathbb{Z}_2$  is abelian.

+	(0, 0)	(0, 1)	(1, 0)	(1, 1)	(2, 0)	(2, 1)	(3, 0)	(3, 1)	(4, 0)	(4, 1)	(5, 0)	(5, 1)
(0, 0)	(0, 0)	(0, 1)	(1, 0)	(1, 1)	(2, 0)	(2, 1)	(3, 0)	(3, 1)	(4, 0)	(4, 1)	(5, 0)	(5, 1)
(0, 1)	(0, 1)	(0, 0)	(1, 1)	(1, 0)	(2, 1)	(2, 0)	(3, 1)	(3, 0)	(4, 1)	(4, 0)	(5, 1)	(5, 0)
(1, 0)	(1, 0)	(1, 1)	(2, 0)	(2, 1)	(3, 0)	(3, 1)	(4, 0)	(4, 1)	(5, 0)	(5, 1)	(0, 0)	(0, 1)
(1, 1)	(1, 1)	(1, 0)	(2, 1)	(2, 0)	(3, 1)	(3, 0)	(4, 1)	(4, 0)	(5, 1)	(5, 0)	(0, 1)	(0, 0)
(2, 0)	(2, 0)	(2, 1)	(3, 0)	(3, 1)	(4, 0)	(4, 1)	(5, 0)	(5, 1)	(0, 0)	(0, 1)	(1, 0)	(1, 1)
(2, 1)	(2, 1)	(2, 0)	(3, 1)	(3, 0)	(4, 1)	(4, 0)	(5, 1)	(5, 0)	(0, 1)	(0, 0)	(1, 1)	(1, 0)
(3, 0)	(3, 0)	(3, 1)	(4, 0)	(4, 1)	(5, 0)	(5, 1)	(0, 0)	(0, 1)	(1, 0)	(1, 1)	(2, 0)	(2, 1)
(3, 1)	(3, 1)	(3, 0)	(4, 1)	(4, 0)	(5, 1)	(5, 0)	(0, 1)	(0, 0)	(1, 1)	(1, 0)	(2, 1)	(2, 0)
(4, 0)	(4, 0)	(4, 1)	(5, 0)	(5, 1)	(0, 0)	(0, 1)	(1, 0)	(1, 1)	(2, 0)	(2, 1)	(3, 0)	(3, 1)
(4, 1)	(4, 1)	(4, 0)	(5, 1)	(5, 0)	(0, 1)	(0, 0)	(1, 1)	(1, 0)	(2, 1)	(2, 0)	(3, 1)	(3, 0)
(5, 0)	(5, 0)	(5, 1)	(0, 0)	(0, 1)	(1, 0)	(1, 1)	(2, 0)	(2, 1)	(3, 0)	(3, 1)	(4, 0)	(4, 1)
(5, 1)	(5, 1)	(5, 0)	(0, 1)	(0, 0)	(1, 1)	(1, 0)	(2, 1)	(2, 0)	(3, 1)	(3, 0)	(4, 1)	(4, 0)

(b) The operation table for  $D_3 \times \mathbb{Z}_2$  is shown below. To “multiply” two ordered pairs, we multiply the first coordinates using the operation in  $D_3$ , and we add the second coordinates using addition modulo 2. Note that, since  $D_3$  is nonabelian,  $D_3 \times \mathbb{Z}_2$  is nonabelian; for example,  $(a, 0)(b, 0) = (ab, 0)$ , whereas  $(b, 0)(a, 0) = (ba, 0) = (a^2b, 0)$ . ■

Operation table for  $D_3 \times \mathbb{Z}_2$ :

	$(e, 0)$	$(e, 1)$	$(r, 0)$	$(r, 1)$	$(r^2, 0)$	$(r^2, 1)$	$(s, 0)$	$(s, 1)$	$(rs, 0)$	$(rs, 1)$	$(r^2s, 0)$	$(r^2s, 1)$
$(e, 0)$	$(e, 0)$	$(e, 1)$	$(r, 0)$	$(r, 1)$	$(r^2, 0)$	$(r^2, 1)$	$(s, 0)$	$(s, 1)$	$(rs, 0)$	$(rs, 1)$	$(r^2s, 0)$	$(r^2s, 1)$
$(e, 1)$	$(e, 1)$	$(e, 0)$	$(r, 1)$	$(r, 0)$	$(r^2, 1)$	$(r^2, 0)$	$(s, 1)$	$(s, 0)$	$(rs, 1)$	$(rs, 0)$	$(r^2s, 1)$	$(r^2s, 0)$
$(r, 0)$	$(r, 0)$	$(r, 1)$	$(r^2, 0)$	$(r^2, 1)$	$(e, 0)$	$(e, 1)$	$(rs, 0)$	$(rs, 1)$	$(r^2s, 0)$	$(r^2s, 1)$	$(s, 0)$	$(s, 1)$
$(r, 1)$	$(r, 1)$	$(r, 0)$	$(r^2, 1)$	$(r^2, 0)$	$(e, 1)$	$(e, 0)$	$(rs, 1)$	$(rs, 0)$	$(r^2s, 1)$	$(r^2s, 0)$	$(r, 1)$	$(r, 0)$
$(r^2, 0)$	$(r^2, 0)$	$(r^2, 1)$	$(e, 0)$	$(e, 1)$	$(r, 0)$	$(r, 1)$	$(r^2s, 0)$	$(r^2s, 1)$	$(s, 0)$	$(s, 1)$	$(rs, 0)$	$(rs, 1)$
$(r^2, 1)$	$(r^2, 1)$	$(r^2, 0)$	$(e, 1)$	$(e, 0)$	$(r, 1)$	$(r, 0)$	$(r^2s, 1)$	$(r^2s, 0)$	$(s, 1)$	$(s, 0)$	$(rs, 1)$	$(rs, 0)$
$(s, 0)$	$(s, 0)$	$(s, 1)$	$(r^2s, 0)$	$(r^2s, 1)$	$(rs, 0)$	$(rs, 1)$	$(e, 0)$	$(e, 1)$	$(r^2, 0)$	$(r^2, 1)$	$(r, 0)$	$(r, 1)$
$(s, 1)$	$(s, 1)$	$(s, 0)$	$(r^2s, 1)$	$(r^2s, 0)$	$(rs, 1)$	$(rs, 0)$	$(e, 1)$	$(e, 0)$	$(r^2, 1)$	$(r^2, 0)$	$(r, 1)$	$(r, 0)$
$(rs, 0)$	$(rs, 0)$	$(rs, 1)$	$(s, 0)$	$(s, 1)$	$(r^2s, 0)$	$(r^2s, 1)$	$(r, 0)$	$(r, 1)$	$(e, 0)$	$(e, 1)$	$(r^2, 0)$	$(r^2, 1)$
$(rs, 1)$	$(rs, 1)$	$(rs, 0)$	$(s, 1)$	$(s, 0)$	$(r^2s, 1)$	$(r^2s, 0)$	$(r, 1)$	$(r, 0)$	$(e, 1)$	$(e, 0)$	$(r^2, 1)$	$(r^2, 0)$
$(r^2s, 0)$	$(r^2s, 0)$	$(r^2s, 1)$	$(rs, 0)$	$(rs, 1)$	$(s, 0)$	$(s, 1)$	$(r^2, 0)$	$(r^2, 1)$	$(r, 0)$	$(r, 1)$	$(e, 0)$	$(e, 1)$
$(r^2s, 1)$	$(r^2s, 1)$	$(r^2s, 0)$	$(rs, 1)$	$(rs, 0)$	$(s, 1)$	$(s, 0)$	$(r^2, 1)$	$(r^2, 0)$	$(r, 1)$	$(r, 0)$	$(e, 1)$	$(e, 0)$

**Theorem 1:** Let  $G_1$  and  $G_2$  be two groups, with identity elements  $e_1$  and  $e_2$ , respectively. Then:

1. The identity element of the group  $G_1 \times G_2$  is  $(e_1, e_2)$ .
2. The group  $G_1 \times G_2$  is abelian if and only if both  $G_1$  and  $G_2$  are abelian.
3. For  $x_1 \in G_1$  and  $x_2 \in G_2$ ,

$$(x_1, x_2)^{-1} = (x_1^{-1}, x_2^{-1})$$

4. If  $x_1$  has finite order in  $G_1$  and  $x_2$  has finite order in  $G_2$  — in particular, if both  $G_1$  and  $G_2$  are finite, then  $(x_1, x_2)$  has finite order in  $G_1 \times G_2$ ; in fact,

$$|(x_1, x_2)| = \text{lcm}(|x_1|, |x_2|)$$

**Proof:** We prove part 4 and leave the remaining parts to Exercise 2.

Let  $G_1$  and  $G_2$  be two groups, with identity elements  $e_1$  and  $e_2$ , respectively, and assume  $x_1$  has order  $n_1$  in  $G_1$  and  $x_2$  has order  $n_2$  in  $G_2$ . Let  $m = \text{lcm}(n_1, n_2)$ , with  $k_1 = m/n_1$  and  $k_2 = m/n_2$ . Then

$$(x_1, x_2)^m = (x_1^m, x_2^m) = (x_1^{k_1 n_1}, x_2^{k_2 n_2}) = \left( (x_1^{n_1})^{k_1}, (x_2^{n_2})^{k_2} \right) = (e_1^{k_1}, e_2^{k_2}) = (e_1, e_2)$$

Next, let  $t$  be a positive integer, and suppose  $(x_1, x_2)^t = (e_1, e_2)$ . To complete the proof, we must show that  $t$  is a multiple of  $m$ . To that end, let  $r = t \bmod m$ , with  $t = mq + r$ . We want to show that  $r = 0$ . Well,

$$(e_1, e_2) = (x_1, x_2)^t = (x_1^t, x_2^t) = \cdots = (x_1^r, x_2^r)$$

**(Exercise:** Fill in the missing steps above.) Thus,  $x_1^r = e_1$  and  $x_2^r = e_2$ . Hence,  $r$  is a multiple of  $n_1$  and  $r$  is a multiple of  $n_2$ ; that is,  $r$  is a common multiple of  $n_1$  and  $n_2$ . Since  $m$  is the least (positive) common multiple of  $n_1$  and  $n_2$ , this forces  $r$  to be 0, as we wished to show. ■

Armed with Theorem 1, let's see how many different groups of order 12 we can come up with. Right off the top we have two examples,  $\mathbb{Z}_{12}$  and  $D_6$ . These are certainly different, since  $\mathbb{Z}_{12}$  is abelian (in fact, it's cyclic) and  $D_6$  is nonabelian.

