Chapter 4
Factor Groups and Homomorphisms

In the previous chapter, we tended to consider just one group at a time. But we need to find ways of relating groups to each other. For instance, we would like to know if two groups are, in every meaningful sense, the same. This would be the case if we took a group and created a new one by simply changing the labels on the group elements, but left the structure otherwise intact. Surely, we would not wish to think of these as different sorts of groups.[1] This is where the notion of a group homomorphism and, in particular, an isomorphism, will come into the picture.

But first, we will discuss factor groups. These constitute an important way of creating new groups from old ones. As we shall see, there is a natural connection between factor groups and homomorphisms. In order to define a factor group, we require a special sort of subgroup, called a normal subgroup. Let us begin there.

4.1 Normal Subgroups

Let H be a subgroup of G. We would like to form a group whose elements are the left cosets aH. Unfortunately, as we shall see in the next section, not just any subgroup will suffice; we need an extra condition. This is where normal subgroups come in.

Recall that if $H \leq G$, then the left cosets of H do not necessarily coincide with the right cosets. We need to consider subgroups for which they do coincide.

Definition 4.1. Let G be a group and N a subgroup. We say that N is a **normal subgroup** of G if $aN = Na$ for all $a \in G$.

Example 4.1. For every group G, G is a normal subgroup of itself, as $aG = Ga = G$ for all a. Also, $\{e\}$ is normal. Indeed, $a\{e\} = \{e\}a = \{a\}$ for all a.

[1] Upon reading this sentence aloud, the author failed to stop himself from writing "And don't call me Shirley." We miss you, Leslie Nielsen!

G. T. Lee, *Abstract Algebra*, Springer Undergraduate Mathematics Series,
https://doi.org/10.1007/978-3-319-77649-1_4

Example 4.2. The centre of every group is a normal subgroup. Indeed, writing $Z = Z(G)$, we have $aZ = \{az : z \in Z\} = \{za : z \in Z\} = Za$. In fact, every subgroup of $Z(G)$ is normal in G, for precisely the same reason. In particular, every subgroup of an abelian group is normal.

Be warned: this last example can be a bit misleading. Remember, when we say that $aN = Na$, we do not necessarily mean that $an = na$ for all $n \in N$. Indeed, we could have $an = n_1 a$, for some different $n_1 \in N$. The following example may be helpful.

Example 4.3. Refer to Example 3.42. We saw that in D_8, the subgroup $\langle R_{90} \rangle$ is normal. That is, $a\langle R_{90} \rangle = \langle R_{90} \rangle a$ for all $a \in D_8$. This does not mean that $aR_{90} = R_{90}a$, however. Indeed, $F_1 R_{90} = R_{270} F_1$. But as $R_{270} \in \langle R_{90} \rangle$, this is fine. We also saw in that example that $\langle F_1 \rangle$ is not a normal subgroup of D_8, as $R_{90}\langle F_1 \rangle \neq \langle F_1 \rangle R_{90}$.

There is one special case in which we do not need to worry about normality.

Theorem 4.1. *If G is a group, then any subgroup of index 2 is normal in G.*

Proof. Let H be a subgroup of index 2. Then one of the left cosets is H, and the other must consist of everything outside of H. In particular, $aH = H$ if $a \in H$ and aH is the other left coset if $a \notin H$. But exactly the same thing can be said for right cosets! So the left and right cosets agree. □

Example 4.4. It is worth noting that if N is a normal subgroup of G and H is a normal subgroup of N, it does not necessarily follow that H is normal in G. For instance, $N = \{R_0, R_{180}, F_1, F_2\}$ is a normal subgroup of D_8. (To check that it is a subgroup, use Theorem 3.14. To check that it is normal, use Theorem 4.1.) Also, $H = \langle F_1 \rangle$ is normal in N. (Again, it has index 2.) But as we saw in Example 4.3, H is not normal in D_8.

Let us define a new subgroup.

Definition 4.2. Let H be a subgroup of G. Then for any $a \in G$, we write $a^{-1}Ha = \{a^{-1}ha : h \in H\}$.

Theorem 4.2. *If H is a subgroup of G and $a \in G$, then $a^{-1}Ha$ is a subgroup of G. Furthermore, $|a^{-1}Ha| = |H|$.*

Proof. We have $e \in H$, and therefore $e = a^{-1}ea \in a^{-1}Ha$. If $a^{-1}h_1a, a^{-1}h_2a \in a^{-1}Ha$, then

$$(a^{-1}h_1a)(a^{-1}h_2a) = a^{-1}h_1(aa^{-1})h_2a = a^{-1}h_1eh_2a = a^{-1}h_1h_2a \in a^{-1}Ha,$$

since $h_1h_2 \in H$. Finally, if $a^{-1}ha \in a^{-1}Ha$, then $(a^{-1}ha)^{-1} = a^{-1}h^{-1}a \in a^{-1}Ha$, since $h^{-1} \in H$. Thus, $a^{-1}Ha$ is a subgroup of G. Also, given the definition of $a^{-1}Ha$, it is clear that we can only get one element for each element of H. But if $a^{-1}h_1a = a^{-1}h_2a$, then by cancellation, $h_1 = h_2$. Thus, $|a^{-1}Ha| = |H|$. □

We can use this to give several different ways of saying that a subgroup is normal.

Theorem 4.3. *Let G be a group and H a subgroup. Then the following are equivalent:*

1. *H is normal in G;*
2. *$a^{-1}ha \in H$ for all $h \in H$ and all $a \in G$;*
3. *$a^{-1}Ha \subseteq H$ for all $a \in G$; and*
4. *$a^{-1}Ha = H$ for all $a \in G$.*

Proof. It is clear that (4) implies (3) and (3) implies (2). Let us show that (2) implies (1). Suppose that (2) holds. Take any $a \in G$. Then for any $h \in H$, we have $a^{-1}ha = h_1$, for some $h_1 \in H$. Thus, $ha = ah_1 \in aH$. That is, $Ha \subseteq aH$. Also, $(a^{-1})^{-1}ha^{-1} = h_2$, for some $h_2 \in H$. That is, $aha^{-1} = h_2$, and therefore $ah = h_2a \in Ha$. Thus, $aH \subseteq Ha$, so $aH = Ha$ and (1) is proved.

Finally, let us show that (1) implies (4). Let H be a normal subgroup of G. Take any $a \in G$. Then $Ha = aH$. Thus, for any $h \in H$, we have $ha \in aH$, and therefore $ha = ah_1$, for some $h_1 \in H$. That is, $a^{-1}ha = h_1 \in H$. Therefore, $a^{-1}Ha \subseteq H$. But using a^{-1} in place of a, we also get $aHa^{-1} \subseteq H$. Hence, if $h \in H$, then $aha^{-1} = h_2$, for some $h_2 \in H$. But now $h = a^{-1}h_2a \in a^{-1}Ha$. That is, $H \subseteq a^{-1}Ha$, and we are done. □

Example 4.5. Let $SL_n(\mathbb{R})$ denote the set of all matrices in $GL_n(\mathbb{R})$ having determinant 1. We call this the **special linear group**. In view of Exercise 3.33, we know that $SL_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$. In fact, it is a normal subgroup. Indeed, if $A \in SL_n(\mathbb{R})$ and $B \in GL_n(\mathbb{R})$, then

$$\det(B^{-1}AB) = \det(B^{-1})\det(A)\det(B) = \det(B^{-1})\det(B)\det(A),$$

since the determinants are just real numbers. But this is $\det(B^{-1}B)\det(A) = 1$, since $B^{-1}B$ is the identity matrix and $\det(A) = 1$. Therefore, $B^{-1}AB \in SL_n(\mathbb{R})$, and by Theorem 4.3, $SL_n(\mathbb{R})$ is indeed normal.

Another useful construction is the following.

Definition 4.3. If H and K are subgroups of G, then we write $HK = \{hk : h \in H, k \in K\}$. (If the group operation is addition, write $H+K = \{h+k : h \in H, k \in K\}$.)

Note that HK is a subset of G, not necessarily a subgroup! It is easy to come up with examples where HK is not a subgroup, but the following theorem will lead us to some that cannot possibly work.

Theorem 4.4. *If H and K are finite subgroups of a group G, then*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Proof. Considering all possible $h \in H$ and $k \in K$, it is clear that we can produce at most $|H||K|$ elements hk, but we must determine how many times each unique group element appears in such a list. Note that if $h_1k_1 = h_2k_2$, with $h_i \in H$ and $k_i \in K$, then $h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K$. Thus, $h_1 = h_2g$ and $k_2 = gk_1$, for some $g \in H \cap K$. Conversely, if $h_1 = h_2g$ and $k_2 = gk_1$, with $g \in H \cap K$, then $h_1k_1 = h_2gk_1 = h_2gg^{-1}k_2 = h_2k_2$. In other words, each hk will occur once for every element of $H \cap K$. The result follows. □

Example 4.6. Let $G = S_3$ and let H and K be any two different subgroups of order 2. Then $H \cap K$ can only contain the identity, and therefore $|HK| = 4$. But by Lagrange's theorem, a group of order 6 cannot have a subgroup of order 4. Therefore, HK is not a subgroup.

