Theorem 2–38. If f is a homomorphism from the group $(G, *)$ into the group $(G', \circ)$, then

1) f maps the identity element e of $(G, *)$ onto the identity element e' of $(G', \circ)$: $f(e) = e'$,
2) f maps the inverse of an element $a \in G$ onto the inverse of $f(a)$ in $(G', \circ)$: $f(a^{-1}) = f(a)^{-1}$ for each $a \in G$.

Proof. To prove the first assertion, it is enough to observe that under the hypothesis of the theorem,

$$f(a) \circ e' = f(a) = f(a * e) = f(a) \circ f(e),$$

whenever $a \in G$. By the cancellation law in $(G', \circ)$, we then have

$$f(e) = e'.$$

In the second part of the theorem, it is first necessary to show that

$$f(a) \circ f(a^{-1}) = e' = f(a^{-1}) \circ f(a).$$

We can then conclude from the uniqueness of the inverse of $f(a)$ in $(G', \circ)$ that $f(a)^{-1} = f(a^{-1})$. To obtain this result, we make use of part (1) to get

$$f(a) \circ f(a^{-1}) = f(a * a^{-1}) = f(e) = e'.$$

Similarly,

$$f(a^{-1}) \circ f(a) = e'.$$

Example 2–44. As an immediate application of these ideas, we propose to establish that for each real number $r \neq 0$ there is exactly one homomorphism f from the group $(Z, +)$ into the group $(R' - \{0\}, \cdot)$ for which $f(1) = r$. The existence of such a function is trivial, for we need only consider the mapping $f(n) = r^n$, $n \in Z$.

To prove there can be at most one function satisfying the indicated conditions provides a more challenging problem. The basic idea is simple enough: assume there are two functions, f and g, having the required properties, and show that they are actually the same. Now, each positive integer n may be written as

$$n = 1 + 1 + \cdots + 1 \qquad (n \text{ summands}).$$

The operation-preserving character of f and g thus implies

$$f(n) = f(1)^n = r^n = g(1)^n = g(n), \qquad n \in Z_+.$$

On the other hand, if n is a nonzero negative integer, $-n \in Z_+$. Hence,

$$f(n) = f\big(-(-n)\big) = f(-n)^{-1} = g(-n)^{-1} = g\big(-(-n)\big) = g(n).$$

The crucial step, $f(-n) = g(-n)$, is justified by the fact f and g are already known to agree on the positive integers. By the first part of Theorem 2–38, $f(0) = 1 = g(0)$, so that $f(n) = g(n)$ for every integer n; therefore, $f = g$.

The next result indicates the algebraic nature of direct and inverse images of subgroups under homomorphisms. Among other things, we shall see that if f is a homomorphism from the group $(G, *)$ into the group $(G', \circ)$, then $(f(G), \circ)$ forms a subgroup of $(G', \circ)$. The complete story is told below:

Theorem 2–39. Let f be a homomorphism from the group $(G, *)$ into the group $(G', \circ)$. Then

1) for each subgroup $(H, *)$ of $(G, *)$, the pair $(f(H), \circ)$ is a subgroup of $(G', \circ)$,
2) for each subgroup $(H', \circ)$ of $(G', \circ)$, the pair $(f^{-1}(H'), *)$ is a subgroup of $(G, *)$.

Proof. To obtain the first part of the theorem, recall the definition of the image set $f(H)$:

$$f(H) = \{f(h) \mid h \in H\}.$$

Now, suppose $f(h)$ and $f(k)$ are arbitrary elements of $f(H)$. Then both h and k belong to the set H, as does the product $h * k^{-1}$. Hence,

$$f(h) \circ f(k)^{-1} = f(h) \circ f(k^{-1}) = f(h * k^{-1}) \in f(H).$$

Our argument shows that whenever $f(h), f(k) \in f(H)$, then $f(h) \circ f(k)^{-1}$ lies in $f(H)$; this is a sufficient condition for $(f(H), \circ)$ to be a subgroup of $(G', \circ)$.

The proof of the second statement proceeds in a similar manner. First, remember that

$$f^{-1}(H') = \{a \in G \mid f(a) \in H'\}.$$

Thus, if $a, b \in f^{-1}(H')$, the images $f(a)$ and $f(b)$ must be elements of H'. It follows at once that

$$f(a * b^{-1}) = f(a) \circ f(b^{-1}) = f(a) \circ f(b)^{-1} \in H'.$$

This means $a * b^{-1} \in f^{-1}(H')$, from which we conclude $(f^{-1}(H'), *)$ is a subgroup of $(G, *)$.