What about  $\mathbb{Z}_6 \times \mathbb{Z}_2$  and  $\mathbb{Z}_4 \times \mathbb{Z}_3$ ? Both of these groups are abelian, so the question is, "Are the groups  $\mathbb{Z}_{12}$ ,  $\mathbb{Z}_6 \times \mathbb{Z}_2$ , and  $\mathbb{Z}_4 \times \mathbb{Z}_3$  three different groups?"

Suppose we have two groups  $G_1$  and  $G_2$ , both of order  $n$ , and some factor  $k$  of  $n$ . Suppose the number of elements in  $G_1$  of order  $k$  is different than the number of elements in  $G_2$  of order  $k$ . Then it seems reasonable to say that the groups  $G_1$  and  $G_2$  are different.

**Example 2:** For each of the following groups of order 12, find the number of elements of order 1, 2, 3, 4, 6, and 12.

(a)  $\mathbb{Z}_{12}$

(b)  $\mathbb{Z}_6 \times \mathbb{Z}_2$

(c)  $\mathbb{Z}_4 \times \mathbb{Z}_3$

**Solution:**

(a) Refer to Theorem 8 in *Cyclic Groups*. This result states that, if  $g$  is a generator for a cyclic group of order  $n$ , then, for  $0 \leq k < n$ ,

$$|g^k| = \frac{n}{\gcd(k, n)}$$

If we interpret this result in the context of  $\mathbb{Z}_n$ , we see that, for  $0 \leq k < n$ ,

$$|k| = \frac{n}{\gcd(k, n)}$$

This is Corollary 9 in *Cyclic Groups*. Also there, we find Theorem 10, which tells us that  $\mathbb{Z}_n$  has  $\phi(m)$  elements of order  $m$  for each positive factor  $m$  of  $n$ .

Applying these results to  $\mathbb{Z}_{12}$ , we obtain the following table:

order	elements	number
1	0	1
2	6	1
3	4, 8	2
4	3, 9	2
6	2, 10	2
12	1, 5, 7, 11	4
total		12

(b) For  $\mathbb{Z}_6 \times \mathbb{Z}_2$ , let's find the order of each element. In  $\mathbb{Z}_6$ , 0 has order 1, the element 3 has order 2, the elements 2 and 4 have order 3, and the elements 1 and 5 have order 6. In  $\mathbb{Z}_2$ , 0 has order 1 and the element 1 has order 2. Now apply Theorem 1, part 4, to obtain the following table:

$(x, y)$	$ x $	$ y $	$ (x, y)  = \text{lcm}( x ,  y )$
(0, 0)	1	1	1
(3, 0)	2	1	2
(2, 0), (4, 0)	3	1	3
(1, 0), (5, 0)	6	1	6
(0, 1)	1	2	2
(3, 1)	2	2	2
(2, 1), (4, 1)	3	2	6
(1, 1), (5, 1)	6	2	6

The results are summarized in the following table:

order	elements	number
1	(0, 0)	1
2	(3, 0), (0, 1), (3, 1)	3
3	(2, 0), (4, 0)	2
4	none	0
6	(1, 0), (5, 0), (2, 1), (4, 1), (1, 1), (5, 1)	6
12	none	0
total		12

Comparing the order results for  $\mathbb{Z}_{12}$  and  $\mathbb{Z}_6 \times \mathbb{Z}_2$ , we can say that these two groups are definitely different; in particular,  $\mathbb{Z}_6 \times \mathbb{Z}_2$  is not cyclic.

(c) **Exercise:** Verify the following results for  $\mathbb{Z}_4 \times \mathbb{Z}_3$ :

order	elements	number
1	(0, 0)	1
2	(2, 0)	1
3	(0, 1), (0, 2)	2
4	(1, 0), (3, 0)	2
6	(2, 1), (2, 2)	2
12	(1, 1), (1, 2), (3, 1), (3, 2)	4
total		12

Thus, for each factor  $k$  of 12, the groups  $\mathbb{Z}_{12}$  and  $\mathbb{Z}_4 \times \mathbb{Z}_3$  have the same number of elements of order  $k$ . Very interesting!

■

Since  $\mathbb{Z}_4 \times \mathbb{Z}_3$  has an element of order 12 (four of them, in fact), it is a cyclic group, just like  $\mathbb{Z}_{12}$ . For  $\mathbb{Z}_{12}$ , 1 is a generator, and for  $\mathbb{Z}_4 \times \mathbb{Z}_3$ , (1, 1) is a generator, and we have the following table of powers of (1, 1):

$x$	$(1, 1)^x$
0	(0, 0)
1	(1, 1)
2	(2, 2)
3	(3, 0)
4	(0, 1)
5	(1, 2)
6	(2, 0)
7	(3, 1)
8	(0, 2)
9	(1, 0)
10	(2, 1)
11	(3, 2)

Note that, in  $\mathbb{Z}_4 \times \mathbb{Z}_3$ ,  $(1, 1)^x = (x \bmod 4, x \bmod 3)$ . Thus, as  $x$  runs through the values  $0, 1, 2, \dots$ , the first coordinate of  $(1, 1)^x$  cycles through the four values  $0, 1, 2, 3$ , while the second coordinate of  $(1, 1)^x$  cycles through the three values  $0, 1, 2$ . Hence, since 4 and 3 are relatively prime,  $(1, 1)^x$  cycles through all twelve elements of  $\mathbb{Z}_4 \times \mathbb{Z}_3$  before repeating; that is, for  $0 \leq x \leq y$ ,

$$(1, 1)^x = (1, 1)^y \iff y - x \text{ is a multiple of } 12$$

Adding ordered pairs in the group  $\mathbb{Z}_4 \times \mathbb{Z}_3$  isn't difficult, but most of us would rather perform addition modulo 12 instead. The one-to-one correspondence between the elements of  $\mathbb{Z}_{12}$  and the elements of  $\mathbb{Z}_4 \times \mathbb{Z}_3$  provided by the table above allows us to do this. For example, suppose we want to add the ordered pairs  $(3, 1)$  and  $(2, 1)$ . Since  $(3, 1)$  corresponds to 7 and  $(2, 1)$  corresponds to 10, we can instead add 7 and 10 in  $\mathbb{Z}_{12}$ . This yields 5. Then we note that 5 corresponds to the ordered pair  $(1, 2)$ . Therefore, in  $\mathbb{Z}_4 \times \mathbb{Z}_3$ ,  $(3, 1) + (2, 1) = (1, 2)$ . Symbolically,

$$(3, 1) + (2, 1) \equiv 7 + 10 = 17 \bmod 12 = 5 \equiv (1, 2)$$

where the symbol “ $\equiv$ ” means “corresponds to.” In general we have,

$$(1, 1)^x + (1, 1)^y \equiv (x + y) \bmod 12 \equiv (1, 1)^{(x+y) \bmod 12}$$

In this sense, the groups  $\mathbb{Z}_{12}$  and  $\mathbb{Z}_4 \times \mathbb{Z}_3$  are structurally the same. Mathematically, we say that the two groups are *isomorphic*.

In general, two groups  $(G, *)$  and  $(\overline{G}, \overline{*})$  are *isomorphic* provided there is a one-to-one correspondence between  $G$  and  $\overline{G}$ , with an arbitrary element  $x$  in  $G$  corresponding to  $\overline{x}$  in  $\overline{G}$ , such that:

(1) If one needs to compute  $\overline{x} \overline{*} \overline{y}$  in  $\overline{G}$ , and one would rather perform the operation  $*$  in  $G$ , then

$$\overline{x} \overline{*} \overline{y} \equiv x * y = z \equiv \overline{z}$$

(2) Or, if one needs to compute  $x * y$  in  $G$ , and one would rather perform the operation  $\overline{*}$  in  $\overline{G}$ , then

$$x * y \equiv \overline{x} \overline{*} \overline{y} = \overline{z} \equiv z$$

Formally, we have the following definition.