But HK will be a subgroup if either H or K is normal.

Theorem 4.5. *Let H and K be subgroups of G. Then*

1. *if either H or K is normal in G, then HK is a subgroup of G; and*
2. *if both H and K are normal in G, then HK is normal as well.*

Proof. (1) Observe that $e = ee \in HK$. Suppose that H is normal. Let us show closure. If $h_i \in H$ and $k_i \in K$, then

$$(h_1k_1)(h_2k_2) = h_1(k_1h_2k_1^{-1})k_1k_2.$$

Since H is normal, $k_1h_2k_1^{-1} \in H$, and therefore $h_1k_1h_2k_1^{-1} \in H$, $k_1k_2 \in K$, as required. Also,

$$(h_1k_1)^{-1} = k_1^{-1}h_1^{-1} = (k_1^{-1}h_1^{-1}k_1)k_1^{-1}.$$

Again, since H is normal, $k_1^{-1}h_1^{-1}k_1 \in H$, so $(h_1k_1)^{-1} \in HK$. If K is normal, the proof is similar and left as an exercise.

(2) Take $h \in H$, $k \in K$ and $a \in G$. Then

$$a^{-1}hka = (a^{-1}ha)(a^{-1}ka).$$

But $a^{-1}ha \in H$ and $a^{-1}ka \in K$. Thus, $a^{-1}hka \in HK$. □

Exercises

4.1. Is each of the following sets a normal subgroup of $GL_2(\mathbb{R})$?

1. $H = \{A \in GL_2(\mathbb{R}) : \det(A) \in \mathbb{Q}\}$
2. the set of diagonal matrices $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ in $GL_2(\mathbb{R})$

4.2. Find every normal subgroup of S_3.

4.3. If N is a normal subgroup of G, and $|N| = 2$, show that $N \leq Z(G)$.

4.4. Let N be a normal subgroup of G. Let H be the set of all elements h of G such that $hn = nh$ for all $n \in N$. Show that H is a normal subgroup of G.

4.5. Show that the intersection of two normal subgroups of G is also a normal subgroup. Then extend this to show that if N_i is a normal subgroup of G for every i in some set T, then $\bigcap_{i \in T} N_i$ is a normal subgroup of G.

4.6. Let $N_1 \leq N_2 \leq N_3 \leq \cdots$ be normal subgroups of G. Show that $\bigcup_{i=1}^{\infty} N_i$ is a normal subgroup of G.

4.7. Let G be a group having exactly one subgroup H of order n. Show that H is normal in G.

4.8. Let $G = H \times K$. If N is a normal subgroup of H and L is a normal subgroup of K, show that $N \times L$ is a normal subgroup of G. Is every normal subgroup of G of this form?

4.9. Suppose that H is a subgroup of G and $a^{-1}b^{-1}ab \in H$, for all $a, b \in G$. Show that H is normal.

4.10. Let H and K be subgroups of G. Show that HK is a subgroup if and only if $HK = KH$.

4.2 Factor Groups

We are now in a position to construct a new sort of group.

Definition 4.4. Let G be a group and N a normal subgroup. Then the **factor group** (or **quotient group**) G/N is the set of all left cosets aN, with $a \in G$, under the operation $(aN)(bN) = abN$.

The fact that the factor group is indeed a group needs proving. Then we can look at some examples.

Theorem 4.6. *If G is any group and N is a normal subgroup, then G/N is a group of order $[G : N]$.*

Proof. The main point is to verify that the operation is well-defined. The rest will follow easily from the fact that G is a group. In other words, suppose that $a_1N = a_2N$ and $b_1N = b_2N$. We must show that $a_1b_1N = a_2b_2N$. Otherwise, this operation is nonsensical. But as $a_1N = a_2N$, we have $a_1^{-1}a_2 = n_1$, for some $n_1 \in N$. Similarly, $b_1^{-1}b_2 = n_2 \in N$. Then

$$(a_1b_1)^{-1}a_2b_2 = b_1^{-1}a_1^{-1}a_2b_2 = b_1^{-1}n_1b_2 = (b_1^{-1}n_1b_1)(b_1^{-1}b_2) = b_1^{-1}n_1b_1n_2.$$

Now, as N is normal, $b_1^{-1}n_1b_1 \in N$. Thus, $(a_1b_1)^{-1}a_2b_2 \in N$, which means that $a_1b_1N = a_2b_2N$, as required.

Let us check the group properties. As for closure, if aN and bN are left cosets, then so is abN. Also, for any $a, b, c \in G$, we have

$$aN(bNcN) = aNbcN = a(bc)N = (ab)cN = (aNbN)cN,$$

so associativity is proved. If $a \in G$, then $aNeN = aN = eNaN$; thus, eN is the identity of G/N. Finally, $aNa^{-1}N = eN = a^{-1}NaN$; that is, $a^{-1}N$ is the inverse of aN. Therefore, G/N is a group. The group consists of the left cosets, so the order is the number of left cosets, which is $[G : N]$. The proof is complete. □

Notice that the proposed group operation would not even be well-defined if N were not a normal subgroup.

Example 4.7. Let $G = U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$, and let $N = \langle 14 \rangle = \{1, 14\}$. There is no need to worry about normality, since G is abelian. The left cosets are $1N = \{1, 14\}$, $2N = \{2, 13\}$, $4N = \{4, 11\}$ and $7N = \{7, 8\}$. Thus, $G/N = \{1N, 2N, 4N, 7N\}$. We note that $(4N)(7N) = 13N = 2N$ and $(2N)(4N) = 8N = 7N$. The rest of the group table is given in Table 4.1. We can also use this table to find inverses; for instance, $2N7N = 1N$. Since $1N$ is the identity, $(2N)^{-1} = 7N$.

Table 4.1 Group table for $U(15)/\langle 14 \rangle$

	$1N$	$2N$	$4N$	$7N$
$1N$	$1N$	$2N$	$4N$	$7N$
$2N$	$2N$	$4N$	$7N$	$1N$
$4N$	$4N$	$7N$	$1N$	$2N$
$7N$	$7N$	$1N$	$2N$	$4N$

Example 4.8. Let $G = \mathbb{Z}$ and $N = 5\mathbb{Z}$. Again, N is certainly a normal subgroup of G. Also, $G/N = \{0 + N, 1 + N, 2 + N, 3 + N, 4 + N\}$. Addition in the factor group behaves like modular arithmetic; indeed, $(1 + N) + (2 + N) = 3 + N$ and $(3 + N) + (4 + N) = 7 + N = 2 + N$. The full group table is given in Table 4.2. Note that $\mathbb{Z}/5\mathbb{Z}$ has precisely the same group table as $\mathbb{Z}_5$ (see Table 3.1).

Table 4.2 Group table for $\mathbb{Z}/5\mathbb{Z}$

	$0+N$	$1+N$	$2+N$	$3+N$	$4+N$
$0+N$	$0+N$	$1+N$	$2+N$	$3+N$	$4+N$
$1+N$	$1+N$	$2+N$	$3+N$	$4+N$	$0+N$
$2+N$	$2+N$	$3+N$	$4+N$	$0+N$	$1+N$
$3+N$	$3+N$	$4+N$	$0+N$	$1+N$	$2+N$
$4+N$	$4+N$	$0+N$	$1+N$	$2+N$	$3+N$

Example 4.9. Let $G = D_8$ and $N = \langle R_{90} \rangle$. As N has index 2, it is necessarily a normal subgroup, by Theorem 4.1. In fact, there are only two left cosets, R_0N, which consists of all of the rotations, and F_1N, which consists of all of the flips. The group table is given in Table 4.3.

Table 4.3 Group table for $D_8/\langle R_{90} \rangle$

	R_0N	F_1N
R_0N	R_0N	F_1N
F_1N	F_1N	R_0N

Observe that powers of group elements in a quotient group work as we would expect. Indeed, $(aN)^m = a^mN$, for any integer m. In particular, $(aN)^{-1} = a^{-1}N$. Let us prove a few other useful facts.

Theorem 4.7. *Let G be a group, with $a \in G$ and N a normal subgroup of G. Then*

1. *if G is abelian, then so is G/N;*
2. *if G is cyclic, then so is G/N; and*
3. *if $|a| = m < \infty$, then $|aN|$ divides m.*

Proof. (1) If $b, c \in G$, then $(bN)(cN) = bcN = cbN = (cN)(bN)$.

(2) If $G = \langle b \rangle$, then for any $cN \in G/N$, let us say that $c = b^k$. Then $cN = b^kN = (bN)^k$. Thus, $G/N = \langle bN \rangle$.

(3) Note that $(aN)^m = a^mN = eN$. Thus, by Corollary 3.2, the order of aN divides m. □

A small word of caution is in order. Do not assume that the order of a equals that of aN. All we know is that $|aN|$ divides $|a|$. Also, if a has infinite order, then we know nothing about $|aN|$; it could be finite or infinite.

The following theorem tells us how to determine the subgroups of a factor group. The proof, however, is left as Exercise 4.18.

Theorem 4.8. *Let G be a group and N a normal subgroup. Then the subgroups of G/N are precisely of the form H/N, where H is a subgroup of G containing N. Furthermore, H/N is normal in G/N if and only if H is normal in G.*

Here is one more rather neat fact about factor groups.