Left unresolved, as yet, is the matter of replacing the term "subgroup" in Theorem 2–39 by "normal subgroup." It is not particularly difficult to show that part (2) of the theorem remains true under such a substitution. Precisely speaking, if $(H', \circ)$ is a normal subgroup of $(G', \circ)$, the subgroup $(f^{-1}(H'), *)$ is normal in $(G, *)$. In establishing this fact, we will utilize both implications of Theorem 2–32. Suppose now $h \in f^{-1}(H')$, so that $f(h) \in H'$, and let a be

an arbitrary element of G. Then,

$$f(a * h * a^{-1}) = f(a) \circ f(h) \circ f(a)^{-1} \in H'.$$

In other words, $a * h * a^{-1} \in f^{-1}(H')$, or in terms of sets,

$$a * f^{-1}(H') * a^{-1} \subseteq f^{-1}(H').$$

According to Theorem 2–32, this inclusion is enough to make $(f^{-1}(H'), *)$ a normal subgroup of $(G, *)$.

Without further restriction, it cannot be inferred that the image subgroup $(f(H), \circ)$ will be normal in $(G', \circ)$ whenever $(H, *)$ is itself a normal subgroup of $(G, *)$. One would need to know that

$$a' \circ f(h) \circ (a')^{-1} \in f(H)$$

for all $a' \in G'$ and $h \in H$. In general, there is no way of replacing the element a' by some $f(a)$ in order to exploit the normality of $(H, *)$. A slight strengthening of the hypothesis overcomes this difficulty; simply take f to be an onto mapping. (Recall that the word "onto" requires every member of G' to be the image of at least one element of G.)

Summarizing these remarks, we may now state:

Corollary. 1) For each normal subgroup $(H', \circ)$ of $(G', \circ)$, the subgroup $(f^{-1}(H'), *)$ is normal in $(G, *)$.

2) If $f(G) = G'$, then for each normal subgroup $(H, *)$ of $(G, *)$, the subgroup $(f(H), \circ)$ is normal in $(G', \circ)$.

In much of our subsequent work, the object of interest will be the kernel of a homomorphism.

Definition 2–28. Let f be a homomorphism from the group $(G, *)$ into the group $(G', \circ)$ and let e' be the identity element of $(G', \circ)$. The *kernel* of f, denoted by $\ker(f)$, is the set

$$\ker(f) = \{a \in G \mid f(a) = e'\}.$$

Thus $\ker(f)$ consists of those elements in G which are mapped by f onto the identity element of the group $(G', \circ)$. Theorem 2–38 indicates that $\ker(f)$ is a nonempty subset of G, since $e \in \ker(f)$. It may well happen, as Example 2–41 shows, that $\ker(f) = G$. Except for the trivial function indicated there, the kernel is always a proper subset of G.

Our definition of a homomorphism did not require that it be a one-to-one function, and indeed, we have presented several examples where it failed to be so. There is, however, a simple characterization of a one-to-one homomorphic mapping in terms of the kernel.

Theorem 2-40. Let f be a homomorphism from the group $(G, *)$ into the group $(G', \circ)$. Then f is one-to-one if and only if $\ker(f) = \{e\}$.

Proof. Suppose the function f is one-to-one. We already know that $e \in \ker(f)$. Our aim is to show that this is the only element in the kernel. If there existed another element $a \in \ker(f)$, $a \neq e$, then we would have $f(a) = e' = f(e)$. That is, $f(a) = f(e)$ but $a \neq e$. This would contradict the hypothesis that f is one-to-one.

On the other hand, suppose that $\ker(f) = \{e\}$. Let $a, b \in G$ and $f(a) = f(b)$. To prove f is one-to-one, we must show that $a = b$. But if $f(a) = f(b)$, then

$$\begin{aligned} f(a * b^{-1}) &= f(a) \circ f(b^{-1}) = f(a) \circ f(b)^{-1} \\ &= f(a) \circ f(a)^{-1} = e', \end{aligned}$$

which implies $a * b^{-1} \in \ker(f)$. But, $\ker(f) = \{e\}$. Therefore $a * b^{-1} = e$ or $a = b$.

The next theorem will establish the algebraic character of the pair $(\ker(f), *)$.

Theorem 2-41. If f is a homomorphism from the group $(G, *)$ into the group $(G', \circ)$, then the pair $(\ker(f), *)$ is a normal subgroup of $(G, *)$.