**Definition 2:** Two groups  $G_1$  and  $G_2$  are *isomorphic* provided there is a bijection  $\phi : G_1 \rightarrow G_2$  such that

$$\phi(x_1 y_1) = \phi(x_1) \phi(y_1)$$

for all  $x_1, y_1 \in G_1$ . In this context, the function  $\phi$  is called an *isomorphism*. We denote the fact that  $G_1$  and  $G_2$  are isomorphic groups by writing  $G_1 \cong G_2$ . ■

**Example 3:** The group  $D_6$  is a nonabelian group of order 12, as is the group  $D_3 \times \mathbb{Z}_2$ . Determine whether these groups are isomorphic or not.

**Solution:** To avoid confusion, let's use  $r$  and  $s$  to name the generators for  $D_3$  and  $c$  and  $d$  to name the generators for  $D_6$ . Also, let  $e$  and  $f$  denote the identity elements in  $D_3$  and  $D_6$ , respectively. So,

$$\begin{aligned} D_3 &= \langle r, s \mid |r| = 3, |s| = 2, sr = r^2 s \rangle, \text{ and} \\ D_6 &= \langle c, d \mid |c| = 6, |d| = 2, d \notin \langle c \rangle, dc = c^5 d \rangle \end{aligned}$$

We begin by computing orders of elements. The results of this are shown in the tables on the next page.

For  $D_6$ :

order	elements	number
1	$f$	1
2	$c^3, d, cd, c^2d, c^3d, c^4d, c^5d$	7
3	$c^2, c^4$	2
4	none	0
6	$c, c^5$	2
12	none	0
total		12

For  $D_3 \times \mathbb{Z}_2$ :

order	elements	number
1	$(e, 0)$	1
2	$(e, 1), (s, 0), (s, 1), (rs, 0), (rs, 1), (r^2s, 0), (r^2s, 1)$	7
3	$(r, 0), (r^2, 0)$	2
4	none	0
6	$(r, 1), (r^2, 1)$	2
12	none	0
total		12

Thus, both  $D_6$  and  $D_3 \times \mathbb{Z}_2$  have one element of order 1, seven elements of order 2, two elements of order 3, and two elements of order 6, so they may be isomorphic. Let's see if we can construct an isomorphism  $\phi : D_6 \rightarrow D_3 \times \mathbb{Z}_2$ .

Now, the group  $D_6$  is generated by the elements  $c$  and  $d$ , so a candidate isomorphism  $\phi$  is completely determined by the images  $\phi(c)$  and  $\phi(d)$ . For example, given  $\phi(c)$  and  $\phi(d)$ , we have that

$$\phi(c^2d) = \phi(c^2)\phi(d) = (\phi(c)\phi(c))\phi(d) = (\phi(c))^2\phi(d)$$

Likewise, an isomorphism should “preserve order.” For instance, since  $c$  has order 6 and  $d$  has order 2 in  $D_6$ , their images  $\phi(c)$  and  $\phi(d)$  should have order 6 and 2, respectively, in  $D_3 \times \mathbb{Z}_2$ .

Thus, let's try letting

$$\phi(c) = (r, 1) \quad \text{and} \quad \phi(d) = (s, 0)$$

**Exercise:** Using the defining property of an isomorphism, namely, that

$$\phi(xy) = \phi(x)\phi(y)$$

complete the following table:

$x \in D_6$	$\phi(x) \in D_3 \times \mathbb{Z}_2$
$f$	$e$
$c$	$(r, 1)$
$c^2$	
$c^3$	
$c^4$	
$c^5$	
$d$	$(s, 0)$
$cd$	
$c^2d$	
$c^3d$	
$c^4d$	
$c^5d$	

Again,  $D_6$  is generated by  $c$  and  $d$ , with  $c$  having order 6,  $d$  having order 2, and with the additional rule that  $dc = c^5d$ . We have defined  $\phi$  so that  $\phi(c) = (a, 1)$  has order 6 and  $\phi(d) = (b, 0)$  has order 2. Thus, to check that  $\phi$  is indeed an isomorphism, it suffices to check that

$$\phi(d)\phi(c) = (\phi(c))^5\phi(d)$$

**Exercise:** Check that the above relation holds.



**Theorem 2:** Let  $G_1$  and  $G_2$  be groups, with identity elements  $e_1$  and  $e_2$ , respectively. If  $G_1$  and  $G_2$  are isomorphic and  $\phi : G_1 \rightarrow G_2$  is an isomorphism, then:

1.  $\phi(e_1) = e_2$ .
2. For every element  $x \in G_1$ ,  $\phi(x^{-1}) = (\phi(x))^{-1}$ .
3. For  $x, y \in G_1$ ,  $xy = yx$  in  $G_1$  if and only if  $\phi(x)\phi(y) = \phi(y)\phi(x)$  in  $G_2$ . Hence,  $G_1$  is abelian if and only if  $G_2$  is abelian.
4. For every element  $x \in G_1$  and any nonnegative integer  $n$ ,  $\phi(x^n) = (\phi(x))^n$ .
5. For every element  $x \in G_1$ ,  $x$  has finite order in  $G_1$  if and only if  $\phi(x)$  has finite order in  $G_2$ . Moreover, if  $x$  has finite order in  $G_1$ , then  $|\phi(x)| = |x|$ .
6. If  $H$  is a subgroup of  $G_1$ , then  $\phi(H)$  is a subgroup of  $G_2$ . Moreover, if  $H$  is cyclic, then  $\phi(H)$  is cyclic.
7.  $\phi^{-1} : G_2 \rightarrow G_1$  is an isomorphism.

**Proof:** We prove parts 1, 2, and 6, and leave the remaining parts as exercises. Let  $G_1$  and  $G_2$  be groups, with identity elements  $e_1$  and  $e_2$ , respectively, and assume  $\phi : G_1 \rightarrow G_2$  is an isomorphism.

For 1,

$$(\phi(e_1))^2 = \phi(e_1)\phi(e_1) = \phi(e_1^2) = \phi(e_1)$$

It follows that  $\phi(e_1) = e_2$ .

For 2,

$$\phi(x)\phi(x^{-1}) = \phi(xx^{-1}) = \phi(e_1) = e_2$$

Therefore,  $(\phi(x))^{-1} = \phi(x^{-1})$ .

To prove 6, assume  $H$  is a subgroup of  $G_1$ , and let  $x_2, y_2 \in \phi(H)$ , with  $x_1, y_1 \in H$  such that  $\phi(x_1) = x_2$  and  $\phi(y_1) = y_2$ . First, since  $e_1 \in H$ ,  $e_2 = \phi(e_1) \in \phi(H)$ . Second, since  $x_1^{-1} \in H$ ,

$$x_2^{-1} = (\phi(x_1))^{-1} = \phi(x_1^{-1}) \in \phi(H)$$

This shows that  $\phi(H)$  is closed under inverses. Finally, since  $x_1 y_1 \in H$ ,

$$x_2 y_2 = \phi(x_1)\phi(y_1) = \phi(x_1 y_1) \in \phi(H)$$

This shows that  $\phi(H)$  is closed under the operation for  $G_2$ . Therefore,  $\phi(H) \leq G_2$ .

Moreover, if  $H$  is a cyclic subgroup of  $G_1$  and  $a$  is a generator for  $H$ , then it follows from part 4 that  $\phi(a)$  is a generator for  $\phi(H)$ ; hence,  $\phi(H)$  is a cyclic subgroup of  $G_2$ .

■

Let's return to the problem of cataloging the groups of order 12. We now know what this means. We want to make a list of groups of order 12 such that (1) no two groups on the list are isomorphic, and (2) any group of order 12 is isomorphic to one of the groups on the list. So far, we have the following partial list:

$$\mathbb{Z}_{12}, \quad \mathbb{Z}_6 \times \mathbb{Z}_2, \quad D_6$$

As additional candidates, we considered  $\mathbb{Z}_4 \times \mathbb{Z}_3$  and  $D_3 \times \mathbb{Z}_2$ . However, we saw that  $\mathbb{Z}_4 \times \mathbb{Z}_3 \cong \mathbb{Z}_{12}$  and  $D_3 \times \mathbb{Z}_2 \cong D_6$ .

What about  $\mathbb{Z}_3 \times \mathbb{Z}_4$ ? It should be fairly obvious that  $\mathbb{Z}_3 \times \mathbb{Z}_4 \cong \mathbb{Z}_4 \times \mathbb{Z}_3$ . In fact, in Exercise 4, you are asked to show that, for any two groups  $G_1$  and  $G_2$ ,

$$G_1 \times G_2 \cong G_2 \times G_1$$

Note that  $D_3 \times \mathbb{Z}_2$  is, up to isomorphism, the only nonabelian group of order 12 that is the direct product of two smaller groups. This is because  $D_3$  is the only nonabelian group of order 6, and any group of order less than 6 is abelian. There is, however, one additional direct product of abelian groups we can try, namely,  $K \times \mathbb{Z}_3$ , with  $K$  being the Klein four-group. Recall that

$$K = \langle a, b \mid |a| = 2 = |b|, b \neq a, ba = ab \rangle$$

**Example 4:** Determine whether  $K \times \mathbb{Z}_3$  is isomorphic to either  $\mathbb{Z}_{12}$  or  $\mathbb{Z}_6 \times \mathbb{Z}_2$ .

