Corollary. Any two cyclic groups of the same order are isomorphic.

Trivially, any group $(G, *)$ is isomorphic to itself under the identity mapping i_G. A reasonable query is whether $(G, *)$ is isomorphic to any group other than itself. The concluding theorem in this section, a classical result due to Cayley, answers the question in the affirmative.

We begin, however, by recalling some definitions and notation. For an arbitrary element a in G, the left-multiplication function $f_a: G \to G$ was defined by taking $f_a(x) = a * x$ for every $x \in G$. The collection of all functions obtained in this way is labeled by $F_G: F_G = \{f_a \mid a \in G\}$. Example 2–25 established the structural nature of the pair $(F_G, \circ)$—in the present context $\circ$ indicates the operation of functional composition—when this system was shown to be a group. Our task now is to prove the isomorphism of $(G, *)$ and $(F_G, \circ)$.

Theorem 2–45. (*Cayley*). If $(G, *)$ is an arbitrary group, then

$$(G, *) \simeq (F_G, \circ).$$

Proof. Define the mapping $f: G \to F_G$ by the rule $f(a) = f_a$ for each $a \in G$. That the function f is onto F_G is obvious. If $f(a) = f(b)$, so $f_a = f_b$, then $a * x = b * x$ for all elements x of G. In particular,

$$a = a * e = b * e = b,$$

which shows that f is one-to-one. We complete the proof by establishing that f is a homomorphism:

$$f(a * b) = f_{a*b} = f_a \circ f_b = f(a) \circ f(b).$$

As an illustration of this theorem, consider the group $(R^\#, +)$. Corresponding to an element $a \in R^\#$ is the left-multiplication function f_a, defined by

$$f_a(x) = a + x, \qquad x \in R^\#.$$

That is, the function f_a merely has the effect of translating or shifting elements by an amount a. Cayley's Theorem asserts that the group $(R^\#, +)$ and the group $(F_G, \circ)$ of translations of the real line are indistinguishable as far as their algebraic properties are concerned.

PROBLEMS

1. In the following situations, determine whether the indicated function f is a homomorphism from the first group into the second group.

   a) $f(a) = -a$, $(R^\#, +)$, $(R^\#, +)$
   b) $f(a) = |a|$, $(R^\# - \{0\}, \cdot)$, $(R^\#_+, \cdot)$
   c) $f(a) = a + 1$, $(Z, +)$, $(Z, +)$

d) $f(a) = a^2$, $(R^\# - \{0\}, \cdot)$, $(R^\#_+, \cdot)$
e) $f(a) = a/q$ (q a fixed nonzero integer), $(Z, +)$, $(Q, +)$
f) $f(a) = na$ (n a fixed integer), $(Z, +)$, $(Z, +)$

2. Suppose f is a homomorphism from the group $(G, *)$ into the group $(G', \circ)$:

   a) If e designates the identity element of $(G, *)$, show that the kernel of f may be described by $\ker(f) = f^{-1}(f(e))$.
   b) Provided the group $(G', \circ)$ is commutative, establish the inclusion $[G, G] \subseteq \ker(f)$.

3. Let $(Z_8, +_8)$ be the group of integers modulo 8 and $((a), *)$ be any finite cyclic group of order 12. Assume further that the mapping $f: Z_8 \to (a)$ is defined as follows:

$$f(0) = f(4) = e, \qquad f(1) = f(5) = a^3,$$
$$f(2) = f(6) = a^6, \qquad f(3) = f(7) = a^9.$$

   a) Prove that the function f, so defined, is a homomorphism.
   b) Describe the subgroups $(\ker(f), +_8)$ and $(f(Z_8), *)$.
   c) If $H = \{e, a^6\}$, show the pair $(f^{-1}(H), +_8)$ is a subgroup of $(Z_8, +_8)$.