Proof. We have already indicated that the trivial subgroup $(\{e'\}, \circ)$ is a normal subgroup of $(G', \circ)$. Since $\ker(f) = f^{-1}(e')$, the conclusion follows from the general result stated in part (1) of the last corollary.

Example 2-45. As a simple illustration of the above theorems, consider the two groups $(Z, |\ )$ and $(R' - \{0\}, \cdot)$. The mapping $f: Z \to R' - \{0\}$ defined by

$$f(n) = \begin{cases} 1 & \text{if } n \in Z_e, \\ -1 & \text{if } n \in Z_o \end{cases}$$

is a homomorphism, as the reader may verify by checking the various cases that could arise. In the situation considered,

$$\ker(f) = \{n \in Z \mid f(n) = 1\} = Z_e,$$

while the direct image

$$f(Z) = \{1, -1\}.$$

It is not particularly difficult to show that $(Z_e, +)$ is a normal subgroup of $(Z, +)$ and that $(\{1, -1\}, \cdot)$ is a subgroup of $(R' - \{0\}, \cdot)$.

We have just seen that every homomorphism determines a normal subgroup by means of its kernel. On the other hand, the following theorem will show that every normal subgroup gives rise to a homomorphic mapping, the so-called natural mapping. Simply put, the problems of finding homomorphisms and normal subgroups are inseparable.

Theorem 2-42. Let $(H, *)$ be a normal subgroup of the group $(G, *)$. Then the mapping $\text{nat}_H: G \to G/H$ defined by

$$\text{nat}_H(a) = a * H$$

is a homomorphism from $(G, *)$ onto the quotient group $(G/H, \otimes)$; the kernel of nat_H is precisely the set H.

Proof. The fact that the mapping nat_H is homomorphic follows directly from the manner in which multiplication is defined in the quotient group:

$$\begin{aligned}\text{nat}_H(a * b) &= (a * b) * H \\ &= (a * H) \otimes (b * H) = \text{nat}_H(a) \otimes \text{nat}_H(b).\end{aligned}$$

To show that nat_H is an onto function is almost trivial, since every element of G/H is a coset $a * H$ where $a \in G$ and $\text{nat}_H(a) = a * H$.

Inasmuch as the coset H serves as the identity element for $(G/H, \otimes)$, we must have

$$\begin{aligned}\ker(\text{nat}_H) &= \{a \in G \mid \text{nat}_H(a) = H\} \\ &= \{a \in G \mid a * H = H\} = H.\end{aligned}$$

The last equality was achieved by the use of Theorem 2-26.

It is possible, and sometimes convenient, to phrase Theorem 2-42 so that no reference is made to the notion of quotient group:

Theorem 2-43. Let $(H, *)$ be a normal subgroup of the group $(G, *)$. Then there exists a group $(G', \circ)$, and a homomorphism f from $(G, *)$ onto $(G', \circ)$ such that $\ker(f) = H$.

Of course, we take $(G', \circ)$ to be the quotient group $(G/H, \otimes)$ and $f = \text{nat}_H$.

The usual custom is to refer to the function nat_H as the *natural or canonical mapping* of G onto G/H. Provided there is no danger of confusion, we shall frequently omit the subscript H in writing this function.

As a related remark, it might be emphasized that the natural mapping is not generally one-to-one. For if $a, b \in G$ are elements such that the product $a^{-1} * b$ is in H, then by Theorem 2-27, $a * H = b * H$, and consequently $\text{nat}_H(a) = \text{nat}_H(b)$.

Let us pause for a moment to interpret Theorem 2-42 in the case of the additive group of integers $(Z, +)$. We already know that its normal subgroups are the cyclic groups $((n), +)$, where n is a nonnegative integer. Moreover, the quotient group corresponding to any fixed $n \in Z_+$ is simply $(Z_n, +_n)$, the group of integers modulo n; that is, $Z/(n) = Z_n$. It is fairly evident from this that the natural mapping $\text{nat}: Z \to Z_n$ does nothing more than send each integer into its congruence class modulo n: $\text{nat}(a) = [a]$.

Definition 2–29. Two groups $(G, *)$ and $(G', \circ)$ are said to be *isomorphic*, denoted $(G, *) \simeq (G', \circ)$, if there exists a one-to-one homomorphism f of $(G, *)$ onto $(G', \circ)$, that is, $f(G) = G'$. Such a homomorphism f is called an *isomorphism*, or isomorphic mapping, of $(G, *)$ onto $(G', \circ)$.