Theorem 4.9. *Let G be any group. If $G/Z(G)$ is cyclic, then G is abelian.*

Proof. Let $Z = Z(G)$, and suppose that $G/Z = \langle aZ \rangle$. Take any $b, c \in G$. Then $bZ = a^mZ$, for some integer m, and $cZ = a^nZ$, for some integer n. Thus, $b = a^my$ and $c = a^nz$, for some $y, z \in Z$. But noting that powers of a commute with each other and elements of Z commute with everything, we have $bc = a^mya^nz = a^nza^my = cb$. Thus, G is abelian. □

Corollary 4.1. *The centre of a group cannot have prime index in that group.*

Proof. If $G/Z(G)$ has prime order, then by Corollary 3.6, $G/Z(G)$ is cyclic. But then the preceding theorem tells us that G is abelian; therefore, $Z(G) = G$ has index 1, which is not prime. □

Note that it is entirely possible for G to be nonabelian but $G/Z(G)$ to be abelian. See Exercise 4.13.

Exercises

4.11. Let G be a group having a normal subgroup N. Suppose that in G/N, the order of aN is 5. If $|N| = 14$, what are the possible orders of a? Show that each order you find can actually occur in some group.

4.12. Write the group table for

1. $D_8/\langle R_{180}\rangle$
2. $U(40)/\langle 3\rangle$.

4.13. Find a nonabelian group G such that

1. $G/Z(G)$ is abelian
2. G is infinite, but $G/Z(G)$ is finite.

4.14. Show that an element of the factor group $\mathbb{R}/\mathbb{Z}$ has finite order if and only if it is in $\mathbb{Q}/\mathbb{Z}$.

4.15. Let G be a finite group having a normal subgroup N. If G/N has an element of order 42, show that G has an element of order 42. Does the same hold for infinite groups?

4.16. Let N be a normal subgroup of G. Show that G/N is abelian if and only if $a^{-1}b^{-1}ab \in N$ for all $a, b \in G$.

4.17. Suppose that G has normal subgroups K and N such that G/K and G/N are abelian. If $K \cap N = \{e\}$, show that G is abelian.

4.18. Let G have a normal subgroup N. Show that the subgroups of G/N are precisely of the form H/N, where H is a subgroup of G with $N \subseteq H$. Furthermore, show that H is normal in G if and only if H/N is normal in G/N.

4.19. Let G be an abelian group. Show that the elements of finite order in G form a normal subgroup N, and that the only element of finite order in G/N is the identity.

4.20. Let G be a nonabelian group. Show that there exists a subgroup H of G such that $Z(G) \subsetneq H \subsetneq G$.

4.3 Homomorphisms

We would like to talk about functions from one group to another. But an arbitrary function is not necessarily very useful. We need it to respect the group operation. This is the first step towards our goal (realized in the next section) of describing a way of determining if two groups have the same structure.

Definition 4.5. Let G and H be groups. Then a **group homomorphism** (or, simply, **homomorphism**) from G to H is a function $\alpha : G \to H$ such that

$$\alpha(g_1 g_2) = \alpha(g_1)\alpha(g_2)$$

for all $g_1, g_2 \in G$.

Note that in the above definition, the product $g_1 g_2$ is the product in G, whereas the product $\alpha(g_1)\alpha(g_2)$ takes place in H. These group operations need not be the same.

Definition 4.6. If $\alpha : G \to H$ is a homomorphism, then the **kernel** of α is the set

$$\ker(\alpha) = \{g \in G : \alpha(g) = e\}.$$

Example 4.10. If $n \geq 2$ is a positive integer, then $\alpha : \mathbb{Z} \to \mathbb{Z}_n$ given by $\alpha(a) = [a]$ (where we insert the equivalence class brackets for clarity) is a homomorphism. Indeed, $\alpha(a + b) = [a + b] = [a] + [b] = \alpha(a) + \alpha(b)$, for all $a, b \in \mathbb{Z}$. Here, $\ker(\alpha) = \{a \in \mathbb{Z} : [a] = [0]\} = n\mathbb{Z}$.

Example 4.11. Let G be the additive group of integers, and let H be the multiplicative group of nonzero rational numbers. Then the function $\alpha : G \to H$ given by $\alpha(a) = 2^a$ is a homomorphism. To check this, we had first better verify that α does indeed map G into H. But if a is an integer, then 2^a is a nonzero rational number. Also, $\alpha(a + b) = 2^{a+b} = 2^a 2^b = \alpha(a)\alpha(b)$, as required. We see that $\ker(\alpha) = \{a \in \mathbb{Z} : 2^a = 1\} = \{0\}$.

Example 4.12. Let G be any group, and consider the map $\alpha : G \times G \to G$ given by $\alpha((g_1, g_2)) = g_2$. Then α is a homomorphism. Indeed, if $g_i \in G$, then

$$\alpha((g_1, g_2)(g_3, g_4)) = \alpha((g_1 g_3, g_2 g_4)) = g_2 g_4,$$

and this is also equal to $\alpha((g_1, g_2))\alpha((g_3, g_4))$. Furthermore, the kernel is $\{(g, e) : g \in G\} = G \times \{e\}$.

Example 4.13. If G and H are any groups, then $\alpha : G \to H$ given by $\alpha(g) = e$ for all $g \in G$ is a homomorphism. Indeed, $\alpha(g_1 g_2) = e$, and $\alpha(g_1)\alpha(g_2) = e^2 = e$. The kernel of α is all of G.

We can give a few basic properties of homomorphisms.

Theorem 4.10. *Let $\alpha : G \to H$ be a homomorphism, and take any $g \in G$. Then*

1. $\alpha(e) = e$;
2. $\alpha(g^n) = (\alpha(g))^n$, *for any integer* n; *and*
3. *if* $|g| = m < \infty$, *then the order of* $\alpha(g)$ *divides* m.

Proof. (1) Note that

$$\alpha(e) = \alpha(ee) = \alpha(e)\alpha(e).$$

Cancelling, we find that $\alpha(e)$ is the identity of H.

(2) If $n > 0$, then note that

$$\alpha(g^n) = \alpha(\underbrace{gg \cdots g}_{n \text{ times}}) = \underbrace{\alpha(g)\alpha(g) \cdots \alpha(g)}_{n \text{ times}} = (\alpha(g))^n.$$

If $n = 0$, then use part (1). If $n = -1$, then note that

$$\alpha(g)\alpha(g^{-1}) = \alpha(gg^{-1}) = \alpha(e) = e.$$

Similarly, $\alpha(g^{-1})\alpha(g) = e$. Therefore, $\alpha(g^{-1}) = (\alpha(g))^{-1}$. Combining what we already know, the case where $n < -1$ follows immediately.

(3) We have $(\alpha(g))^m = \alpha(g^m) = \alpha(e) = e$. Thus, by Corollary 3.2, the order of $\alpha(g)$ divides m. □

The kernel of a homomorphism is rather important, as the following result suggests.

Theorem 4.11. *Let $\alpha : G \to H$ be a homomorphism. Then*

1. $\ker(\alpha)$ *is a normal subgroup of* G; *and*
2. α *is one-to-one if and only if* $\ker(\alpha) = \{e\}$.

Proof. Let $K = \ker(\alpha)$. Let us show that K is a subgroup of G. By Theorem 4.10, $\alpha(e) = e$, so $e \in K$. Suppose $k_1, k_2 \in K$. Then $\alpha(k_1k_2) = \alpha(k_1)\alpha(k_2) = ee = e$; hence, $k_1k_2 \in K$. Also, $\alpha(k_1^{-1}) = (\alpha(k_1))^{-1} = e^{-1} = e$. Thus, $k_1^{-1} \in K$, and K is a subgroup. If $k \in K$ and $g \in G$, then

$$\alpha(g^{-1}kg) = \alpha(g^{-1})\alpha(k)\alpha(g) = \alpha(g^{-1})e\alpha(g) = (\alpha(g))^{-1}\alpha(g) = e.$$

Therefore, $g^{-1}kg \in K$, and K is normal.

Now, suppose that α is one-to-one. Since $\alpha(e) = e$, we know that if $\alpha(g) = e$, then $g = e$. Therefore, the kernel is simply $\{e\}$. Conversely, suppose that $\ker(\alpha) = \{e\}$. If $\alpha(g_1) = \alpha(g_2)$, then $\alpha(g_1)(\alpha(g_2))^{-1} = e$. But this means that $\alpha(g_1g_2^{-1}) = e$, and therefore $g_1g_2^{-1} \in K = \{e\}$. That is, $g_1 = g_2$, and α is one-to-one. □

Two other sorts of subgroups are also useful.

Definition 4.7. Let $\alpha : G \to H$ be a homomorphism. If L is any subgroup of G, then the **image** of L is $\alpha(L) = \{\alpha(l) : l \in L\}$. If M is any subgroup of H, then the **preimage** (or **inverse image**) of M is the set $\alpha^{-1}(M) = \{g \in G : \alpha(g) \in M\}$.

Note that the use of the notation $\alpha^{-1}(M)$ does not imply that the function α is invertible. It may or may not be.