4. Consider the two groups $(Z, +)$ and $(\{1, -1, i, -i\}, \cdot)$, where $i^2 = -1$. Show that the mapping defined by $f(n) = i^n$ for $n \in Z$ is a homomorphism from $(Z, +)$ onto $(\{1, -1, i, -i\}, \cdot)$, and determine its kernel.

5. Let f be a homomorphism from the group $(G, *)$ into itself and let H denote the set of elements of G which are left fixed by f:

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

   Prove that $(H, *)$ is a subgroup of $(G, *)$.

6. Let $(G, *)$ be a group and the element $a \in G$ be fixed. Prove that $(G, *)$ is isomorphic to itself—that is, $(G, *) \simeq (G, *)$— under the mapping f defined by

$$f(x) = a * x * a^{-1}, \qquad x \in G.$$

   What is the kernel of this function?

7. Prove that if the group $(G, *)$ is commutative (cyclic) and $(G, *) \simeq (G', \circ)$ then the group $(G', \circ)$ is also commutative (cyclic).

8. Let the set $G = Z \times Z$ and the binary operation $*$ on G be given by the rule $(a, b) * (c, d) = (a + c, b + d)$. It is easily verified that the pair $(G, *)$ is a commutative group.

   a) Show that the mapping $f: G \to Z$ defined by $f[(a, b)] = a$ is a homomorphism from $(G, *)$ onto the group $(Z, +)$.
   b) Determine the kernel of this mapping.
   c) If $H = \{(a, a) \mid a \in Z\}$, prove that $(H, *)$ is a subgroup of $(G, *)$, which is isomorphic to $(Z, +)$ under the function f.

9. Show that the two groups $(R^\#, +)$ and $(R^\# - \{0\}, \cdot)$ are not isomorphic.

10. Prove that all finite groups of order two are isomorphic.

11. If

$$G = \left\{1, \frac{-1 + i\sqrt{3}}{2}, \frac{-1 - i\sqrt{3}}{2}\right\},$$

where $i^2 = -1$, then the pair $(G, \cdot)$ forms a group. Determine whether $(G, \cdot) \simeq (Z_3, +_3)$.

12. Let f and g be two homomorphisms from the group $(G, *)$ into the group $(G', \circ)$. Define the function $h: G \to G'$ by

$$h(a) = f(a) \circ g(a).$$

Show that if the group $(G', \circ)$ is commutative, then h is also a homomorphism.

13. Consider the following two groups: $(G_1, *)$, where

$$G_1 = \{R_{180}, R_{360}, H, V\},$$

and the operation $*$ consists of following one symmetry of the square by another; $(G_2, \circ)$, where G_2 consists of the four functions on $R^{\sharp} - \{0\}$,

$$f_1(x) = x, \qquad f_2(x) = -x, \qquad f_3(x) = 1/x, \qquad f_4(x) = -1/x,$$

and $\circ$ denotes functional composition. Verify that $(G_1, *) \simeq (G_2, \circ)$.

14. Given f is a homomorphism from a simple group $(G, *)$ onto a group $(G', \circ)$, show that either $(G, *) \simeq (G', \circ)$ or else that f must be the trivial homomorphism.

15. Let $(G, *)$ be an arbitrary group and j be the mapping of the set G onto itself defined by $j(a) = a^{-1}$, for all $a \in G$.

a) Prove that the function j is a homomorphism if and only if $(G, *)$ is commutative.

b) Generalize the result of Example 2-49 to the following: if $(G, *)$ is an infinite cyclic group, then $A(G) = \{i_G, j\}$.

16. Prove that any group $(G, *)$ is isomorphic to some subgroup of its symmetric group $(\text{sym } G, \circ)$. [*Hint:* Use Theorem 2-45.]

17. Obtain the group of left-multiplication functions corresponding to the group $(Z_5, +_5)$; set up the homomorphism which results in the isomorphism of these groups.