**Solution:** As usual, we begin by computing the orders of the elements in  $K \times \mathbb{Z}_3$ :

order	elements	number
1	$(e, 0)$	1
2	$(a, 0), (b, 0), (ab, 0)$	3
3	$(e, 1), (e, 2)$	2
4	none	0
6	$(a, 1), (a, 2), (b, 1), (b, 2), (ab, 1), (ab, 2)$	6
12	none	0
total		12

**Exercise:** Finish the solution, showing that  $K \times \mathbb{Z}_3 \cong \mathbb{Z}_6 \times \mathbb{Z}_2$ .



Applying the Fundamental Theorem of Finite Abelian Groups (Theorem 4 in *Abelian Groups*), we can say that  $\mathbb{Z}_{12}$  and  $\mathbb{Z}_6 \times \mathbb{Z}_2$  are the only two abelian groups of order 12, up to isomorphism. To generate additional nonabelian groups of order 12, we need the semi-direct product. And, to understand the idea of the semi-direct product, we need to understand the notions of *homomorphism* and *automorphism*.

Given two isomorphic groups  $G_1$  and  $G_2$  with  $x_1 \in G_1$  and  $x_2 \in G_2$ , if  $\phi : G_1 \rightarrow G_2$  is an isomorphism and  $\phi(x_1) = x_2$ , then  $x_1$  and  $x_2$  play the same role, structurally, within their respective groups. In a similar way, we can focus on a single group  $G$  and ask whether two elements of the group play structurally equivalent roles.

**Definition 3:** An isomorphism from a group  $(G, *)$  to itself is called an *automorphism* of  $G$ . That is, an automorphism of  $G$  is a bijection  $\phi : G \rightarrow G$  such that

$$\phi(x_1 * x_2) = \phi(x_1) * \phi(x_2)$$

for all  $x_1, x_2 \in G$ . ■

**Example 5:** Here are several examples of automorphisms.

(a) Define  $\phi : \mathbb{Z} \rightarrow \mathbb{Z}$  by  $\phi(x) = -x$ . Then  $\phi$  is clearly a permutation of  $\mathbb{Z}$ . Furthermore, for any integers  $x_1$  and  $x_2$ ,

$$\phi(x_1 + x_2) = -(x_1 + x_2) = -x_1 + -x_2 = \phi(x_1) + \phi(x_2)$$

Therefore,  $\phi$  is an automorphism. The fact that  $\phi$  is an automorphism means that any integer  $m$  and its inverse  $-m$  play structurally equivalent roles in the group  $(\mathbb{Z}, +)$ ; in particular, 1 and  $-1$  play equivalent roles.

(b) Let  $n$  be an integer,  $n > 2$  and let  $k$  be an integer such that  $1 < k < n$  and  $\gcd(k, n) = 1$ . Define  $\phi : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$  by

$$\phi(x) = (kx) \bmod n$$

**Exercise:** Show that  $\phi$  is one-to-one. Hint: Since  $\gcd(k, n) = 1$ ,  $|k| = n$ .

Then, for  $x_1, x_2 \in \mathbb{Z}_n$ ,

$$\phi(x_1 + x_2) = \dots = \phi(x_1) + \phi(x_2)$$

**(Exercise:** Fill in the details.) Therefore,  $\phi$  is an automorphism. The fact that  $\phi$  is an automorphism means that 1 and  $k$  play the same roles in  $\mathbb{Z}_n$ ; in fact, both 1 and  $k$  are generators for  $\mathbb{Z}_n$ .

(c) Consider the group  $D_4 = \langle r, s \mid |r| = 4, |s| = 2, s \notin \langle r \rangle, sr = r^3s \rangle$ . Is there an automorphism of  $D_4$  that maps  $s$  to  $rs$ ? Is there an automorphism of  $D_4$  that maps  $r^2$  to  $s$ ? Note that, since  $r$  and  $s$  generate  $D_4$ , an automorphism  $\phi$  on  $D_4$  is completely determined by  $\phi(r)$  and  $\phi(s)$ .

Suppose there is an automorphism  $\phi : D_4 \rightarrow D_4$  such that  $\phi(s) = rs$ . Since an automorphism is an isomorphism,  $\phi(r)$  must have the same order as  $r$  does, namely, 4. Thus,  $\phi(r) = r$  or  $r^3$ . If  $\phi(r) = r$ , then we obtain the following table of images:

$x$	$\phi(x)$
$e$	$e$
$r$	$r$
$r^2$	$r^2$
$r^3$	$r^3$
$s$	$rs$
$rs$	$r^2s$
$r^2s$	$r^3s$
$r^3s$	$s$

For example,  $\phi(rs) = \phi(r)\phi(s) = r(rs) = r^2s$ . Since  $\phi$  so defined is a permutation of  $D_4$ ,  $\phi$  is an automorphism of  $D_4$  such that  $\phi(s) = rs$ .

**Exercise:** Show that there is no automorphism of  $D_4$  that maps  $r^2$  to  $s$ .

Conclusion: In the group  $D_4$ , the elements  $s$  and  $rs$  (as well as  $r^2s$  and  $r^3s$ ) play equivalent roles; however, the element  $r^2$  plays a different role, even though it also has order 2. In fact, note that the center of  $D_4 = \{e, r^2\}$ .



For any set  $X$ , the set  $\mathcal{S}(X)$  of permutations of  $X$  is a group under the operation of composition. In *Permutation Groups*, we considered some specific examples of this group. The identity permutation  $\epsilon$  on  $X$  is the group identity, and the inverse of a given permutation  $\alpha$  is the permutation  $\alpha^{-1}$ .

Let  $G$  be a group and consider the set  $\mathcal{A}(G)$  of all automorphisms of  $G$ . Since an automorphism of  $G$  is a permutation of  $G$ , we ask, Is  $\mathcal{A}(G)$  a subgroup of  $\mathcal{S}(G)$ ?

**Theorem 3:** For any group  $G$ ,  $(\mathcal{A}(G), \circ)$  is a group; in fact,  $(\mathcal{A}(G), \circ)$  is a subgroup of  $(\mathcal{S}(G), \circ)$ .

**Proof:** We apply SJST (Smokin' Joe's Subgroup Test).

1. The identity permutation  $\epsilon$  is an automorphism of  $G$ .
2. Let  $\phi_1$  and  $\phi_2$  be automorphisms of  $G$ . We want to show that  $\phi_2 \circ \phi_1$  is an automorphism of  $G$ . Clearly,  $\phi_2 \circ \phi_1$  is a permutation of  $G$ , so it remains to show that  $\phi_2 \circ \phi_1$  distributes across the operation in  $G$ . Well, let  $x_1, x_2 \in G$ ; then

$$\begin{aligned}
 (\phi_2 \circ \phi_1)(x_1x_2) &= \phi_2(\phi_1(x_1x_2)) \\
 &= \phi_2(\phi_1(x_1)\phi_1(x_2)) && \text{since } \phi_1 \text{ is an isomorphism} \\
 &= [\phi_2(\phi_1(x_1))][\phi_2(\phi_1(x_2))] && \text{since } \phi_2 \text{ is an isomorphism} \\
 &= [(\phi_2 \circ \phi_1)(x_1)][(\phi_2 \circ \phi_1)(x_2)]
 \end{aligned}$$

as we wished to show.

3. Finally, for any automorphism  $\phi$  of  $G$ , we must show that  $\phi^{-1}$  is an automorphism of  $G$ . Again, it is clear that  $\phi^{-1}$  is a permutation of  $G$ , so we must show that  $\phi^{-1}$  distributes across the operation in  $G$ . To that end let  $x_1, x_2, y_1, y_2 \in G$  with  $\phi(x_1) = y_1$  and  $\phi(x_2) = y_2$ . Then:

$$\phi^{-1}(y_1y_2) = \phi^{-1}[\phi(x_1)\phi(x_2)] = \phi^{-1}(\phi(x_1x_2)) = x_1x_2 = \phi^{-1}(y_1)\phi^{-1}(y_2)$$

QED ■

We note that some texts use the notation  $\text{Aut}(G)$  for the automorphism group.

**Example 6:** As alluded to in Example 5, part (c), given integers  $i$  and  $j$  with  $i \in \{1, 3\}$  and  $j \in \{0, 1, 2, 3\}$ , there is an automorphism  $\phi_{ij}$  of  $D_4$  that maps  $a$  to  $a^i$  and  $b$  to  $a^j b$ , and these are the only automorphisms of  $D_4$ . Hence,

$$\mathcal{A}(D_4) = \{\phi_{10}, \phi_{11}, \phi_{12}, \phi_{13}, \phi_{30}, \phi_{31}, \phi_{32}, \phi_{33}\}$$

is a group of order 8. In *Groups of Order 8*, we catalog the groups of order 8; up to isomorphism, they are:

$$\mathbb{Z}_8, \quad \mathbb{Z}_4 \times \mathbb{Z}_2, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad D_4, \quad Q$$

with  $Q$  denoting the quaternion group.