Example 4.14. Consider Example 4.11. If $L = 3\mathbb{Z}$, then $\alpha(L) = \{2^{3a} : a \in \mathbb{Z}\} = \{8^a : a \in \mathbb{Z}\}$. If $M = \{\pm 4^a : a \in \mathbb{Z}\}$, then $\alpha^{-1}(M) = 2\mathbb{Z}$.

Example 4.15. Let $G = \mathbb{Z}$, and consider $\alpha : G \times G \to G$, as in Example 4.12. Let $L = 3\mathbb{Z} \times 5\mathbb{Z}$. Then $\alpha(L) = 5\mathbb{Z}$. If $M = 6\mathbb{Z}$, then $\alpha^{-1}(M) = \mathbb{Z} \times 6\mathbb{Z}$.

We conclude with a few properties of images and preimages.

Theorem 4.12. *Let $\alpha : G \to H$ be a homomorphism. Then*

1. *if L is a subgroup of G, then $\alpha(L)$ is a subgroup of H;*
2. *if L is normal in G, then $\alpha(L)$ is normal in $\alpha(G)$;*
3. *if L is cyclic, then $\alpha(L)$ is cyclic;*
4. *if L is abelian, then $\alpha(L)$ is abelian;*
5. *α is onto if and only if $\alpha(G) = H$;*
6. *if $M \leq H$, then $\alpha^{-1}(M) \leq G$; and*
7. *if M is a normal subgroup of H, then $\alpha^{-1}(M)$ is normal in G.*

Proof. (1) We have $e \in L$, so $e = \alpha(e) \in \alpha(L)$. If $\alpha(l_1), \alpha(l_2) \in \alpha(L)$, then $\alpha(l_1)\alpha(l_2) = \alpha(l_1 l_2) \in \alpha(L)$, since $l_1 l_2 \in L$. Also, $(\alpha(l_1))^{-1} = \alpha(l_1^{-1}) \in \alpha(L)$, since $l_1^{-1} \in L$.

(2) If $l \in L, g \in G$, then $(\alpha(g))^{-1}\alpha(l)\alpha(g) = \alpha(g^{-1}lg) \in \alpha(L)$, since $g^{-1}lg \in L$.

(3) If $L = \langle k \rangle$, then for any $\alpha(l) \in \alpha(L)$, we have $l = k^m$, for some integer m. Then $\alpha(l) = \alpha(k^m) = (\alpha(k))^m$. Thus, $\alpha(L) = \langle \alpha(k) \rangle$.

(4) If $l_1, l_2 \in L$, then $\alpha(l_1)\alpha(l_2) = \alpha(l_1 l_2) = \alpha(l_2 l_1) = \alpha(l_2)\alpha(l_1)$.

(5) This is the definition of "onto".

(6) Notice that $\alpha(e) = e \in M$; hence, $e \in \alpha^{-1}(M)$. Also, if $g_1, g_2 \in \alpha^{-1}(M)$, then $\alpha(g_1 g_2) = \alpha(g_1)\alpha(g_2) \in M$, since $\alpha(g_1), \alpha(g_2) \in M$. Thus, $g_1 g_2 \in \alpha^{-1}(M)$. Furthermore, $\alpha(g_1^{-1}) = (\alpha(g_1))^{-1} \in M$, since $\alpha(g_1) \in M$. Thus, $g_1^{-1} \in \alpha^{-1}(M)$.

(7) Take $a \in \alpha^{-1}(M), g \in G$. Then $\alpha(g^{-1}ag) = (\alpha(g))^{-1}\alpha(a)\alpha(g) \in M$, since $\alpha(a) \in M$ and M is normal. Thus, $g^{-1}ag \in \alpha^{-1}(M)$. □

Exercises

4.21. Are α and β, described below, homomorphisms? If so, are they one-to-one and onto?

1. G is the group of positive real numbers under multiplication, H is $\mathbb{R}$ (under addition), $\alpha : G \to H$ via $\alpha(a) = \log_{10} a$
2. $\beta : \mathbb{Z} \to \mathbb{Z}$, $\beta(a) = a + 1$

4.22. Let $\alpha : \mathbb{Z}_9 \times \mathbb{Z}_{27} \to \mathbb{Z}_{27}$ be given by $\alpha((a, b)) = 3b$, for all $a \in \mathbb{Z}_9$, $b \in \mathbb{Z}_{27}$. Show that α is a homomorphism. Also, find $\ker(\alpha)$, and decide if α is onto.

4.23. Define $\alpha : U(16) \times U(16) \to U(16)$ via $\alpha((a, b)) = ab^{-1}$. Show that α is a homomorphism, and find $\alpha^{-1}(\langle 7 \rangle)$.

4.24. Describe every homomorphism $\alpha : \mathbb{Z}_{10} \to \mathbb{Z}_{15}$.

4.25. Let G be a finite group and $\alpha : G \to H$ an onto homomorphism.

1. If G has an element of order n, must H have one?
2. If H has an element of order n, must G have one?

4.26. Let $\alpha : G \to H$ be a homomorphism, and suppose that $\alpha(g) = h$. For any $a \in G$, show that $\alpha(a) = h$ if and only if $a = gk$ for some $k \in \ker(\alpha)$.

4.27. Define $\alpha : G \times G \to G$ via $\alpha((g, h)) = gh$. If α is a homomorphism, show that G is abelian.

4.28. Show that a group G is cyclic if and only if there exists an onto homomorphism from $\mathbb{Z}$ to G.

4.29. Let N be a normal subgroup of G. Show that there exist a group H and a homomorphism $\alpha : G \to H$ with kernel N.

4.30. Let G be the multiplicative group of nonzero complex numbers and H the multiplicative group of nonzero real numbers. Does there exist a one-to-one homomorphism from G to H?

4.4 Isomorphisms

One of our goals is to establish if two groups are, in effect, the same. To this end, we need to strengthen the notion of a homomorphism.

Definition 4.8. Let G and H be groups. Then a **group isomorphism** (or, simply, **isomorphism**) from G to H is a homomorphism from G to H that is bijective. When such an isomorphism exists, we say that G and H are **isomorphic** groups.

Isomorphic groups have precisely the same structure. The isomorphism simply provides new labels for the group elements.

Theorem 4.13. *On any collection of groups, isomorphism is an equivalence relation.*

Proof. Reflexivity: Use the function $\alpha : G \to G$ given by $\alpha(g) = g$ for all g. It is easily seen to be an isomorphism. Symmetry: Suppose that $\alpha : G \to H$ is an isomorphism. By Theorem 1.3, there exists a function $\beta : H \to G$ given by $\beta(h) = g$, where $\alpha(g) = h$, and this β is also bijective. We must check that it is a homomorphism. Take any $h_1, h_2 \in H$, and suppose that $\beta(h_i) = g_i$. Then $\alpha(g_1 g_2) = \alpha(g_1)\alpha(g_2) = h_1 h_2$; thus, $\beta(h_1 h_2) = g_1 g_2 = \beta(h_1)\beta(h_2)$, as required. Transitivity: Suppose that $\alpha : G \to H$ and $\beta : H \to K$ are isomorphisms. Let $\gamma = \beta \circ \alpha$. By Theorem 1.2, γ is bijective. We must check that it is a homomorphism. Take any $g_1, g_2 \in G$. Then

$$\gamma(g_1 g_2) = \beta(\alpha(g_1 g_2)) = \beta(\alpha(g_1)\alpha(g_2)) = \beta(\alpha(g_1))\beta(\alpha(g_2)) = \gamma(g_1)\gamma(g_2).$$

We are done. □

Therefore, it makes sense to say that G and H are isomorphic; we do not have to specify that G is isomorphic to H. In order to verify that a particular function is an isomorphism, we have to check three things: it must respect the group operation, it must be one-to-one and it must be onto. We can use Theorem 4.11 for the second of these; to show that it is one-to-one, it is enough to show that the kernel is trivial.

Example 4.16. Let us show that $\mathbb{Z}_3 \times \mathbb{Z}_5$ and $\mathbb{Z}_{15}$ are isomorphic groups. We define $\alpha : \mathbb{Z}_{15} \to \mathbb{Z}_3 \times \mathbb{Z}_5$ via $\alpha(a) = (a, a)$. First, is this well-defined? If $a = b$ in $\mathbb{Z}_{15}$, then $15|(a-b)$, so $3|(a-b)$ and $5|(a-b)$, and therefore $(a, a) = (b, b)$ in $\mathbb{Z}_3 \times \mathbb{Z}_5$. Check that it is a homomorphism. If $a, b \in \mathbb{Z}_{15}$, then $\alpha(a+b) = (a+b, a+b) = (a, a) + (b, b) = \alpha(a) + \alpha(b)$. Next, let us show that it is one-to-one. If $a \in \ker(\alpha)$, then $(a, a) = (0, 0)$. That is, $3|a$ and $5|a$. Therefore, $15|a$, so $a = 0$ in $\mathbb{Z}_{15}$, and α is one-to-one. In this case, we do not need to check surjectivity, because the 15 elements of $\mathbb{Z}_{15}$ map to 15 different elements of $\mathbb{Z}_3 \times \mathbb{Z}_5$. But $\mathbb{Z}_3 \times \mathbb{Z}_5$ only has 15 elements! Hence, the function must be onto.

