with any one system will also be true for the other system after the labels are changed. We shall now formalize these ideas for any two algebraic systems.

Definition 3-1.1 Let $\langle X, \circ\rangle$ and $\langle Y, *\rangle$ be two algebraic systems of the same type in the sense that both $\circ$ and $*$ are binary (n-ary) operations. A mapping $g\colon X \to Y$ is called a *homomorphism*, or simply morphism, from $\langle X, \circ\rangle$ to $\langle Y, *\rangle$ if for any $x_1, x_2 \in X$

$$g(x_1 \circ x_2) = g(x_1) * g(x_2) \tag{2}$$

If such a function g exists, then it is customary to call $\langle Y, *\rangle$ a homomorphic image of $\langle X, \circ\rangle$, although we must note that $g(X) \subseteq Y$.

The concept of homomorphism is not restricted to algebraic systems with one binary operation. One can extend this definition to any two algebraic systems of the same type. Since in a homomorphism the operations are preserved, we shall see that several properties of the operations are also preserved.

For the algebraic systems $\langle F, \circ\rangle$ and $\langle \mathbf{Z}_4, +_4\rangle$, the mapping $\psi\colon F \to \mathbf{Z}_4$ given by Eq. (1) is a homomorphism. Any mapping which satisfies the condition given by Eq. (2) is a homomorphism. In the example of the algebraic systems $\langle F, \circ\rangle$ and $\langle \mathbf{Z}_4, +_4\rangle$, the mapping is bijective, which is a special case of homomorphism as can be seen from Definition 3-1.2 which follows. It is possible to have more than one homomorphic mapping from one algebraic system to another.

P

Definition 3-1.2 Let g be a homomorphism from $\langle X, \circ\rangle$ to $\langle Y, *\rangle$. If $g\colon X \to Y$ is onto, then g is called an *epimorphism*. If $g\colon X \to Y$ is one-to-one, then g is called a *monomorphism*. If $g\colon X \to Y$ is one-to-one onto, then g is called an *isomorphism*.

Definition 3-1.3 Let $\langle X, \circ\rangle$ and $\langle Y, *\rangle$ be two algebraic systems of the same type. If there exists an isomorphic mapping $g\colon X \to Y$, then $\langle X, \circ\rangle$ and $\langle Y, *\rangle$ are said to be *isomorphic*.

In the case when $\langle X, \circ\rangle$ and $\langle Y, *\rangle$ are isomorphic, then the two algebraic systems are structurally indistinguishable in the sense that they differ only in the labels used to denote the elements of the sets and the operations involved. It is easy to see that the inverse of an isomorphism is also an isomorphism. Also all the properties of the operations are preserved in an isomorphism.

P

Definition 3-1.4 Let $\langle X, \circ\rangle$ and $\langle Y, *\rangle$ be two algebraic systems such that $Y \subseteq X$. A homomorphism g from $\langle X, \circ\rangle$ to $\langle Y, *\rangle$ in such a case is called an *endomorphism*. If $Y = X$, then an isomorphism from $\langle X, \circ\rangle$ to $\langle Y, *\rangle$ is called an *automorphism*.

EXAMPLE 5 Show that the algebraic systems of $\langle F, \circ\rangle$ and $\langle \mathbf{Z}_4, +_4\rangle$ given in Examples 3 and 4 are isomorphic.

SOLUTION The mapping $\psi\colon F \to \mathbf{Z}_4$ defined by Eq. (1) is one-to-one onto and is a homomorphism; hence ψ is an isomorphism. ////

EXAMPLE 6 Let $\langle \mathbf{Z}_4, +_4 \rangle$ and $\langle B, + \rangle$ be the algebraic systems given in Example 4 of Sec. 3-1.2 and Example 6 of Sec. 3-1.1 respectively. Show that $\langle B, + \rangle$ is a homomorphic image of $\langle \mathbf{Z}_4, +_4 \rangle$.