Any property of $(G, *)$ which can be expressed in terms of the operation $*$ is preserved under f and consequently becomes a property of $(G', \circ)$ as well. The upshot is that the mapping f has the effect of transferring the algebraic structure of the group $(G, *)$ to the group $(G', \circ)$. Isomorphic groups are thus indistinguishable from the abstract point of view, even though they may differ in the notation for and nature of their elements and operations. Two such groups, while not in general formally identical, are the same for all practical purposes.

Actually, the concept of isomorphism is applicable to all types of mathematical systems, for it seems reasonable to treat two systems as essentially equal when they have exactly the same properties. The essence of the notion is that we can always find a one-to-one mapping between the elements of the two systems which preserves whatever structure we are interested in studying.

The observant reader probably noticed that Definition 2–29 is unsymmetric in that it makes mention of a function from one particular group to another. However, if $f: G \to G'$ is a one-to-one, onto, operation-preserving mapping, the function $f^{-1}: G' \to G$ also has these properties. We may therefore ignore this initial lack of symmetry and merely speak of two groups $(G, *)$ and $(G', \circ)$ as being isomorphic to each other; to indicate this, it suffices to write either $(G, *) \simeq (G', \circ)$ or $(G', \circ) \simeq (G, *)$.

Before proceeding further, a knowledge of several specific examples will provide some basis for an understanding of the general idea of isomorphism.

Example 2–46. Consider the two groups $(Z_4, +_4)$ and $(G, \cdot)$, where

$$G = \{1, -1, i, -i\}$$

and $i^2 = -1$. The operation tables for these two systems are

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

We wish to prove that the groups $(Z_4, +_4)$ and $(G, \cdot)$ are abstractly "equal." To do so, we must produce a one-to-one homomorphism f from Z_4 onto G.

Since the preservation of identity elements is a general feature of any homomorphism, f must be such that $f(0) = 1$. Let us suppose for the moment that we were to define $f(1) = -1$. The image of an inverse element must equal

the inverse of the image. We would then have

$$f(3) = f(1^{-1}) = f(1)^{-1} = (-1)^{-1} = -1,$$

or $f(3) = f(1)$. This, however, would prevent f from being one-to-one.

A more appropriate choice, in the sense that it avoids the above difficulty, is to take $f(1) = i$. The condition on inverses then implies $f(3) = -i$. Since f is further required to preserve modular addition,

$$f(2) = f(1 +_4 1) = f(1) \cdot f(1) = i \cdot i = -1.$$

We are thus led in a natural way to consider the function defined by

$$f(0) = 1, \quad f(1) = i, \quad f(2) = 1, \quad f(3) = -i.$$

Clearly this function is a one-to-one mapping of the set Z_4 onto the set G. Furthermore, f actually preserves the operations of the groups. Merely to verify one instance, we observe that

$$f(1 +_4 2) = f(3) = -i = i \cdot -1 = f(1) \cdot f(2).$$

Consequently, we have $(Z_4, +_4) \simeq (G, \cdot)$.

Loosely speaking, two finite groups are isomorphic if it is possible to obtain each multiplication table from the other by merely renaming the elements. The nature of the function f suggests the appropriate rearrangement of the table for $(G, \cdot)$ is

$\cdot$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Apart from the particular symbols used, this group table is identical to that of $(Z_4, +_4)$, for corresponding elements appear at the same place in each table. Both groups are simply disguises for the same abstract system.

In passing, we might note that $(Z_4, +_4)$ is also isomorphic to $(G, \cdot)$ under the function g, whereby $g(0) = 1$, $g(1) = -i$, $g(2) = -1$, $g(3) = i$.

Example 2–47. Let $G = \{e, a, b, c\}$ and the operation $*$ be defined by the table at the right. The reader may verify that the pair $(G, *)$ is a group, known as Klein's four-group. The two groups $(Z_4, +_4)$ and $(G, *)$ are not abstractly equal, however, for every one-to-one function f from the set Z_4 onto G fails to be operation-preserving.

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

From this we conclude that there are at least two distinct algebraic structures for groups with four elements.

To illustrate this point, we shall check several possibilities for the function f. Consider the mapping defined on the set Z_4 by

$$f(0) = e, \quad f(1) = a, \quad f(2) = b, \quad f(3) = c.$$

Then

$$f(1 +_4 3) = f(0) = e \neq b = a * c = f(1) * f(3),$$

which shows that the proposed f is not a homomorphism. Another possibility for f might be

$$f(0) = e, \quad f(1) = b, \quad f(2) = c, \quad f(3) = a.$$

Note that we must always map identity elements to identify elements. This choice of f also fails to preserve the operations, since

$$f(1 +_4 1) = f(2) = c \neq e = b * b = f(1) * f(1).$$

We shall leave the test of the remaining possibilities as an exercise.