Example 4.17. Lest we get too comfortable, $\mathbb{Z}_{24}$ is not isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_6$. Why not? Notice that 1 has order 24 in $\mathbb{Z}_{24}$. If these groups had precisely the same structure, then $\mathbb{Z}_4 \times \mathbb{Z}_6$ would have to have an element of order 24 as well. But it is easy to see that $12(a, b) = (0, 0)$ for every $(a, b) \in \mathbb{Z}_4 \times \mathbb{Z}_6$, so every element has order dividing 12.

Example 4.18. As we noted following Example 3.4, the set $G = \{1, -1, i, -i\}$ (where i is the complex number) is a group under multiplication. We claim that it is isomorphic to the additive group $\mathbb{Z}_4$. To see this, we define $\alpha : \mathbb{Z}_4 \to G$ via $\alpha(0) = 1$, $\alpha(1) = i$, $\alpha(2) = -1$ and $\alpha(3) = -i$. This function is clearly bijective, and we can check that it respects the group operations by comparing the group tables. The tables for $\mathbb{Z}_4$ and G are shown in Tables 4.4 and 4.5. Note that if we replace 0 and $\alpha(0)$ with A, 1 and $\alpha(1)$ with B, and so on, we see that both groups have Table 4.6. Thus, α is just a relabelling of the group elements.

In fact, we can classify all cyclic groups up to isomorphism.

Table 4.4 Group table for the additive group $\mathbb{Z}_4$

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Table 4.5 Group table for the multiplicative group $\{1, -1, i, -i\}$

	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Table 4.6 Group table for both Tables 4.4 and 4.5 after relabelling

	A	B	C	D
A	A	B	C	D
B	B	C	D	A
C	C	D	A	B
D	D	A	B	C

Theorem 4.14. *Let $G = \langle a \rangle$ be a cyclic group. If a has infinite order, then G is isomorphic to $\mathbb{Z}$. If a has order $n < \infty$, then G is isomorphic to $\mathbb{Z}_n$.*

Proof. Let G be infinite cyclic. Define $\alpha : \mathbb{Z} \to G$ via $\alpha(i) = a^i$. We claim that α is an isomorphism. If $i, j \in \mathbb{Z}$, then $\alpha(i + j) = a^{i+j} = a^i a^j = \alpha(i)\alpha(j)$, as required. If $i \in \ker(\alpha)$, then $a^i = e = a^0$. By Theorem 3.8, $i = 0$. Thus, α is one-to-one. Furthermore, if $i \in \mathbb{Z}$, then $a^i \in \alpha(\mathbb{Z})$, as $\alpha(i) = a^i$. Thus, α is onto as well, and therefore an isomorphism.

Now suppose that $|a| = n < \infty$. Define $\alpha : \mathbb{Z}_n \to G$ via $\alpha(i) = a^i$. Here, we must check that α is well-defined. But if $i = j$ in $\mathbb{Z}_n$, then $n|(i - j)$. Thus, by Theorem 3.8, $a^i = a^j$. The fact that α is an onto homomorphism follows as above. If $i \in \ker(\alpha)$, then $a^i = e$, and by Corollary 3.2, n divides i. Thus, in $\mathbb{Z}_n$, $i = 0$. □

Corollary 4.2. *If a group G has prime order p, then G is isomorphic to $\mathbb{Z}_p$.*

Proof. Combine Corollary 3.6 and Theorem 4.14. □

So, groups of prime order have as nice a structure as we could ask. With a little more work, we can also classify the groups with order twice a prime.

Lemma 4.1. *Let G be a group having distinct commuting elements a and b of order 2. Then G has a subgroup isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.*

Proof. Given the conditions upon a and b, we can see that $H = \{e, a, b, ab\}$ is a subgroup. (It contains the identity, and closure is easily checked.) Also, H contains four distinct elements. (Clearly, e, a and b are distinct. If $ab = e = bb$, then $a = b$. If $ab = a = ae$, then $b = e$. If $ab = b = eb$, then $a = e$. These are all impossible.) We claim that it is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. Let $\alpha : H \to \mathbb{Z}_2 \times \mathbb{Z}_2$ be given by $\alpha(e) = (0, 0)$, $\alpha(a) = (1, 0)$, $\alpha(b) = (0, 1)$ and $\alpha(ab) = (1, 1)$. This function is clearly bijective, and running through the possible pairs of group elements, we see that it is a homomorphism. □

Corollary 4.3. *Every group G of order 4 is isomorphic to either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.*

Proof. In a group of order 4, every nonidentity element has order 2 or 4. If there is an element of order 4, G is cyclic and, by Theorem 4.14, isomorphic to $\mathbb{Z}_4$. Otherwise, every nonidentity element has order 2. By Exercise 3.32, G is abelian, and the preceding lemma tells us that G has a subgroup isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. Given the order of the group, we are done. □

When p is a prime larger than 2, we are already aware of two possible groups of order $2p$; the cyclic group and the dihedral one. In fact, those are all of the options.

Theorem 4.15. *Let $|G| = 2p$, where p is an odd prime. Then G is isomorphic to either $\mathbb{Z}_{2p}$ or D_{2p}.*

Proof. The possible orders for nonidentity elements of G are 2, p and $2p$. If G has an element of order $2p$ then it is cyclic and, by Theorem 4.14, isomorphic to $\mathbb{Z}_{2p}$. So, assume that every nonidentity element has order 2 or p.

If every nonidentity element has order 2, then once again, G is abelian and, by Lemma 4.1, G has a subgroup of order 4, contradicting Lagrange's theorem. Therefore, let $a \in G$ have order p. Take any $b \notin \langle a \rangle$. Suppose that $|b| = p$. Then noting that $\langle a \rangle \cap \langle b \rangle$ is a subgroup of both $\langle a \rangle$ and $\langle b \rangle$ (see Exercise 3.37), Lagrange's theorem tells us that it can only have order 1 or p. As $b \notin \langle a \rangle$, it must be 1. Thus, by Theorem 4.4, $|\langle a \rangle \langle b \rangle| = |\langle a \rangle||\langle b \rangle|/|\langle a \rangle \cap \langle b \rangle| = p^2/1 = p^2$. But this exceeds the order of G. Therefore, $|b| = 2$.

Now, as $\langle a \rangle$ has index 2, Theorem 4.1 tells us that it is normal. Thus, $b^{-1}ab \in \langle a \rangle$, say $b^{-1}ab = a^i$. But then

$$a = b^{-2}ab^2 = b^{-1}(b^{-1}ab)b = b^{-1}a^ib = (b^{-1}ab)^i = (a^i)^i = a^{i^2}.$$

As a has order p, we have $i^2 \equiv 1 \pmod{p}$. That is, $p|(i^2 - 1) = (i - 1)(i + 1)$. As p is prime, $i \equiv \pm 1 \pmod{p}$. Thus, $b^{-1}ab = a$ or a^{-1}.

Suppose that $b^{-1}ab = a$. Then a and b commute. But consider the order of ab. If $(ab)^n = e$, then $a^n = b^{-n} \in \langle a \rangle \cap \langle b \rangle = \{e\}$, as a and b have different prime orders. Thus, $p|n$ and $2|n$, so $2p|n$. That is, ab has order $2p$, which we have excluded. Therefore, $b^{-1}ab = a^{-1}$.

We now know everything about the group. As $\langle a \rangle$ has index 2 and $b \notin \langle a \rangle$, the elements of G are precisely a^i and ba^i, $0 \leq i < p$. Furthermore, we know how to find the product of any two elements. Indeed, $a^i a^j = a^{i+j}$ (reducing the exponent modulo p if necessary), $ba^i a^j = ba^{i+j}$,

$$a^i ba^j = b(b^{-1}a^i b)a^j = b(b^{-1}ab)^i a^j = b(a^{-1})^i a^j = ba^{j-i}$$

and $ba^i ba^j = b(ba^{j-i}) = a^{j-i}$. Thus, we can fill in the entire group table for G, and we have precisely the same group structure as in the dihedral group! Indeed, letting F be any flip in D_{2p}, we define $\alpha : G \to D_{2p}$ via $\alpha(a^i) = R_{360i/p}$ and $\alpha(ba^i) = FR_{360i/p}$. Then α is certainly bijective and it is a homomorphism as well. □

We can also mop up a proof we postponed.