SOLUTION Let a mapping $g\colon \mathbf{Z}_4 \to B$ be given by

$$g([0]) = g([2]) = 0 \qquad \text{and} \qquad g([1]) = g([3]) = 1$$

It is easy to verify that g is an epimorphism from $\langle \mathbf{Z}_4, +_4 \rangle$ to $\langle B, + \rangle$ because for any $i, j = 0, 1, 2, 3$

$$g([i] +_4 [j]) = g([i]) + g([j])$$

////

EXAMPLE 7 Let $S = \{a, b, c\}$ and let $*$ denote a binary operation on S given by Table 3-1.4. Also let $P = \{1, 2, 3\}$ and $\oplus$ be a binary operation on P given by Table 3-1.4. Show that $\langle S, * \rangle$ and $\langle P, \oplus \rangle$ are isomorphic.

SOLUTION Consider a mapping $g\colon S \to P$ given by

$$g(a) = 3 \qquad g(b) = 1 \qquad \text{and} \qquad g(c) = 2$$

Obviously, g is one-to-one onto. Also a check of entries in Table 3-1.4 shows that g is a homomorphism.

////

EXAMPLE 8 Given the algebraic system $\langle \mathbf{N}, + \rangle$ and $\langle \mathbf{Z}_4, +_4 \rangle$, where $\mathbf{N}$ is the set of natural numbers and $+$ is the operation of addition on $\mathbf{N}$, show that there exists a homomorphism from $\langle \mathbf{N}, + \rangle$ to $\langle \mathbf{Z}_4, +_4 \rangle$.

SOLUTION Define $g\colon \mathbf{N} \to \mathbf{Z}_4$ given by

$$g(a) = [a(\text{mod } 4)] \qquad \text{for any } a \in \mathbf{N}$$

For $a, b \in \mathbf{N}$, let $g(a) = [i]$ and $g(b) = [j]$; then

$$g(a + b) = [(i + j)(\text{mod } 4)] = [i] +_4 [j] = g(a) +_4 g(b)$$

Observe that $g(0) = [0]$; that is, the mapping g also preserves the identity element.

////

Let $\langle X, \circ \rangle$ be an algebraic system in which $\circ$ is a binary operation on X. Let us assume that E is an equivalence relation on X. The equivalence relation E is said to have the *substitution property* with respect to the operation $\circ$ iff for any $x_1, x_2 \in X$.

$$(x_1 \mathrel{E} x_1') \wedge (x_2 \mathrel{E} x_2') \Rightarrow (x_1 \circ x_2) \mathrel{E} (x_1' \circ x_2') \tag{3}$$

where $x_1', x_2' \in X$. Implication (3) states that in $x_1 \circ x_2$ if we substitute for x_1

Table 3-1.4

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

$\oplus$	1	2	3
1	1	2	1
2	1	2	2
3	1	2	3

any other element of X which is equivalent to it and similarly for x_2 any other element of X which is equivalent to x_2, then the resulting element is equivalent to $x_1 \circ x_2$; that is, the equivalence relationship is unaltered by such substitutions. The substitution property can be defined for any n-ary operation and also for any number of operations.

Definition 3-1.5 Let $\langle X, \circ \rangle$ be an algebraic system and E be an equivalence relation on X. The relation E is called a *congruence relation* on $\langle X, \circ \rangle$ if E satisfies the substitution property with respect to the operation $\circ$.

This definition of congruence relation can be generalized to any algebraic system, whenever the substitution property is satisfied with respect to all the operations of that system.

With the help of congruence relations it is possible to construct new and simpler algebraic systems from a given algebraic system. Also the concept of congruence relation is closely connected to that of homomorphism, as will be shown now.

Let $\langle X, \circ \rangle$ be an algebraic system in which $\circ$ is a binary operation on X. Let E be a congruence relation on $\langle X, \circ \rangle$. Since E is an equivalence relation on X, it partitions X into equivalence classes. The set of equivalence classes is the quotient set X/E. Let $x_1, x_2, y_1, y_2 \in X$ with $x_1 \, E \, y_1$ and $x_2 \, E \, y_2$. Since E is a congruence relation, $(x_1 \circ x_2) \, E \, (y_1 \circ y_2)$, so that $[x_1 \circ x_2] = [y_1 \circ y_2]$ where $[x_j]$ is used to denote the equivalence class in which x_j is a member. Corresponding to the operation $\circ$ on X, we now define a binary operation $*$ on X/E such that for any $x_1, x_2 \in X$

$$[x_1] * [x_2] = [x_1 \circ x_2] \tag{4}$$

It is easy to see that the operation $*$ is well defined on X/E because $[x_1 \circ x_2]$ is independent of the elements chosen to represent the equivalence classes $[x_1]$ and $[x_2]$. We therefore have an algebraic system $\langle X/E, * \rangle$ called the *quotient algebra* which is of the same type as the algebra $\langle X, \circ \rangle$. In fact, several properties of the operation $\circ$ are preserved by the operation $*$.