**Exercise:** To which of these five groups is  $\mathcal{A}(D_4)$  isomorphic? Hint:  $\phi_{10} = \epsilon$ ; also,

$$\begin{aligned}
 (\phi_{11} \circ \phi_{11})(a) &= \phi_{11}(\phi_{11}(a)) = \phi_{11}(a) = a \\
 (\phi_{11} \circ \phi_{11})(b) &= \phi_{11}(\phi_{11}(b)) = \phi_{11}(ab) = \phi_{11}(a)\phi_{11}(b) = a(ab) = a^2b
 \end{aligned}$$

Thus,  $\phi_{11} \circ \phi_{11} = \phi_{12}$ . ■

**Example 7:** As alluded to in Example 5, part (b), given integers  $n$  and  $k$  with  $1 \leq k < n$  and  $\gcd(k, n) = 1$ , there is an automorphism  $\theta_k$  of  $\mathbb{Z}_n$  such that  $\theta_k(x) = kx \pmod n$ . Moreover, since any automorphism  $\theta$  of  $\mathbb{Z}_n$  must map 1 to an element of order  $n$ , these are the only automorphisms of  $\mathbb{Z}_n$ . Hence,

$$\mathcal{A}(\mathbb{Z}_n) = \{\theta_k \mid 1 \leq k < n \text{ and } \gcd(k, n) = 1\}$$

Thus,  $\mathcal{A}(\mathbb{Z}_n)$  has order  $\phi(n)$ . Also,  $\mathcal{A}(\mathbb{Z}_n)$  is abelian:

$$\begin{aligned}
(\theta_{k_2} \circ \theta_{k_1})(x) &= \theta_{k_2}(\theta_{k_1}(x)) \\
&= \theta_{k_2}(k_1x \bmod n) \\
&= [k_2(k_1x \bmod n)] \bmod n \\
&= k_1k_2x \bmod n = (\theta_{k_1} \circ \theta_{k_2})(x)
\end{aligned}$$

We already know an abelian group of order  $\phi(n)$ , namely  $U_n$ . Could it be that  $\mathcal{A}(\mathbb{Z}_n)$  and  $U_n$  are isomorphic? You betcha!

**Exercise:** Define  $f : U_n \rightarrow \mathcal{A}(\mathbb{Z}_n)$  by  $f(k) = \theta_k$ . Show that  $f$  is an isomorphism. ■

**Definition 4:** Given two groups  $G_1$  and  $G_2$ , a function  $\theta : G_1 \rightarrow G_2$  is called a *homomorphism* provided

$$\theta(x_1y_1) = \theta(x_1)\theta(y_1)$$

for all  $x_1, y_1 \in G_1$ . ■

Thus, an isomorphism is a homomorphism that is one-to-one and onto.

**Example 8:** We give two examples of homomorphisms.

(a) Let  $n$  be an integer,  $n > 1$ , and define  $\theta : \mathbb{Z} \rightarrow \mathbb{Z}_n$  by  $\theta(x) = x \bmod n$ . Then, for any  $x, y \in \mathbb{Z}$ ,

$$\theta(x + y) = (x + y) \bmod n = [(x \bmod n) + (y \bmod n)] \bmod n = \theta(x) + \theta(y)$$

Therefore,  $\theta$  is a homomorphism.

(b) Let  $m$  and  $n$  be integers with  $1 < m < n$  such that  $m$  is a factor of  $n$ . Define  $\theta : \mathbb{Z}_n \rightarrow \mathbb{Z}_m$  by  $\theta(x) = x \bmod m$ .

**Exercise:** Verify that  $\theta$  is a homomorphism. Also, give an example to show the necessity of requiring that  $m$  be a factor of  $n$ . ■

We next give a basic theorem about homomorphisms, leaving the proof as an exercise.

**Theorem 4:** Let  $G_1$  and  $G_2$  be two groups with identity elements  $e_1$  and  $e_2$ , respectively. If  $\theta : G_1 \rightarrow G_2$  is a homomorphism, then:

1.  $\theta(e_1) = e_2$ .
2. For every element  $x \in G_1$ ,  $\theta(x^{-1}) = (\theta(x))^{-1}$ .
3. For every element  $x \in G_1$  and any nonnegative integer  $n$ ,  $\theta(x^n) = (\theta(x))^n$ .

4. For every element  $x \in G_1$ , if  $x$  has finite order in  $G_1$ , then  $\theta(x)$  has finite order in  $G_2$ , and the order of  $\theta(x)$  is a factor of the order of  $x$ .
5. If  $H$  is a subgroup of  $G_1$ , then  $\theta(H)$  is a subgroup of  $G_2$ .

■

We are now prepared to define the semi-direct product of two groups.

**Definition 5:** Let  $G_1$  and  $G_2$  be two groups with identity elements  $e_1$  and  $e_2$ , respectively, and let  $\theta : G_1 \rightarrow \mathcal{A}(G_2)$  be a homomorphism; that is, assume

$$\theta(xy) = \theta(x) \circ \theta(y)$$

for all  $x, y \in G_1$ . For notational convenience, denote  $\theta(x)$  by  $\theta_x$ . Define the operation  $\#$  on the set  $G_1 \times G_2$  by

$$(x_1, x_2) \# (y_1, y_2) = (x_1 y_1, x_2 \theta_{x_1}(y_2))$$

Then  $(G_1 \times G_2, \#)$  is a group, called the **semi-direct product of  $G_1$  with  $G_2$  using  $\theta$** . It is denoted by  $G_1 \rtimes_{\theta} G_2$ , or simply by  $G_1 \rtimes G_2$  as long as the homomorphism  $\theta$  being used is understood.

■

**Exercise:** Verify that  $(G_1 \times G_2, \#)$  is a group by showing that:

- (a)  $\#$  is associative;
- (b)  $(e_1, e_2)$  is the identity element;
- (c)

$$(x_1, x_2)^{-1} = (x_1^{-1}, \theta_{x_1^{-1}}(x_2^{-1}))$$

(d) Also, show that, if  $\theta$  is the trivial homomorphism — the homomorphism that maps every element of  $G_1$  to the identity automorphism of  $G_2$  — then  $G_1 \rtimes G_2$  is simply the direct product of  $G_1$  with  $G_2$ . Hence, the semi-direct product is a generalization of the direct product.

■

It can be shown that (see Exercise 26), if  $G_1$  and  $G_2$  are finite abelian groups and  $\theta : G_1 \rightarrow \mathcal{A}(G_2)$  is not the trivial homomorphism, then the semi-direct product of  $G_1$  with  $G_2$  using  $\theta$  is a finite nonabelian group of order  $|G_1||G_2|$ . Thus, to obtain a nonabelian group of order 12, we can use a nontrivial semi-direct product of abelian groups of orders  $n_1$  and  $n_2$ , with  $1 < n_1, n_2 < 12$  and  $n_1 n_2 = 12$ .

Suppose  $n_1 = 6$  and  $n_2 = 2$ . Then we need a homomorphism  $\theta$  from  $\mathbb{Z}_6$  to  $\mathcal{A}(\mathbb{Z}_2)$ . However, since  $\mathcal{A}(\mathbb{Z}_2)$  is trivial (by Example 7),  $\theta$  must be trivial in this case.

Suppose  $n_1 = 4$  and  $n_2 = 3$ . Then we need a nontrivial homomorphism  $\theta$  from  $\mathbb{Z}_4$  to  $\mathcal{A}(\mathbb{Z}_3)$ , or from  $\mathbb{Z}_2 \times \mathbb{Z}_2$  to  $\mathcal{A}(\mathbb{Z}_3)$ .

First, suppose  $G_1 = \mathbb{Z}_4$ . Since  $\mathcal{A}(\mathbb{Z}_3) \cong U_3 = \{1, 2\}$ , the only nontrivial homomorphism  $\theta : \mathbb{Z}_4 \rightarrow \mathcal{A}(\mathbb{Z}_3)$  must map 1 to the automorphism  $\phi$  of  $\mathbb{Z}_3$  defined by  $\phi(x) = -x$  (that is,  $\phi(0) = 0$ ,  $\phi(1) = 2$ , and  $\phi(2) = 1$ ). So,

$$\theta_0 = \epsilon, \quad \theta_1 = \phi, \quad \theta_2 = \epsilon, \quad \text{and} \quad \theta_3 = \phi$$

Let  $\mathbb{Z}_4 \rtimes \mathbb{Z}_3$  denote the semi-direct product of  $\mathbb{Z}_4$  with  $\mathbb{Z}_3$  using  $\theta$ . As noted above,  $(0, 0)$  is the identity element of  $\mathbb{Z}_4 \rtimes \mathbb{Z}_3$ . It is also easy to see that, for any  $x_1, y_1 \in \mathbb{Z}_4$  and any  $x_2, y_2 \in \mathbb{Z}_3$ ,

$$(x_1, 0) \# (y_1, 0) = ((x_1 + y_1) \bmod 4, 0), \text{ and} \\ (0, x_2) \# (0, y_2) = (0, (x_2 + y_2) \bmod 3)$$

It follows that, in  $\mathbb{Z}_4 \rtimes \mathbb{Z}_3$ :

$$|(1, 0)| = 4, \quad |(2, 0)| = 2, \quad |(3, 0)| = 4, \quad |(0, 1)| = 3, \quad |(0, 2)| = 3$$

**Exercise:** For each  $x_1 \in \mathbb{Z}_4 - \{0\}$  and each  $x_2 \in \mathbb{Z}_3 - \{0\}$ , find the order of the element  $(x_1, x_2)$  in  $\mathbb{Z}_4 \rtimes \mathbb{Z}_3$ . As an example, let's find the order of  $(1, 2)$ :

$$(1, 2)^2 = (1, 2) \# (1, 2) = (1 + 1, 2 + \theta_1(2)) = (2, 2 + 1) = (2, 0)$$

Since  $(2, 0)$  has order 2, the element  $(1, 2)$  has order 4. Also, since

$$(1, 2)^{-1} = (1^{-1}, \theta_{1^{-1}}(2^{-1})) = (-1, \theta_{-1}(-2)) = (3, \theta_3(1)) = (3, 2)$$

the element  $(3, 2)$  also has order 4.