Theorem 4.16. *If m and n are relatively prime, then $U(mn)$ is isomorphic to $U(m) \times U(n)$.*

Proof. Define $\alpha : U(mn) \to U(m) \times U(n)$ via $\alpha(a) = (a, a)$. If $(a, mn) = 1$, then $(a, m) = (a, n) = 1$, so we have $(a, a) \in U(m) \times U(n)$ whenever $a \in U(mn)$. Let us verify that α is well-defined. But if $a = b$ in $\mathbb{Z}_{mn}$, then $mn|(a - b)$, so $m|(a - b)$ and $n|(a - b)$, and therefore $(a, a) = (b, b)$ in $U(m) \times U(n)$. It is also a homomorphism; indeed, if $a, b \in U(mn)$, then $\alpha(ab) = (ab, ab) = (a, a)(b, b) = \alpha(a)\alpha(b)$. Let us check that α is one-to-one. But if $a \in \ker(\alpha)$, then $(a, a) = (1, 1)$ in $U(m) \times U(n)$; that is, $m|(a - 1)$ and $n|(a - 1)$. As m and n are relatively prime, $mn|(a - 1)$. That is, $a = 1$ in $U(mn)$; hence, α is one-to-one. Finally, we must show that α is onto. Take any $(c, d) \in U(m) \times U(n)$. By the Chinese Remainder Theorem, there exists an a such that $a \equiv c \pmod{m}$ and $a \equiv d \pmod{n}$. Furthermore, to show that a is in $U(mn)$, it suffices to show that it is relatively prime to both m and n. Without loss of generality, suppose that $(a, m) = k > 1$. Then as $k|a$ and $k|m$, we see that $k|c$ as well. But then $(c, m) \neq 1$, which is impossible. Therefore, $a \in U(mn)$ and $\alpha(a) = (c, d)$. Thus, α is indeed an isomorphism. □

This gives us the second part of Theorem 3.19.

Corollary 4.4. *If m and n are relatively prime, then $\varphi(mn) = \varphi(m)\varphi(n)$.*

Proof. The order of $U(k)$ is $\varphi(k)$. As isomorphic groups have the same order, the preceding theorem completes the proof. □

We wish to add one more point to Corollary 4.3 and Theorem 4.15. If we are to classify groups of a particular order up to isomorphism, we had better ensure that the groups we have listed are not isomorphic to each other. Proving that two groups are not isomorphic generally involves finding a property that one has but the other lacks. For instance, $\mathbb{Z}_{2p}$ is cyclic for all primes p, but neither $\mathbb{Z}_2 \times \mathbb{Z}_2$ nor D_{2p} is cyclic (indeed, D_{2p} is not even abelian). Some properties that can be useful follow.

Theorem 4.17. *Let G and H be isomorphic groups. Then*

1. *G is abelian if and only if H is abelian;*
2. *G is cyclic if and only if H is cyclic;*
3. *$|G| = |H|$;*
4. *for any positive integer n, G and H have the same number of elements of order n (which could be an infinite number);*
5. *for any positive integer n, G and H have the same number of subgroups of order n (which could be an infinite number); and*
6. *for any positive integer n, G and H have the same number of normal subgroups of order n (which could be an infinite number).*

Proof. Let $\alpha : G \to H$ be an isomorphism. (1) As $\alpha(G) = H$, we see from Theorem 4.12 that if G is abelian, so is H. But the same can be said for $\alpha^{-1} : H \to G$.

(2) Same idea.

(3) An isomorphism is a bijection.

(4) Take $g \in G$ of order n. By Theorem 4.10, $|\alpha(g)|$ divides $|g|$. But by the same argument, $|g| = |\alpha^{-1}(\alpha(g))|$ divides $|\alpha(g)|$. Thus, $|g| = |\alpha(g)|$. That is, the elements of order n in G are in one-to-one correspondence with the elements of order n in H.

(5) Let L be a subgroup of G of order n. Then $\alpha(L)$ is a subgroup of H, and it is isomorphic to L; hence, it has the same order. If M is some other subgroup of G, then since α is one-to-one, $\alpha(M)$ is a different group. Thus, H has at least as many subgroups of order n as G does. But applying α^{-1}, we find that G has at least as many subgroups of order n as H does.

(6) Let L be a normal subgroup of order n in G. Then by Theorem 4.12, $\alpha(L)$ is a normal subgroup of $\alpha(G) = H$. Now proceed as in (5). □

Example 4.19. As $U(10) = \langle 3 \rangle$ is cyclic of order 4, we know that $U(10)$ is isomorphic to $\mathbb{Z}_4$. Now, $U(8)$ is an abelian group of order 4, but it is not cyclic, so it is not isomorphic to $U(10)$. By Corollary 4.3, $U(8)$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Example 4.20. Consider the groups $U(20)$ and $U(8) \times U(3)$. Each is an abelian group of order 8 and neither is cyclic; however, they are not isomorphic. To see this, note that $U(20)$ has exactly three elements of order 2; namely, 9, 11 and 19. However, $U(8) \times U(3)$ has too many elements of order 2; in fact, all seven nonidentity elements have that order.

Exercises

4.31. For each of the following pairs of groups, explain why they are not isomorphic.

1. $\mathbb{Z}_4 \times \mathbb{Z}_4$ and $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
2. $GL_2(\mathbb{R})$ and $\mathbb{R}$
3. $\mathbb{Z}$ and $\mathbb{Z} \times \mathbb{Z}$

4.32. For each of the following pairs of groups, explain why they are or are not isomorphic.

1. $\mathbb{Z}_9 \times \mathbb{Z}_3$ and $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$
2. $\mathbb{Z}_{21}$ and $\mathbb{Z}_3 \times \mathbb{Z}_7$
3. $U(22)$ and $\mathbb{Z}_{10}$
4. D_{20} and $\mathbb{Z}_2 \times \mathbb{Z}_{10}$

4.33. Let G be the set of all matrices of the form $\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$, for all integers a. Show that G is a subgroup of $GL_2(\mathbb{R})$. To what familiar group is it isomorphic?

4.34. Show that $\mathbb{Z}$ is not isomorphic to $\mathbb{Q}$.

4.35. Let $H \leq G$ and $a \in G$. Show that H and $a^{-1}Ha$ are isomorphic.

4.36. Show that $G \times H$ is isomorphic to $H \times G$.

4.37. Show that $\mathbb{Z}$ is isomorphic to a proper subgroup of itself.

4.38. Let G be any group. Let H consist of the same set of elements as G, but with a new operation given by $a * b = ba$, for all a and b. Show that H is a group, and that it is isomorphic to G.

4.39. Consider the group G from Exercise 3.42. Show that it is isomorphic to a proper subgroup of itself.

4.40. Consider the group H from Exercise 3.42. Show that it is isomorphic to the multiplicative group of positive rational numbers.

4.5 The Isomorphism Theorems for Groups

In this section, we will discuss three theorems that can aid us in showing that certain groups are isomorphic. The first of these theorems is the most important, and is used to prove the other two.

Theorem 4.18 (First Isomorphism Theorem for Groups). *Let $\alpha : G \to H$ be a homomorphism. Then $G/\ker(\alpha)$ is isomorphic to $\alpha(G)$.*

Proof. Let $K = \ker(\alpha)$. We know that K is a normal subgroup of G. Define $\beta : G/K \to \alpha(G)$ via $\beta(aK) = \alpha(a)$. We claim that β is an isomorphism.

First, we must show that β is well-defined. Suppose that $aK = bK$. Then $a^{-1}b \in K$, and therefore $\alpha(a^{-1}b) = e$. That is, $(\alpha(a))^{-1}\alpha(b) = e$, so $\alpha(a) = \alpha(b)$. Thus, β is well-defined.

Also, β is a homomorphism. Indeed,

$$\beta(aKbK) = \beta(abK) = \alpha(ab) = \alpha(a)\alpha(b) = \beta(aK)\beta(bK).$$

Next, let us check that β is one-to-one. Suppose that $aK \in \ker(\beta)$. Then $\alpha(a) = e$, which means that $a \in K$, so $aK = eK$. That is, $\ker(\beta) = \{eK\}$, and β is one-to-one.

Finally, we must verify that β is onto. Take $\alpha(a) \in \alpha(G)$. Then $\beta(aK) = \alpha(a)$. We are done. □

The First Isomorphism Theorem is a crucial tool in proving that groups are isomorphic. It is also an enormous time-saver! Whenever we are asked to show that something along the lines of G/N is isomorphic to H, all we need to do is find a homomorphism from G onto H with kernel N. We do not need to define a function on cosets and check that it is well-defined.

Example 4.21. For any integer $n \geq 2$, $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$. Indeed, define $\alpha : \mathbb{Z} \to \mathbb{Z}_n$ via $\alpha(a) = [a]$ (where we insert the equivalence class brackets for clarity). This is a homomorphism, as $\alpha(a+b) = [a+b] = [a]+[b] = \alpha(a)+\alpha(b)$, for all $a, b \in \mathbb{Z}$. Also $\ker(\alpha) = \{a \in \mathbb{Z} : a \equiv 0 \pmod{n}\} = n\mathbb{Z}$. Finally, if $[a] \in \mathbb{Z}_n$, then $\alpha(a) = [a]$, so α is onto. The First Isomorphism Theorem completes the proof.

Example 4.22. We claim that $GL_2(\mathbb{R})/SL_2(\mathbb{R})$ is isomorphic to the multiplicative group of nonzero real numbers, which we denote by H. Indeed, define $\alpha : GL_2(\mathbb{R}) \to H$ via $\alpha(A) = \det(A)$. As an invertible matrix has a nonzero determinant, the image of $GL_2(\mathbb{R})$ is indeed contained in H. Also, if $A, B \in GL_2(\mathbb{R})$, then $\alpha(AB) = \det(AB)$ and since determinants respect products, this is $\det(A)\det(B) = \alpha(A)\alpha(B)$. Thus, α is a homomorphism. By definition, its kernel is $SL_2(\mathbb{R})$. Finally, if $a \in H$, then

$$\alpha\left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}\right) = a,$$

and therefore α is onto. Now we apply the First Isomorphism Theorem.