In order to show a connection between a homomorphism and congruence relation, we first show that corresponding to a congruence relation E on $\langle X, \circ \rangle$ we can define a homomorphism g_E from $\langle X, \circ \rangle$ onto the quotient algebra $\langle X/E, * \rangle$ that is given by $g_E(x) = [x]$ for any $x \in X$. Obviously,

$$g_E(x_1 \circ x_2) = [x_1 \circ x_2] = [x_1] * [x_2] = g_E(x_1) * g_E(x_2) \tag{5}$$

The homomorphism g_E is called the *natural homomorphism* associated with the congruence relation E.

As a next step, let us consider a homomorphism f from $\langle X, \circ \rangle$ onto $\langle Y, \oplus \rangle$. Now we show that corresponding to f we can define a congruence relation E_f on $\langle X, \circ \rangle$ by

$$x_1 \, E_f \, x_2 \Leftrightarrow f(x_1) = f(x_2) \qquad \text{for any } x_1, x_2 \in X \tag{6}$$

This definition guarantees that E_f is an equivalence relation for any mapping

$f: X \to Y$. On the other hand, the fact that f is a homomorphism guarantees that E_f is a congruence relation on $\langle X, \circ \rangle$.

So far we have established that for every congruence relation E on $\langle X, \circ \rangle$, we can define a natural homomorphism g_E. Also, for any homomorphism f from $\langle X, \circ \rangle$ to $\langle Y, \oplus \rangle$, we can define a congruence relation E_f so that there is a one-to-one correspondence between the homomorphisms and congruence relations on $\langle X, \circ \rangle$. As a final step, we now show that if f is a homomorphism from $\langle X, \circ \rangle$ onto $\langle Y, \oplus \rangle$, if E is a congruence relation corresponding to f (called E_f earlier), and if g_E is the natural homomorphism from $\langle X, \circ \rangle$ to $\langle X/E, * \rangle$, then there exists an isomorphism h between $\langle X/E, * \rangle$ and $\langle Y, \oplus \rangle$. With the definitions of $E_f = E$ and g_E as given in Eqs. (5) and (6), let us now define a mapping $h: X/E \to Y$ such that

$$h[x_1] = f(x_1) \qquad \text{for any } x_1 \in X \tag{7}$$

Observe that for $x_1, x_2 \in X$, $x_1 \circ x_2 \in X$ and

$$g_E(x_1 \circ x_2) = [x_1 \circ x_2] \qquad \text{from (5)}$$

This means

$$h(g_E(x_1 \circ x_2)) = h([x_1 \circ x_2]) = f(x_1 \circ x_2) \qquad \text{from (7)}$$

The mapping h is one-to-one onto, and

$$h([x_1] * [x_2]) = h(g_E(x_1 \circ x_2)) = f(x_1 \circ x_2) = f(x_1) \oplus f(x_2)$$

Hence h is an isomorphism. These mappings can be shown diagrammatically as given in Fig. 3-1.3. In particular, if $Y = X$, then

$$g_{E_f} = f$$

EXAMPLE 9 Let $\langle \mathbf{N}, + \rangle$ be the algebraic system of natural numbers as given in Example 8. Define an equivalence relation E on $\mathbf{N}$ such that $x_1 \, E \, x_2$ iff either $x_1 - x_2$ or $x_2 - x_1$ is divisible by 4. Show that E is a congruence relation and that the homomorphism g defined in Example 8 is the natural homomorphism associated with E.