Summarizing our results, we obtain the following “order profile” for the group  $\mathbb{Z}_4 \rtimes \mathbb{Z}_3$ :

order	elements	number
1	(0, 0)	1
2	(2, 0)	1
3	(0, 1), (0, 2)	2
4	(1, 0), (1, 1), (1, 2), (3, 0), (3, 1), (3, 2)	6
6	(2, 1), (2, 2)	2
12	none	0
total		12

Thus,  $\mathbb{Z}_4 \rtimes \mathbb{Z}_3$  has a different order profile than  $D_6$ , so it is a different nonabelian group of order 12. Therefore, we can add to our list of groups of order 12, so that now there are four groups on our list:

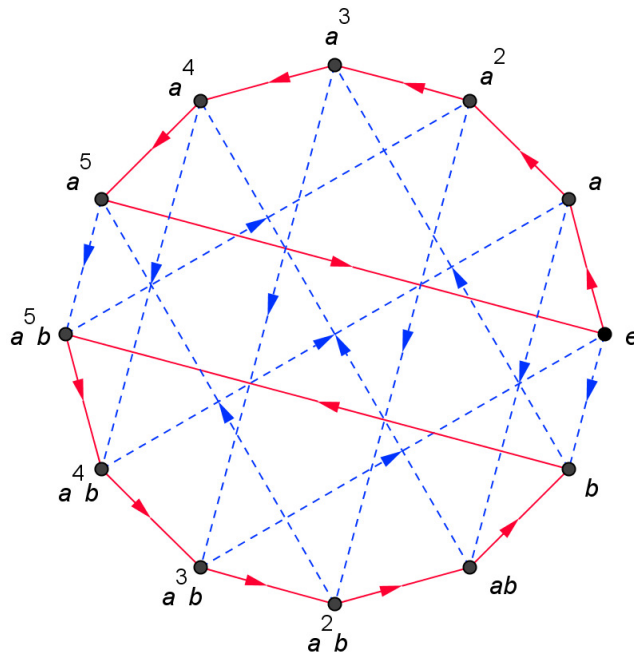
$$\mathbb{Z}_{12}, \quad \mathbb{Z}_6 \times \mathbb{Z}_2, \quad D_6, \quad \mathbb{Z}_4 \rtimes \mathbb{Z}_3$$

It can be shown that  $\mathbb{Z}_4 \rtimes \mathbb{Z}_3$  is isomorphic to the abstract group  $T$  with the presentation

$$T = \langle a, b \mid |a| = 6, |b| = 4, a^3 = b^2, ba = a^5b \rangle$$

**Exercise:** Verify this.

The Cayley digraph for  $T$  using generating set  $\{a, b\}$  is shown in Figure 1.



**Figure 1** Cayley digraph for  $T$  using generating set  $\{a, b\}$

Continuing our search, we can try letting  $G_1 = \mathbb{Z}_2 \times \mathbb{Z}_2$  and  $G_2 = \mathbb{Z}_3$ . Note that a nontrivial homomorphism  $\theta$  from  $\mathbb{Z}_2 \times \mathbb{Z}_2$  to  $\mathcal{A}(\mathbb{Z}_3)$  must map precisely two of the elements  $(0, 1)$ ,  $(1, 0)$ , and  $(1, 1)$  to the automorphism  $\phi$  of  $\mathbb{Z}_3$  (same  $\phi$  as above). By symmetry, we may assume that

$$\theta_{(0,0)} = \epsilon, \quad \theta_{(0,1)} = \phi, \quad \theta_{(1,0)} = \epsilon, \quad \text{and} \quad \theta_{(1,1)} = \phi$$

**Exercise:** In the semi-direct product of  $G_1$  with  $G_2$  using  $\theta$ , let  $r = ((1, 0), 1)$  and  $s = ((0, 1), 0)$ . Verify that  $|r| = 6$ ,  $|s| = 2$ ,  $s \neq a^3$ , and  $sr = r^5s$ . It follows that  $G_1 \rtimes G_2 \cong D_6$ .

Note that, in general,  $G_1 \rtimes G_2$  is not isomorphic to  $G_2 \rtimes G_1$ . So, next, let's consider the case when  $n_1 = 3$  and  $n_2 = 4$ . Thus,  $G_1 = \mathbb{Z}_3$ .

First, we could try letting  $G_2 = \mathbb{Z}_4$ . However, the only homomorphism from  $\mathbb{Z}_3$  to  $\mathcal{A}(\mathbb{Z}_4)$  is the trivial homomorphism, so this won't buy us anything.

Second, we can try letting  $G_2 = \mathbb{Z}_2 \times \mathbb{Z}_2$ . It can be seen that any permutation of  $\mathbb{Z}_2 \times \mathbb{Z}_2$  that maps  $(0, 0)$  to  $(0, 0)$  is an automorphism of  $\mathbb{Z}_2 \times \mathbb{Z}_2$ ; that is,  $\mathcal{A}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$ . Among these, there are two of order 3:  $\phi$ , mapping  $(0, 1)$  to  $(1, 0)$ ,  $(1, 0)$  to  $(1, 1)$ , and  $(1, 1)$  to  $(0, 1)$ , and  $\phi^{-1}$ . Turns out it doesn't matter which one we use for  $\theta(1)$ , so let's let  $\theta : \mathbb{Z}_3 \rightarrow \mathcal{A}(\mathbb{Z}_2 \times \mathbb{Z}_2)$  be defined by

$$\theta_0 = \epsilon, \quad \theta_1 = \phi, \quad \text{and} \quad \theta_2 = \phi^{-1}$$

Let  $\mathbb{Z}_3 \rtimes (\mathbb{Z}_2 \times \mathbb{Z}_2)$  denote the semi-direct product of  $\mathbb{Z}_3$  with  $\mathbb{Z}_2 \times \mathbb{Z}_2$  using  $\theta$ . Again,  $(0, (0, 0))$  is the identity element of  $\mathbb{Z}_3 \rtimes (\mathbb{Z}_2 \times \mathbb{Z}_2)$ , and it is easy to check that

$$|(1, (0, 0))| = |(2, (0, 0))| = 3 \quad \text{and} \quad |(0, (0, 1))| = |(0, (1, 0))| = |(0, (1, 1))| = 2$$

**Exercise:** For each  $x_1 \in \mathbb{Z}_1 - \{0\}$  and each  $(x_2, y_2) \in \mathbb{Z}_2 \times \mathbb{Z}_2 - \{(0, 0)\}$ , find the order of the element  $(x_1, (x_2, y_2))$  in  $\mathbb{Z}_3 \rtimes (\mathbb{Z}_2 \times \mathbb{Z}_2)$ . As an example, let's find the order of  $(1, (0, 1))$ :

$$\begin{aligned} (1, (0, 1))^2 &= (1, (0, 1)) \# (1, (0, 1)) = (1 + 1, (0, 1) + \theta_1(0, 1)) = (2, (0, 1) + (1, 0)) = (2, (1, 1)) \\ (1, (0, 1))^3 &= (1, (0, 1)) \# (2, (1, 1)) = (1 + 2, (0, 1) + \theta_1(1, 1)) = (0, (0, 1) + (0, 1)) = (0, (0, 0)) \end{aligned}$$

Thus,  $(1, (0, 1))$  has order 3 and, since  $(2, (1, 1))$  is the inverse of  $(1, (0, 1))$ , it also has order 3.

Summarizing our results, we obtain the following “order profile” for the group  $\mathbb{Z}_3 \rtimes (\mathbb{Z}_2 \times \mathbb{Z}_2)$ :

order	elements	number
1	$(0, (0, 0))$	1
2	$(0, (0, 1)), (0, (1, 0)), (0, (1, 1))$	3
3	rest	8
4	none	0
6	none	0
12	none	0
total		12

Thus,  $\mathbb{Z}_3 \rtimes (\mathbb{Z}_2 \times \mathbb{Z}_2)$  has a different order profile than either  $D_6$  or  $\mathbb{Z}_4 \times \mathbb{Z}_3$ , so it is a different nonabelian group of order 12. Therefore, we can add to our list of groups of order 12, so that now there are five groups on our list:

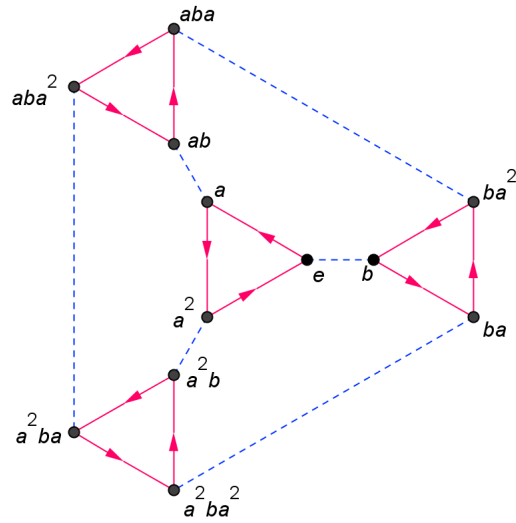
$$\mathbb{Z}_{12}, \quad \mathbb{Z}_6 \times \mathbb{Z}_2, \quad D_6, \quad \mathbb{Z}_4 \times \mathbb{Z}_3, \quad \mathbb{Z}_3 \rtimes (\mathbb{Z}_2 \times \mathbb{Z}_2)$$

It can be shown that  $\mathbb{Z}_3 \rtimes (\mathbb{Z}_2 \times \mathbb{Z}_2)$  is isomorphic to the abstract group  $A_4$  with the presentation

$$A_4 = \langle a, b \mid |a| = 3, |b| = 2, aba = ba^2b \rangle$$

**Exercise:** Verify this.

The Cayley digraph for  $A_4$  using generating set  $\{a, b\}$  is shown in Figure 2. In *Permutation Groups*, we meet  $A_4$  in another context, as the subgroup of  $S_4$  consisting of the even permutations of  $\{1, 2, 3, 4\}$ .