Example 4.23. Let us show that if G and H are any groups, then $G \times H$ has a factor group isomorphic to G. Define $\alpha : G \times H \to G$ via $\alpha((g,h)) = g$, for all $g \in G$, $h \in H$. Check that α is a homomorphism. If $g_i \in G$, $h_i \in H$, then

$$\alpha((g_1,h_1)(g_2,h_2)) = \alpha((g_1g_2, h_1h_2)) = g_1g_2 = \alpha((g_1,h_1))\alpha((g_2,h_2)).$$

Also, if $g \in G$, then $\alpha((g,e)) = g$, so α is onto. Therefore, $(G \times H)/\ker(\alpha)$ is isomorphic to H. If we wish to specify the group being factored out, note that $\ker(\alpha) = \{(e,h) : h \in H\} = \{e\} \times H$.

Theorem 4.19 (Second Isomorphism Theorem for Groups). *Let G be a group with H and N subgroups, such that N is normal. Then $H/(H \cap N)$ is isomorphic to HN/N.*

Proof. We will show that $H \cap N$ is normal in H by demonstrating that it is the kernel of a homomorphism. Also, by Theorem 4.5, HN is a subgroup of G, since N is normal. Define $\alpha : H \to HN/N$ via $\alpha(h) = hN$. As $H \subseteq HN$, we see that $hN \in HN/N$. Observe that α is a homomorphism. Indeed, if $h_1, h_2 \in H$, then $\alpha(h_1h_2) = h_1h_2N = (h_1N)(h_2N) = \alpha(h_1)\alpha(h_2)$. Also, if $hn \in HN$, then $\alpha(h) = hN = hnN$, since $h^{-1}hn = n \in N$. Thus, α is onto. Finally, $\ker(\alpha) = \{h \in H : hN = eN\} = \{h \in H : h \in N\} = H \cap N$. The First Isomorphism Theorem finishes the proof. □

Theorem 4.20 (Third Isomorphism Theorem for Groups). *Let G be a group and suppose that N and K are normal subgroups, with $K \subseteq N$. Then $(G/K)/(N/K)$ is isomorphic to G/N.*

Proof. Define $\alpha : G/K \to G/N$ via $\alpha(aK) = aN$, for any $a \in G$. First, let us check that this is well-defined. But if $aK = bK$, then $a^{-1}b \in K \subseteq N$, so $aN = bN$. Next, let us show that α is a homomorphism. But

$$\alpha((aK)(bK)) = \alpha(abK) = abN = (aN)(bN) = \alpha(aK)\alpha(bK).$$

Furthermore, if $aN \in G/N$, then $\alpha(aK) = aN$, so α is onto. Finally,

$$\ker(\alpha) = \{aK \in G/K : aN = eN\} = \{aK \in G/K : a \in N\} = N/K.$$

We now apply the First Isomorphism Theorem. □

Example 4.24. The Third Isomorphism Theorem tells us that $(\mathbb{Z}/12\mathbb{Z})/(4\mathbb{Z}/12\mathbb{Z})$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}$. (Admittedly, we could have worked this out by noting that $\mathbb{Z}$ is cyclic, so its factor group is cyclic, and the factor group of the factor group is cyclic, and that every cyclic group of order 4 is isomorphic to $\mathbb{Z}_4$, which in turn is isomorphic to $\mathbb{Z}/4\mathbb{Z}$. But isn't this faster?)

Exercises

4.41. Let $G = \mathbb{Z} \times \mathbb{Z}$ and $N = \{(a, a) : a \in \mathbb{Z}\}$. Show that G/N is isomorphic to $\mathbb{Z}$.

4.42. For any groups G and H, show that $(G \times H)/(G \times \{e\})$ is isomorphic to H.

4.43. Show that $\mathbb{R}/\mathbb{Z}$ is isomorphic to the multiplicative group $H = \{a + bi \in \mathbb{C} : a^2 + b^2 = 1\}$.

4.44. Let G be an abelian group and n a positive integer. Consider the groups H and K from Exercise 3.40. Show that G/H is isomorphic to K.

4.45. Let G be the group from Exercise 3.16.

1. Find $Z(G)$.
2. Show that $G/Z(G)$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}$.

4.46. Let G be a group having subgroups N and K of index 2, such that $N \neq K$.

1. Show that $[N : N \cap K] = 2$.
2. Show that $G/(N \cap K)$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

4.6 Automorphisms

One particular type of isomorphism deserves special mention.

Definition 4.9. Let G be any group. Then an **automorphism** of G is an isomorphism $\alpha : G \to G$. The set of all automorphisms of G is called the **automorphism group** of G, and is denoted $\mathrm{Aut}(G)$.

Example 4.25. Let G be any abelian group. Then the function $\alpha : G \to G$ given by $\alpha(a) = a^{-1}$ for all $a \in G$ is an automorphism. To see that α is a homomorphism, note that $\alpha(ab) = (ab)^{-1} = a^{-1}b^{-1} = \alpha(a)\alpha(b)$. (Note that this would not work if G were nonabelian, as $(ab)^{-1} = b^{-1}a^{-1}$!) If $\alpha(a) = e$, then $a^{-1} = e$, so $a = e$ and α is one-to-one. Also, if $a \in G$, then $\alpha(a^{-1}) = a$. Thus, α is onto as well.

Theorem 4.21. *For any group G, the automorphism group of G is a group under composition of functions.*

Proof. As we noted in Theorem 4.13, the composition of two isomorphisms is an isomorphism; therefore, the same follows for automorphisms, so $\mathrm{Aut}(G)$ is closed. By Theorem 1.2, the composition of functions is always associative. Certainly, the identity function that fixes every element of G is an automorphism, and serves as an identity for $\mathrm{Aut}(G)$. Finally, we saw in Theorem 4.13 that every isomorphism has an inverse isomorphism; thus, each automorphism has an inverse. □

Generally speaking, determining $\mathrm{Aut}(G)$ for an arbitrary group G is a difficult problem. But we can, at least, solve it when G is cyclic.

Theorem 4.22. *Let $G = \langle a \rangle$ be a cyclic group. Then*

1. *if a has infinite order, then* $\mathrm{Aut(G)}$ *is isomorphic to $\mathbb{Z}_2$; and*
2. *if $|a| = n < \infty$, then* $\mathrm{Aut(G)}$ *is isomorphic to $U(n)$.*

Proof. Let $\alpha \in \mathrm{Aut}(G)$. If $\alpha(a) = a^i$, then for every $j \in \mathbb{Z}$, we have $\alpha(a^j) = (\alpha(a))^j = (a^i)^j$. In particular, $G = \alpha(G) = \langle a^i \rangle$. Thus, a^i must generate G. Conversely, suppose that $G = \langle a^i \rangle$, and $\alpha(a) = a^i$. Then we can only have $\alpha(a^j) = a^{ij}$ for all integers j. We claim such an α is an automorphism. Indeed,

$$\alpha(a^j a^k) = \alpha(a^{j+k}) = a^{i(j+k)} = a^{ij}a^{ik} = \alpha(a^j)\alpha(a^k),$$

so α is a homomorphism. If $\alpha(a^j) = e$, then $(a^i)^j = e$. If a has infinite order, then $ij = 0$, and therefore $j = 0$. If $|a| = n < \infty$, then $n|ij$. But as $|a| = |a^i| = |G|$, Corollary 3.2 tells us that $(n, i) = 1$. This means that $n|j$, so $a^j = e$. Either way, $\ker(\alpha) = \{e\}$. As a^i is a generator, it follows immediately that α is onto. The claim is proved. Thus, the automorphisms of G are precisely given by $\alpha(a^j) = a^{ij}$, where a^i is a fixed generator of G.

If a has infinite order, then the only generators of $\langle a \rangle$ are a and a^{-1}. Indeed, if a^m were a generator, then we would have to have $a = (a^m)^l$, for some $l \in \mathbb{Z}$. But

then $ml = 1$, which means that $m \in \{1, -1\}$. It is clear, on the other hand, that both a and a^{-1} are generators. Thus, $\mathrm{Aut}(G)$ has order 2. By Corollary 4.2, $\mathrm{Aut}(G)$ is isomorphic to $\mathbb{Z}_2$.

Now suppose that $|a| = n < \infty$. Let us define $\gamma : \mathrm{Aut}(G) \to U(n)$ via $\gamma(\alpha) = i$, where $\alpha(a) = a^i$. Again, Corollary 3.2 tells us that since $|a| = |a^i| = |G|$, we have $(i, n) = 1$, so $i \in U(n)$. Now, if $\alpha, \beta \in \mathrm{Aut}(G)$, with $\alpha(a) = a^i$ and $\beta(a) = a^j$, then

$$(\alpha \circ \beta)(a) = \alpha(\beta(a)) = \alpha(a^j) = (\alpha(a))^j = a^{ij}.$$

Thus, $\gamma(\alpha \circ \beta) = ij$ (reducing modulo n if necessary). But $\gamma(\alpha)\gamma(\beta) = ij$ as well, so γ is a homomorphism. If $\gamma(\alpha) = 1$, then $\alpha(a) = a$, and hence α is the identity automorphism. Therefore, $\ker(\gamma)$ is trivial. Finally, if $i \in U(n)$, then as we have observed, a^i is a generator of G, and we obtain $\alpha \in \mathrm{Aut}(G)$ such that $\alpha(a) = a^i$. Therefore, $\gamma(\alpha) = i$, and γ is onto. Hence, γ is the isomorphism we seek. □

In particular, we see that the automorphism group of a cyclic group is abelian. It would be a mistake to think that the automorphism group of an abelian group is necessarily abelian, as the following example indicates.