2-7 THE FUNDAMENTAL THEOREMS

In this section, we shall discuss a number of significant results having to do with the relationship between homomorphisms and quotient groups. Of these, Theorem 2-47, generally known as the Fundamental Homomorphism Theorem for Groups, is perhaps the most crucial. The importance of this result would be difficult to overemphasize; in a sense, all which follows thereafter may be viewed as an enumeration of its special cases and implications.

Throughout this section, f denotes a homomorphism from the group $(G, *)$ onto the group $(G', \circ)$, that is, $f(G) = G'$. In order to simplify the statements of various theorems, we shall frequently not trouble to specify this familiar opening phrase. Accordingly, unless there is clear indication to the contrary, any reference to the function f is understood implicitly to involve the aforementioned hypothesis.

We begin with a proof of the Factor Theorem, stated here in a form best suited to our immediate needs.

Theorem 2–46. (*Factor Theorem*). Let $(H, *)$ be a normal subgroup of the group $(G, *)$ such that $H \subseteq \ker(f)$. Then there exists a unique homomorphism $\bar{f}\colon G/H \to G'$ with the property

$$f = \bar{f} \circ \mathrm{nat}_H.$$

Proof. Before becoming explicit in the details of the proof, let us remind the reader that the symbol nat_H designates the natural mapping of G onto G/H; that is, $\mathrm{nat}_H\colon G \to G/H$ with $\mathrm{nat}_H(a) = a * H$.

To start with, we define a function $\bar{f}\colon G/H \to G'$, called the *induced mapping*, by taking

$$\bar{f}(a * H) = f(a), \qquad a \in G.$$

The first question to be raised concerns whether or not $\bar{f}$ is actually well-defined. In other words, it must be established that this function depends only on the cosets of H and in no way on the particular representative used. To see that this is so, suppose $a * H = b * H$. As the elements a and b belong to the same coset, the product $a^{-1} * b \in H \subseteq \ker(f)$. This means that

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

and, by the manner in which $\bar{f}$ is defined, that

$$\bar{f}(a * H) = \bar{f}(b * H).$$

Hence, the function $\bar{f}$ is constant on the cosets of H, as we wished to demonstrate.

A routine computation, involving the definition of multiplication in $(G/H, \otimes)$, shows $\bar{f}$ to be a homomorphism:

$$\begin{aligned} f((a * H) \otimes (b * H)) &= f((a * b) * H) \\ &= f(a * b) \\ &= f(a) \circ f(b) = \bar{f}(a * H) \circ \bar{f}(b * H). \end{aligned}$$

Next, we observe that for each element $a \in G$,

$$f(a) = \bar{f}(a * H) = \bar{f}(\mathrm{nat}_H(a)) = (\bar{f} \circ \mathrm{nat}_H)(a),$$

whence the equality $f = \bar{f} \circ \mathrm{nat}_H$. The proof is completed upon showing that this factorization is unique. Thus, suppose also that $f = g \circ \mathrm{nat}_H$ for some other function $g\colon G/H \to G'$. But then,

$$\bar{f}(a * H) = f(a) = (g \circ \mathrm{nat}_H)(a) = g(a * H)$$

for all a in G, so $\bar{f} = g$. The induced mapping $\bar{f}$ is therefore seen to be the only function from G/H to G' satisfying the equation $f = \bar{f} \circ \mathrm{nat}_H$.

Corollary. The function $\bar{f}$ is one-to-one if and only if $\ker(f) \subseteq H$.

Proof. What is required here is an explicit description of the kernel of $\bar{f}$:

$$\begin{aligned}\ker(\bar{f}) &= \{a * H \mid \bar{f}(a * H) = e'\}\\ &= \{a * H \mid f(a) = e'\},\end{aligned}$$

where, of course, e' denotes the identity of the group $(G', \circ)$. Another way of saying the same thing is

$$\ker(\bar{f}) = \{a * H \mid a \in \ker(f)\} = \mathrm{nat}_H(\ker(\mathrm{f})).$$

Now, from Theorem 2–40, a necessary and sufficient condition for $\bar{f}$ to be a one-to-one mapping is that $\ker(\bar{f}) = e * H = H$. In the present situation, this condition reduces to requiring that

$$\mathrm{nat}_H(\ker(f)) = H,$$

which is equivalent to the inclusion $\ker(f) \subseteq H$.