**Figure 2** Cayley digraph for  $A_4$  using generating set  $\{a, b\}$

**Exercises**

1. For each part, list the elements of the given group and find the order of each element. Is the group cyclic?

- (a)  $\mathbb{Z}_5 \times \mathbb{Z}_2$  (b)  $\mathbb{Z}_5 \times \mathbb{Z}_3$
- (c)  $U_8 \times U_{10}$  (d)  $U_8 \times U_{12}$

2. Prove the following parts of Theorem 1:

- (a) part 1 (b) part 2 (c) part 3

3. For each part, find the maximum order among the elements in the given group and give an example of an element having the maximum order.

- (a)  $\mathbb{Z}_7 \times \mathbb{Z}_2$  (b)  $\mathbb{Z}_8 \times \mathbb{Z}_2$
- (c)  $\mathbb{Z}_4 \times \mathbb{Z}_4$  (d)  $(\mathbb{Z}_4 \times \mathbb{Z}_2) \times \mathbb{Z}_2$

Note on part (d):  $(\mathbb{Z}_4 \times \mathbb{Z}_2) \times \mathbb{Z}_2 = \{((x, y), z) \mid x \in \mathbb{Z}_4 \text{ and } y, z \in \mathbb{Z}_2\}$ . Usually, we agree to drop the extra parentheses and write simply

$$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(x, y, z) \mid x \in \mathbb{Z}_4 \text{ and } y, z \in \mathbb{Z}_2\}$$

4. Let  $G, G_1,$  and  $G_2$  be arbitrary groups. Show that:

- (a)  $G \times \mathbb{Z}_1 \cong G$
- (b)  $G_1 \times G_2 \cong G_2 \times G_1$
- (c) If  $e_2$  denotes the identity of  $G_2$ , then  $G_1 \times \{e_2\}$  is a subgroup of  $G_1 \times G_2$  and  $G_1 \times \{e_2\} \cong G_1$ .

(d) If  $e_1$  denotes the identity of  $G_1$ , then  $\{e_1\} \times G_2$  is a subgroup of  $G_1 \times G_2$  and  $\{e_1\} \times G_2 \cong G_2$ .

It follows from parts (c) and (d) that we may consider both  $G_1$  and  $G_2$  to be subgroups of the direct product of  $G_1$  with  $G_2$ .

5. Show that  $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$ .

6. We already know two groups of order 16:  $\mathbb{Z}_{16}$  and  $D_8$ . Give additional examples of groups of order 16 having the form:

- (a)  $G \times \mathbb{Z}_2$ , with  $G$  having order 8
- (b)  $G \times \mathbb{Z}_4$ , with  $G$  having order 4
- (c)  $G \times (\mathbb{Z}_2 \times \mathbb{Z}_2)$ , with  $G$  having order 4

Which of these are not isomorphic? (It is known that there are, up to isomorphism, five abelian groups and nine nonabelian groups of order 16, for a total of fourteen; see [Groups of Order 16](#).)

7. In each part, verify the stated isomorphism.

- (a)  $U_{17} \cong \mathbb{Z}_{16}$
- (b)  $U_{18} \cong \mathbb{Z}_6$
- (c)  $U_{27} \cong \mathbb{Z}_{18}$
- (d)  $U_{21} \cong \mathbb{Z}_6 \times \mathbb{Z}_2$

8. Here are four groups of order 18:

$$\mathbb{Z}_{18}, \quad \mathbb{Z}_6 \times \mathbb{Z}_3, \quad D_9, \quad D_3 \times \mathbb{Z}_3$$

Show that no two of these groups are isomorphic. There is one additional nonabelian group of order 18; refer to Exercise 37.

9. Let  $G$  be a group, let  $n$  be an integer,  $n > 1$ , and let  $\theta : \mathbb{Z}_n \rightarrow G$  be a homomorphism.

- (a) Show that  $\theta$  is completely determined by  $\theta(1)$ .
- (b) With  $D_3 = \langle r, s \mid |r| = 3, |s| = 2, sr = r^2s \rangle$ , determine the homomorphism  $\theta : \mathbb{Z}_6 \rightarrow D_3$  with  $\theta(1) = r$ .
- (c) With  $D_3$  as in part (b), determine the homomorphism  $\theta : \mathbb{Z}_6 \rightarrow D_3$  with  $\theta(1) = s$ .

10. Prove the remaining parts of Theorem 2:

- (a) part 3
- (b) part 4
- (c) part 5
- (d) part 7

11. Let  $G$  be a group, and let  $\theta : \mathbb{Z} \rightarrow G$  be a homomorphism.

- (a) Show that  $\theta$  is completely determined by  $\theta(1)$ .
- (b) With  $D_4 = \langle r, s \mid |r| = 4, |s| = 2, s \neq r^2, sr = r^3s \rangle$ , determine the homomorphism  $\theta : \mathbb{Z} \rightarrow D_4$  with  $\theta(1) = r$ .
- (c) With  $D_4$  as in part (b), determine the homomorphism  $\theta : \mathbb{Z} \rightarrow D_4$  with  $\theta(1) = s$ .

12. Prove Theorem 4.

13. For  $n \in \mathbb{Z}^+$ , recall that  $n\mathbb{Z}$  denotes the set of multiples of  $n$ :

$$n\mathbb{Z} = \{\dots -3n, -2n, -n, 0, n, 2n, 3n, \dots\}$$

(a) Show that  $(n\mathbb{Z}, +)$  is a subgroup of  $(\mathbb{Z}, +)$ .

(b) Show that  $(n\mathbb{Z}, +) \cong (\mathbb{Z}, +)$ .

This shows that an infinite group may be isomorphic to some of its proper subgroups.

14. Let  $n$  be an integer,  $n > 2$ . Recall that

$$D_n = \langle r, s \mid |r| = n, |s| = 2, s \notin \langle r \rangle, sr = r^{n-1}s \rangle$$

If  $n$  is even, show that  $D_n$  has a subgroup isomorphic to  $\mathbb{Z}_2 \times \mathbb{Z}_2$ .

15. Determine all the homomorphisms from:

(a)  $\mathbb{Z}_6$  to  $\mathbb{Z}_4$

(b)  $\mathbb{Z}_6$  to  $\mathbb{Z}_6$

(c)  $\mathbb{Z}_6$  to  $\mathbb{Z}_7$

(d)  $\mathbb{Z}_6$  to  $\mathbb{Z}_9$

16. Let  $G_1$  and  $G_2$  be two groups and let  $\theta : G_1 \rightarrow G_2$  be a homomorphism.

(a) Show that  $\ker(\theta) = \{x \in G_1 \mid \theta(x) = e_2\}$  is a normal subgroup of  $G_1$ . (As usual,  $e_2$  denotes the identity in  $G_2$ .)

(b) Show that  $\text{im}(\theta) = \{\theta(x) \mid x \in G_1\}$  is a subgroup of  $G_2$ .

(c) Show that  $G/\ker(\theta) \cong \text{im}(\theta)$ ; this result is known as the *First Isomorphism Theorem*.

(d) Prove or disprove: If  $G_1$  is abelian, then  $\text{im}(\theta)$  is abelian.

(e) Prove or disprove: If  $G_1$  is abelian, then  $G_2$  is abelian.

17. Determine all the isomorphisms from:

(a)  $\mathbb{Z}_6$  to  $\mathbb{Z}_6$

(b)  $\mathbb{Z}_6$  to  $U_7$

(c)  $\mathbb{Z}$  to  $\mathbb{Z}$

(d)  $\mathbb{Z}$  to  $2\mathbb{Z}$

18. Let  $G$  be a group with  $g \in G$ . Define  $\phi_g : G \rightarrow G$  by  $\phi_g(x) = gxg^{-1}$ .

(a) Show that  $\phi_g$  is an automorphism of  $G$ ;  $\phi_g$  is called the *inner automorphism* of  $G$  determined by  $g$ .

(b) What is  $\phi_g$  if  $g$  belongs to the center of  $G$ ?

(c) For  $G = D_4$ , find  $\phi_a$ .

(d) For  $G = D_4$ , find  $\phi_b$ .

19. Let  $G$  be a group and define  $\theta : G \rightarrow G$  by  $\theta(x) = x^{-1}$ . Prove that  $\theta$  is an automorphism of  $G$  if and only if  $G$  is abelian.