Example 4.26. Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. Then define $\alpha : G \to G$ via $\alpha((0, 0)) = (0, 0)$, $\alpha((1, 0)) = (0, 1)$, $\alpha((0, 1)) = (1, 0)$ and $\alpha((1, 1)) = (1, 1)$. Also, let $\beta((0, 0)) = (0, 0)$, $\beta((1, 0)) = (1, 0)$, $\beta((0, 1)) = (1, 1)$ and $\beta((1, 1)) = (0, 1)$. Clearly, α and β are both bijective. The group is also small enough that one can check all of the possibilities and find that they are homomorphisms. Therefore, $\alpha, \beta \in \mathrm{Aut}(G)$. But $\alpha(\beta((1, 0))) = \alpha((1, 0)) = (0, 1)$, whereas $\beta(\alpha((1, 0))) = \beta((0, 1)) = (1, 1)$. Thus, $\alpha \circ \beta \neq \beta \circ \alpha$, so $\mathrm{Aut}(G)$ is nonabelian. In Exercise 4.49, we must show that $\mathrm{Aut}(G)$ is isomorphic to D_6.

Let us define a particular type of automorphism.

Definition 4.10. Let G be a group and $a \in G$. Then the **inner automorphism** induced by a is $\theta_a : G \to G$ given by $\theta_a(g) = a^{-1}ga$ for all $g \in G$. The **inner automorphism group** of G is $\mathrm{Inn}(G) = \{\theta_a : a \in G\}$.

Inner automorphisms are only interesting when the group G is nonabelian; for abelian groups, every inner automorphism is the identity function, as $a^{-1}ga = g$. Let us list a few basic properties of inner automorphisms.

Lemma 4.2. *Let G be a group and $a, b \in G$. Then*

1. $\theta_a \in \mathrm{Aut(G)}$;
2. $\theta_a \circ \theta_b = \theta_{ba}$; *and*
3. $(\theta_a)^{-1} = \theta_{a^{-1}}$.

Proof. (1) First, let us show that θ_a is a homomorphism. If $g, h \in G$, then

$$\theta_a(gh) = a^{-1}gha = (a^{-1}ga)(a^{-1}ha) = \theta_a(g)\theta_a(h).$$

If $\theta_a(g) = e$, then $a^{-1}ga = e$, so $g = aea^{-1} = e$; thus, $\ker(\theta_a) = \{e\}$, and θ_a is one-to-one. Finally, if $g \in G$, then $\theta_a(aga^{-1}) = a^{-1}aga^{-1}a = g$; thus, θ_a is onto.

(2) If $g \in G$, then $\theta_a(\theta_b(g)) = \theta_a(b^{-1}gb) = a^{-1}b^{-1}gba = \theta_{ba}(g)$. Thus, $\theta_a \circ \theta_b = \theta_{ba}$.

(3) If $g \in G$, then $\theta_a(\theta_{a^{-1}}(g)) = \theta_a(aga^{-1}) = a^{-1}aga^{-1}a = g$; thus, $\theta_a \circ \theta_{a^{-1}}$ is the identity function. Similarly, so is $\theta_{a^{-1}} \circ \theta_a$. □

Theorem 4.23. *For any group G,* Inn(G) *is a normal subgroup of* Aut(G).

Proof. By the preceding lemma, $\text{Inn}(G) \subseteq \text{Aut}(G)$. Certainly $\theta_e \in \text{Inn}(G)$ is the identity automorphism. Also, the preceding lemma shows that $\text{Inn}(G)$ is closed under composition and the taking of inverses. Therefore, $\text{Inn}(G) \leq \text{Aut}(G)$. To show normality, take $\alpha \in \text{Aut}(G)$ and $\theta_a \in \text{Inn}(G)$. Then

$$\begin{aligned}(\alpha^{-1} \circ \theta_a \circ \alpha)(g) &= \alpha^{-1}(\theta_a(\alpha(g))) \\ &= \alpha^{-1}(a^{-1}\alpha(g)a) \\ &= \alpha^{-1}(a^{-1})\alpha^{-1}(\alpha(g))\alpha^{-1}(a) \\ &= (\alpha^{-1}(a))^{-1}g\alpha^{-1}(a) \\ &= \theta_{\alpha^{-1}(a)}(g),\end{aligned}$$

for all $g \in G$. That is, $\alpha^{-1} \circ \theta_a \circ \alpha = \theta_{\alpha^{-1}(a)} \in \text{Inn}(G)$, and $\text{Inn}(G)$ is normal. □

It is certainly possible for $\text{Aut}(G)$ to be larger than G; indeed, Example 4.26 provides such a group. But there is only one inner automorphism for each group element. However, θ_a does not have to be different from θ_b if $a \neq b$. For instance, if a and b are both central, then θ_a and θ_b are both equal to the identity automorphism. The following theorem tells the tale.

Theorem 4.24. *Let G be a group. Then*

1. *if $a, b \in G$, then $\theta_a = \theta_b$ if and only if $ba^{-1} \in Z(G)$; and*
2. *$G/Z(G)$ is isomorphic to* Inn(G).

Proof. (1) Take any $a, b \in G$. Then $\theta_a = \theta_b$ if and only if $a^{-1}ga = b^{-1}gb$ for all $g \in G$. But this occurs if and only if $ba^{-1}g = gba^{-1}$ for all $g \in G$. In other words, if and only if ba^{-1} is central.

(2) Define $\alpha : G \to \text{Inn}(G)$ via $\alpha(a) = \theta_{a^{-1}}$. Let us show that α is a homomorphism. If $a, b \in G$, then

$$\alpha(ab) = \theta_{(ab)^{-1}} = \theta_{b^{-1}a^{-1}} = \theta_{a^{-1}} \circ \theta_{b^{-1}} = \alpha(a)\alpha(b),$$

making use of Lemma 4.2. Also, if $\theta_a \in \text{Inn}(G)$, then $\alpha(a^{-1}) = \theta_a$, so α is onto. Furthermore, $a \in \ker(\alpha)$ if and only if $\theta_a = \theta_e$. By (1), this happens if and only if $a = ae^{-1} \in Z(G)$. Now apply the First Isomorphism Theorem. □

Example 4.27. As the centre of S_3 is trivial, we see that $\text{Inn}(S_3)$ is isomorphic to S_3.

Example 4.28. As $Z(D_8) = \langle R_{180} \rangle$, the distinct elements of $\text{Inn}(D_8)$ are of the form θ_a, where we take one a for each left coset of $\langle R_{180} \rangle$ in D_8. That is, $\text{Inn}(D_8) = \{\theta_{R_0}, \theta_{R_{90}}, \theta_{F_1}, \theta_{F_3}\}$. In particular, it is a group of order 4, so by Corollary 4.3, it is isomorphic to either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$. But every flip in D_8 already has order 2, and the square of every rotation is in $Z(D_8)$. Therefore, we see that there is no element of order 4 in $D_8/Z(D_8)$; thus, it must be isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Exercises

4.47. Let G be an abelian group of order n, and let m be a positive integer relatively prime to n. Show that $\alpha : G \to G$ given by $\alpha(a) = a^m$ is an automorphism of G.

4.48. Let G be a group with automorphism α and H a group with automorphism β. Show that $\gamma : G \times H \to G \times H$ given by $\gamma((g, h)) = (\alpha(g), \beta(h))$ is an automorphism.

4.49. Show that the automorphism group of $\mathbb{Z}_2 \times \mathbb{Z}_2$ is isomorphic to D_6.

4.50. Let G and H be isomorphic groups. Show that their automorphism groups are also isomorphic.

4.51. Let α be an automorphism of G. Show that $\{a \in G : \alpha(a) = a\}$ is a subgroup of G.

4.52. Let α and β be any two automorphisms of G. Show that $\{a \in G : \alpha(a) = \beta(a)\}$ is a subgroup of G.

4.53. For any group G, an automorphism α of G is said to be a power automorphism if $\alpha(H) \subseteq H$ for every subgroup H of G. If $G = \langle a \rangle \times \langle b \rangle$ is the direct product of two cyclic groups, and α is a power automorphism of G, show that there exists a $k \in \mathbb{Z}$ such that $\alpha(g) = g^k$ for all $g \in G$.

4.54. To what familiar group is the inner automorphism group of D_{12} isomorphic?

4.55. Let α be an automorphism of $\mathbb{Q}$. Show that for every $q \in \mathbb{Q}$, we have $\alpha(q) = q\alpha(1)$.

4.56. Let G be a group such that the automorphism group of G is trivial.

1. Show that G is abelian.
2. Show that $a^2 = e$ for every $a \in G$.