SOLUTION Obviously E is an equivalence relation. Also E is a congruence relation because for $x_1 \, E \, x_1'$ and $x_2 \, E \, x_2'$, $(x_1 + x_2) \, E \, (x_1' + x_2')$ because $(x_1 + x_2) - (x_1' + x_2') = (x_1 - x_1') + (x_2 - x_2')$, and both $x_1 - x_1'$ as well as $x_2 - x_2'$ are divisible by 4. Observe also that the mapping $g(i) = [i]$ is the same as required in the definition of natural homomorphism in Eq. (5), so that $g = g_E$. ////

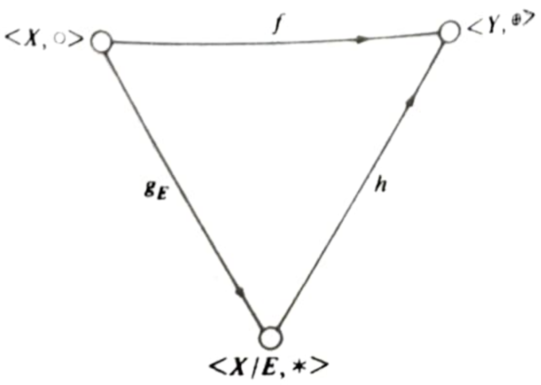

FIGURE 3-1.3

Definition 3-1.6 Let $\langle X, \circ \rangle$ be an algebraic system and $Y \subseteq X$ which is closed under the operation $\circ$. Then $\langle Y, \circ \rangle$ is called a *subalgebra* of $\langle X, \circ \rangle$.

The concept of a subalgebra can be applied to any algebraic system provided the subalgebra is closed under all the operations (including 0-ary operations) of the original system. Naturally a subalgebra is of the same type as the original system, and the operations of the systems being the same, most of their properties are also preserved.

Another useful concept associated with any algebraic system is that of direct product of algebras of the same type.

Definition 3-1.7 Let $\langle X, \circ \rangle$ and $\langle Y, \ast \rangle$ be two algebraic systems of the same type. The algebraic system $\langle X \times Y, \oplus \rangle$ is called the *direct product* of the algebras $\langle X, \circ \rangle$ and $\langle Y, \ast \rangle$ provided the operation $\oplus$ is defined for any $x_1, x_2 \in X$ and $y_1, y_2 \in Y$ as

$$\langle x_1, y_1 \rangle \oplus \langle x_2, y_2 \rangle = \langle x_1 \circ x_2, y_1 \ast y_2 \rangle$$

The algebraic systems $\langle X, \circ \rangle$ and $\langle Y, \ast \rangle$ are called the *factor algebras* of $\langle X \times Y, \oplus \rangle$.

The definition of direct product can be generalized on the one hand to any two algebraic systems of the same type. The operations in the direct product are defined in terms of the corresponding operations of the factor algebras. On the other hand, one can also define by repeated application of the above procedure the direct product of any finite number of algebraic systems of the same type.

The concepts of subalgebras as well as that of direct product of algebras will be used for almost every abstract algebraic system that we shall study in the next section.

EXERCISES 3-1

1 Which of the following systems satisfy the properties of $\langle \mathbf{I}, +, \times \rangle$ which are designated by (**A-1**) to (**A-4**), (**M-1**) to (**M-3**), (**D**), and (**C**)?

(*a*) All odd integers

(*b*) All even integers

(*c*) All positive integers

(*d*) All nonnegative integers

(*e*) $\langle \mathbf{Z}_6, +_6, \times_6 \rangle$

(*f*) $\langle \mathbf{Z}_7, +_7, \times_7 \rangle$

2 In Example 4, Sec. 3-1.1, let $S = \{a\}$. Given the composition tables for the operations $+$ and $\times$, show that the algebraic system $\langle \rho(S), +, \times \rangle$ in this case is isomorphic to the system given in Example 6, Sec. 3-1.2.

3 Show that if $g: A \rightarrow B$ is a homomorphism of an algebraic system $\langle A, \ast \rangle$ onto $\langle B, \Delta \rangle$ and $\langle A_1, \ast \rangle$ is a subalgebra of $\langle A, \ast \rangle$, then the image of A_1 under g is a subalgebra of $\langle B, \Delta \rangle$.

4 Show that the intersection of any two congruence relations on a set is also a congruence relation.

5 Show that the composition of two congruence relations on a set is not necessarily a congruence relation.