In view of the equality $f = \bar{f} \circ \mathrm{nat}_H$, the conclusion of Theorem 2–46 is often described by saying that the function f can be factored through the quotient group $(G/H, \otimes)$ or, alternatively, that f can be factored by nat_H. The following diagram may help to clarify the relations among the various functions:

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "\mathrm{nat}_H"'] & & G' = f(G) \\ & G/H \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

What we have just proved, in effect, is that there exists one and only one function $\bar{f}$ which makes this triangle of maps commutative.

Example 2–50. Let us cite a specific instance of the Factor Theorem. Our contention is that whenever the group $(G', \circ)$ is commutative, the function f can always be factored through the commutator quotient group $(G/[G, G], \otimes)$; otherwise stated,

$$f = \bar{f} \circ \mathrm{nat}_{[G,G]}.$$

For this, consider any commutator $[a, b] = a * b * a^{-1} * b^{-1}$, with $a, b \in G$. As a consequence of the commutativity of $(G', \circ)$,

$$f([a, b]) = [f(a), f(b)] = e',$$

so that $[a, b] \in \ker(f)$. Now, the commutator subgroup $([G, G], *)$ is, so to speak, the smallest subgroup of $(G, *)$ to contain all the commutators. Thus we must conclude that $[G, G] \subseteq \ker(f)$. Having this inclusion, it is only necessary to apply Theorem 2-46 to obtain the desired factorization.

Although we did not expressly require the information in the proof of Theorem 2-46, it might be pointed out that the induced mapping $\bar{f}$ carries G/H onto the set G'. This is readily obtainable from the definition of $\bar{f}$ and the fact f itself is an onto function. To be more specific, if $a' \in G'$, then $a' = f(a)$ for some element a in G; hence,

$$a' = f(a) = \bar{f}(a * H).$$

A rather simple observation, with far-reaching implications, is that whenever $H = \ker(f)$, so that both the Factor Theorem and its corollary are applicable, f induces a mapping $\bar{f}$ under which $(G/H, \otimes)$ and $(G', \circ)$ are isomorphic groups.

The discussion of the foregoing paragraph may be conveniently summarized in the following theorem, a result which will be invoked repeatedly.

Theorem 2-47. (*Fundamental Theorem*). If f is a homomorphism from the group $(G, *)$ onto the group $(G', \circ)$, then

$$(G/\ker(f), \otimes) \simeq (G', \circ).$$

Remark. If in the statement of the theorem, the word "onto" is replaced by "into," the conclusion takes the form $(G/\ker(f), \otimes) \simeq (f(G), \circ)$.

Theorem 2-47 is admittedly rather technical in nature and therefore perhaps a brief explanation of its significance is in order. Suppose that $(G, *)$ is an unfamiliar group whose algebraic properties we wish to determine. Clearly, if $(G, *)$ could be shown to be isomorphic to some well-known group $(G', \circ)$, then our problem is solved; for $(G, *)$, being a replica of $(G', \circ)$, would possess the same algebraic structure.

Another approach, which usually gives a less complete picture of $(G, *)$ is to examine its images under homomorphisms. The difficulty here, of course, is that when these functions fail to be one-to-one, not all the algebraic properties of the images are reflected in the original group. For instance, it is quite possible for the commutative law to hold in an image group without $(G, *)$ itself being commutative. Theorem 2-47 asserts that the images of $(G, *)$ under homomorphisms can be duplicated up to isomorphism by quotient groups of $(G, *)$. In a sense, it is not necessary to go beyond $(G, *)$ to obtain all its images under homomorphic mappings.