20. Refer to Exercise 18. Let

$$\mathcal{I}(G) = \{\phi_g \mid g \in G\}$$

(a) Show that  $\mathcal{I}(G)$  is a subgroup of  $\mathcal{A}(G)$ ;  $\mathcal{I}(G)$  is called the *inner automorphism group* of  $G$ .

(b) What is  $\mathcal{I}(G)$  when  $G$  is abelian?

(c) Show that  $\mathcal{I}(G) \cong G/\mathcal{C}$ , where  $\mathcal{C}$  denotes the center of  $G$ . Hint: Apply the First Isomorphism Theorem (see Exercise 16).

(d) Find  $\mathcal{I}(D_4)$ .

(e) Find  $\mathcal{I}(Q)$ .

21. Let  $G_1$  be the group of nonzero complex numbers under multiplication and let  $G_2$  be the group of invertible 2 by 2 matrices (with real entries) under multiplication. Define  $\theta : G_1 \rightarrow G_2$  by

$$\theta(x + yi) = \begin{bmatrix} x & y \\ -y & x \end{bmatrix}$$

(a) Show that  $\theta$  is a homomorphism.

(b) Show that  $\theta$  is one-to-one but not onto.

22. Consider the group  $G$  of order 12 with the presentation

$$G = \langle s, t \mid |s| = 4, |t| = 3, ts = st^2 \rangle$$

Show that  $G$  is isomorphic to  $T$ .

23. Show that:

(a)  $\mathcal{A}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong D_3$

(b)  $\mathcal{A}(D_3) \cong D_3$

(c)  $\mathcal{A}(\mathbb{Z}_4 \times \mathbb{Z}_2) \cong D_4$

24. For  $n \in \mathbb{Z}^+$ , show that the relation “is isomorphic to” is an equivalence relation on the set  $\mathcal{G}_n$  of all groups of order  $n$ . (It's actually an equivalence relation on the set  $\mathcal{G}$  of all groups.)

25. Show that:

(a)  $\mathcal{A}(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2)$  is a group of order 210

(b)  $\mathcal{A}(Q)$  is a group of order 24

(c)  $\mathcal{A}(D_5)$  is a group of order 20

26. Let  $G_1$  and  $G_2$  be nontrivial groups, let  $\theta : G_1 \rightarrow \mathcal{A}(G_2)$  be a homomorphism, and let  $G_1 \rtimes G_2$  denote the semi-direct product of  $G_1$  with  $G_2$  using  $\theta$ .

(a) If  $\theta$  is the trivial homomorphism, show that  $G_1 \rtimes G_2 \cong G_1 \times G_2$ .

(b) If  $\theta$  is not the trivial homomorphism, show that  $G_1 \rtimes G_2$  is a nonabelian group.

27. Define  $\phi : \mathbb{R}^\# \rightarrow \mathbb{R}^\#$  by  $\phi(x) = \sqrt[3]{x}$ . Show that  $\phi$  is an automorphism of  $(\mathbb{R}^\#, \cdot)$ .

28. Let  $G$  be an abelian group and define  $\theta : G \rightarrow G$  by  $\theta(x) = x^2$ .

(a) Show that  $\theta$  is a homomorphism.

(b) If  $G$  is finite, give a sufficient condition, in terms of the number of elements of order 2, for  $\theta$  to be an automorphism.

(c) Show by example that, if  $G$  is infinite, then the condition found in part (b) may not be sufficient for  $\theta$  to be an automorphism.

29. For an odd prime  $p$ , what can be said about  $\mathcal{A}(U_p)$ ?

30. Refer to Exercise 18.

(a) If  $c$  belongs to the center of  $G$ , show that

$$\phi_g c = \phi_g$$

for every  $g \in G$ .

(b) For  $g_1, g_2 \in G$ , prove: If  $\phi_{g_1} = \phi_{g_2}$ , then  $g_1^{-1}g_2$  belongs to the center of  $G$ .

31. Are the groups  $U_{20}$  and  $U_{24}$  isomorphic? Explain.

32. Refer to Exercise 18. Show that  $|\phi_g|$  is a factor of  $|g|$ .

33. Let  $\phi$  be an automorphism of  $(\mathbb{R}^\#, \cdot)$ . Show that  $\phi(\mathbb{R}^-) = \mathbb{R}^-$  and  $\phi(\mathbb{R}^+) = \mathbb{R}^+$ .

34. Let

$$\begin{aligned} H_1 &= \{(x, e_2) \mid x \in G_1\} \\ H_2 &= \{(e_1, y) \mid y \in G_2\} \end{aligned}$$

(a) Show that  $(H_1, \#)$  is a subgroup of  $(G_1 \times G_2, \#)$  and that  $G_1 \cong H_1$ .

(b) Show that  $(H_2, \#)$  is a normal subgroup of  $(G_1 \times G_2, \#)$  and that  $G_2 \cong H_2$ .

In this sense, both of the groups  $G_1$  and  $G_2$  may be considered to be subgroups of any semi-direct product of  $G_1$  with  $G_2$ .

37. Let  $\theta : \mathbb{Z}_2 \rightarrow \mathcal{A}(\mathbb{Z}_3 \times \mathbb{Z}_3)$  be the homomorphism defined  $\theta(1) = \phi$ , with  $\phi$  the automorphism of  $\mathbb{Z}_3 \times \mathbb{Z}_3$  that maps each element to its inverse. Show that the semi-direct product of  $\mathbb{Z}_2$  with  $\mathbb{Z}_3 \times \mathbb{Z}_3$  using  $\theta$  is a nonabelian group  $G$  of order 18 that is not isomorphic to either  $D_9$  or  $D_3 \times \mathbb{Z}_3$ . Hint: In  $G$ , let  $a = (0, (0, 1))$ ,  $b = (0, (1, 0))$ , and  $c = (1, (0, 0))$ ; show that  $|a| = 3 = |b|$ ,  $|c| = 2$ ,  $ba = ab$ ,  $ca = a^2c$ , and  $cb = b^2c$ . See Exercise 8.

38. Let  $G_1$  and  $G_2$  be two groups, with identity elements  $e_1$  and  $e_2$ , respectively.

(a) Show that, if  $H_1 \leq G_1$  and  $H_2 \leq G_2$ , then  $H_1 \times H_2 \leq G_1 \times G_2$ .

Suppose that  $H$  is a subgroup of  $G_1 \times G_2$ , and define the following subsets  $H_1$  and  $H_2$  of  $G_1$  and  $G_2$ , respectively:

$$H_1 = \{x_1 \in G_1 \mid (x_1, x_2) \in H \text{ for some } x_2 \in G_2\}$$

$$H_2 = \{x_2 \in G_2 \mid (x_1, x_2) \in H \text{ for some } x_1 \in G_1\}$$

(b) Show that  $H_1 \leq G_1$  and  $H_2 \leq G_2$ .

39. Let  $G_1$  and  $G_2$  be two groups, with identity elements  $e_1$  and  $e_2$ , respectively.

(a) Show that, if  $H_1 \triangleleft G_1$  and  $H_2 \triangleleft G_2$ , then  $H_1 \times H_2 \triangleleft G_1 \times G_2$ .

Suppose that  $H$  is a normal subgroup of  $G_1 \times G_2$ , and define the subsets  $H_1$  and  $H_2$  of  $G_1$  and  $G_2$ , respectively, as in Exercise 38.

(b) Show that  $H_1 \triangleleft G_1$  and  $H_2 \triangleleft G_2$ .

40. In the case when both  $G_1$  and  $G_2$  are finite groups, explain how the results of Exercises 38 and 39 relate to the problem of constructing the lattice of subgroups for  $G_1 \times G_2$ , given the lattice of subgroups for  $G_1$  and the lattice of subgroups for  $G_2$ .

41. Given a finite group  $G$ , the *cycle graph* for  $G$  gives a visual representation of the cyclic subgroups of  $G$  and how they intersect. See

[mathworld.wolfram.com/FiniteGroup.html](http://mathworld.wolfram.com/FiniteGroup.html)

for the cycle graphs corresponding to the groups of order 8. Construct a cycle graph for each of the five groups of order 12.

42. Let  $G$  be a (finite) nonabelian group with identity  $e$ , and suppose  $G$  has a normal subgroup  $N$  and a subgroup  $H$  such that  $G = HN$  and  $H \cap N = \{e\}$ .

(a) Since  $G = HN$ , each element  $g \in G$  may be expressed as a product  $hn$  for some elements  $h \in H$  and  $n \in N$ . Show that this representation is unique.

(b) Show that  $H \cong G/N$ . Hint: Define:  $\epsilon' : H \rightarrow G$  by  $\epsilon'(h) = h$  and  $\pi : G \rightarrow G/N$  by  $\pi(g) = Ng$ ; consider the mapping  $\pi \circ \epsilon'$ .

Define  $\theta : H \rightarrow \mathcal{A}(N)$  by  $\theta(h) = \theta_h$ , where

$$\theta_h(n) = h^{-1}nh$$

(c) Verify that  $\theta_h$  is an automorphism of  $N$ .

(d) Show that  $G$  is isomorphic to the semidirect product of  $H$  with  $N$  using  $\theta$ . Hint: For  $h \in H$  and  $n \in N$ , consider the mapping that sends the product  $hn$  in  $G$  to the ordered pair  $(h, n)$  in  $H \rtimes N$ ; also, note that  $h_1 n_1 h_2 n_2 = (h_1 h_2)(h_2^{-1} n_1 h_2) n_2$ .