A standard procedure for showing that two groups are not isomorphic is to find some property of one, not possessed by the other, which by its nature would necessarily be shared if these groups were actually isomorphic. In the present case, the group $(Z_4, +_4)$ and the four-group are differentiated by the fact the former is a cyclic group whereas the latter is not.

Example 2–48. The two groups $(Z, +)$ and $(Q - \{0\}, \cdot)$ are not isomorphic. To see this, suppose that there exists a one-to-one onto function f: $Z \to Q - \{0\}$ with the property

$$f(a + b) = f(a) \cdot f(b)$$

for all $a, b \in Z$. If x denotes the element of Z such that $f(x) = -1$, then

$$f(2x) = f(x + x) = f(x) \cdot f(x) = (-1) \cdot (-1) = 1.$$

According to Theorem 2–40, the identity element of $(Z, +)$ is the unique element of Z corresponding to the identity of $(Q - \{0\}, \cdot)$, so that $2x = 0$ or $x = 0$. Consequently, both $f(0) = 1$, and $f(0) = -1$, contradicting the fact that the function f is one-to-one. This argument shows that $(Z, +)$ cannot be isomorphic to $(Q - \{0\}, \cdot)$, for no function satisfying Definition 2–29 can exist.

Example 2–49. For an instructive example in connection with the additive group of integers consider the following assertion: the only functions under which $(Z, +)$ is isomorphic to itself are the identity mapping and its negative. A fairly succinct description of all this is that $A(Z) = \{i_Z, -i_Z\}$.

Perhaps the quickest proof of the above assertion consists of showing that if $f \in A(Z)$, then the cyclic subgroup $((f(1)), +)$ generated by $f(1)$ is the group $(Z, +)$ itself. Since the inclusion $(f(1)) \subseteq Z$ trivially holds, our aim would be achieved by establishing $Z \subseteq (f(1))$. But this is a straightforward matter. If n is an arbitrary integer, $n = f(m)$ for some $m \in Z$—recall f is a mapping onto Z—so that

$$\begin{aligned} n &= f(1 + 1 + \cdots + 1) \qquad (m \text{ summands}) \\ &= f(1) + f(1) + \cdots + f(1) \\ &= mf(1), \end{aligned}$$

whence $n \in (f(1))$.

Since 1 and -1 are the only generators of $(Z, +)$, either $f(1) = 1$ or $f(1) = -1$. However, the preceding computation indicates $f(n) = nf(1)$ for each $n \in Z$; from this, it is clear that $f = i_Z$ or $f = -i_Z$ according as $f(1) = 1$ or $f(1) = -1$.

Let us return to general considerations by showing that the groups $(Z_n, +_n)$ and $(Z, +)$ are the prototypes of all finite and infinite cyclic groups, respectively.

Theorem 2–44. Every finite cyclic group of order n is isomorphic to $(Z_n, +_n)$ and every infinite cyclic group is isomorphic to $(Z, +)$.

Proof. First, suppose the cyclic group $((a), *)$ is of finite order n. In this case, we know from Theorem 2–23 that

$$(a) = \{e, a, a^2, \ldots, a^{n-1}\}.$$

It seems natural then to investigate the mapping $f: (a) \to Z_n$ given by the rule $f(a^k) = [k]$, $0 \leq k < n$. This function plainly carries (a) onto the set Z_n. Next observe that f is one-to-one: if $f(a^k) = f(a^j)$, then $k \equiv j \pmod{n}$ so that $a^k = a^j$. Finally, for any elements a^k, a^j in (a), we have

$$f(a^k * a^j) = f(a^{k+j}) = [k + j] = [k] +_n [j] = f(a^k) +_n f(a^j).$$

This shows the function f preserves the respective group operations and completes the proof of the isomorphism $((a), *) \simeq (Z_n, +_n)$.

For the second part of the theorem, the cyclic group $((a), *)$ is assumed to be of infinite order. Here, the choice of a mapping f between (a) and Z is obvious: simply take $f(a^k) = k$. It is immediate that f, so defined, is an onto mapping. Further, this function is one-to-one, for all the powers of the generator must be distinct; if two different powers of a were equal, the argument of Theorem 2–23 could be employed to obtain the contradiction that (a) is a finite set. The rest is routine:

$$f(a^k * a^j) = f(a^{k+j}) = k + j = f(a^k) + f(a^j).$$

Hence, as we wished to establish, $((a), *)$ is isomorphic to the group $(Z, +)$.