Module 5 - Algebraic Structures

CE– SE–DSGT

Dr. Anil Kale

Associate Professor

Dept. of Computer Engineering,

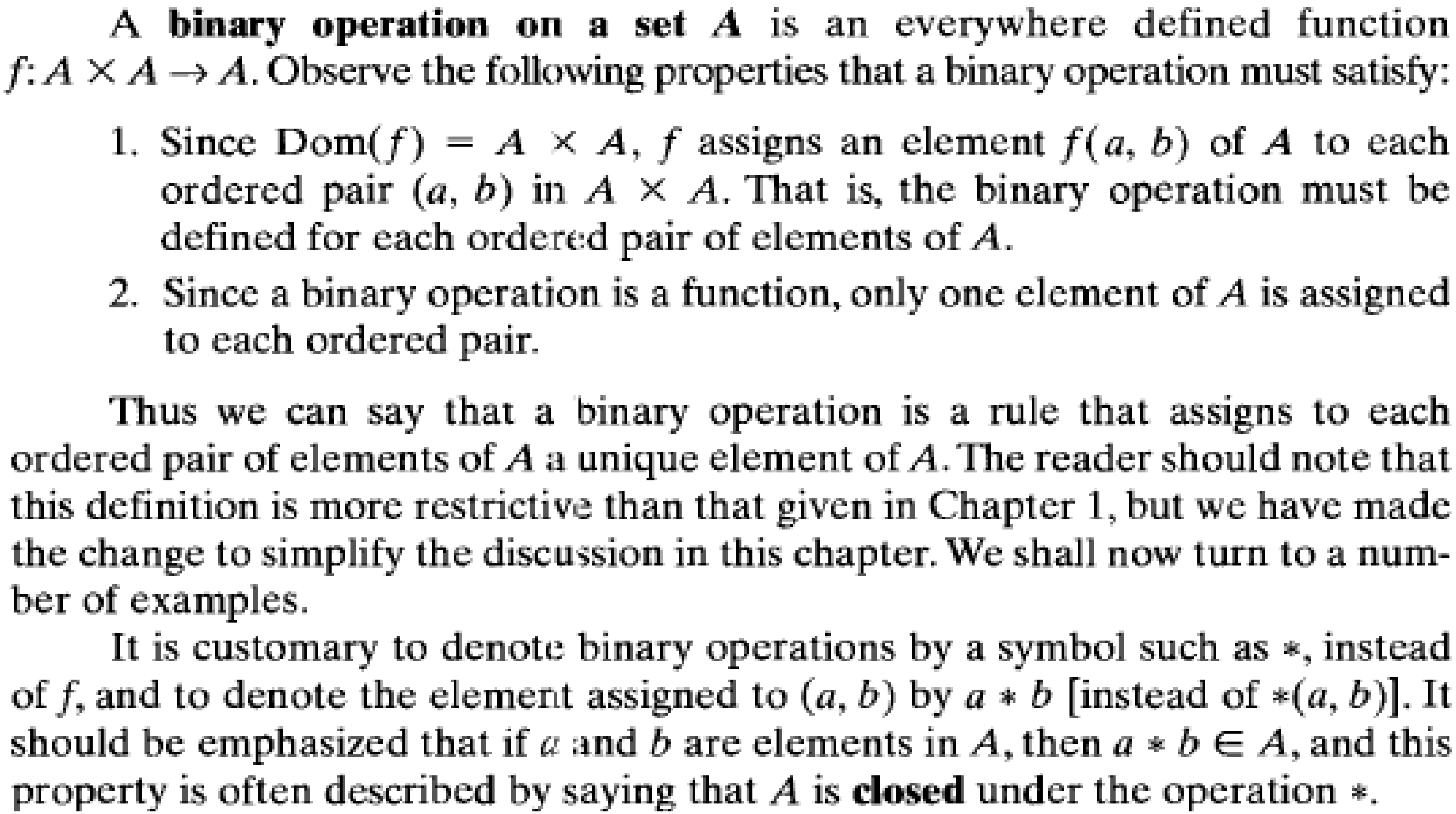
MGMCET, Navi Mumbai

Module 5 - Algebraic Structures

- 5.1 Algebraic structures with one binary operation:Semi group, Monoid, Groups, Subgroups,Abelian Group, Cyclic group, Isomorphism
- 5.2 Algebraic structures with two binary operations: Ring
- 5.3 Coding Theory: Coding, binary information and error detection, decoding and error correction

Algebraic Structures

Binary Operations

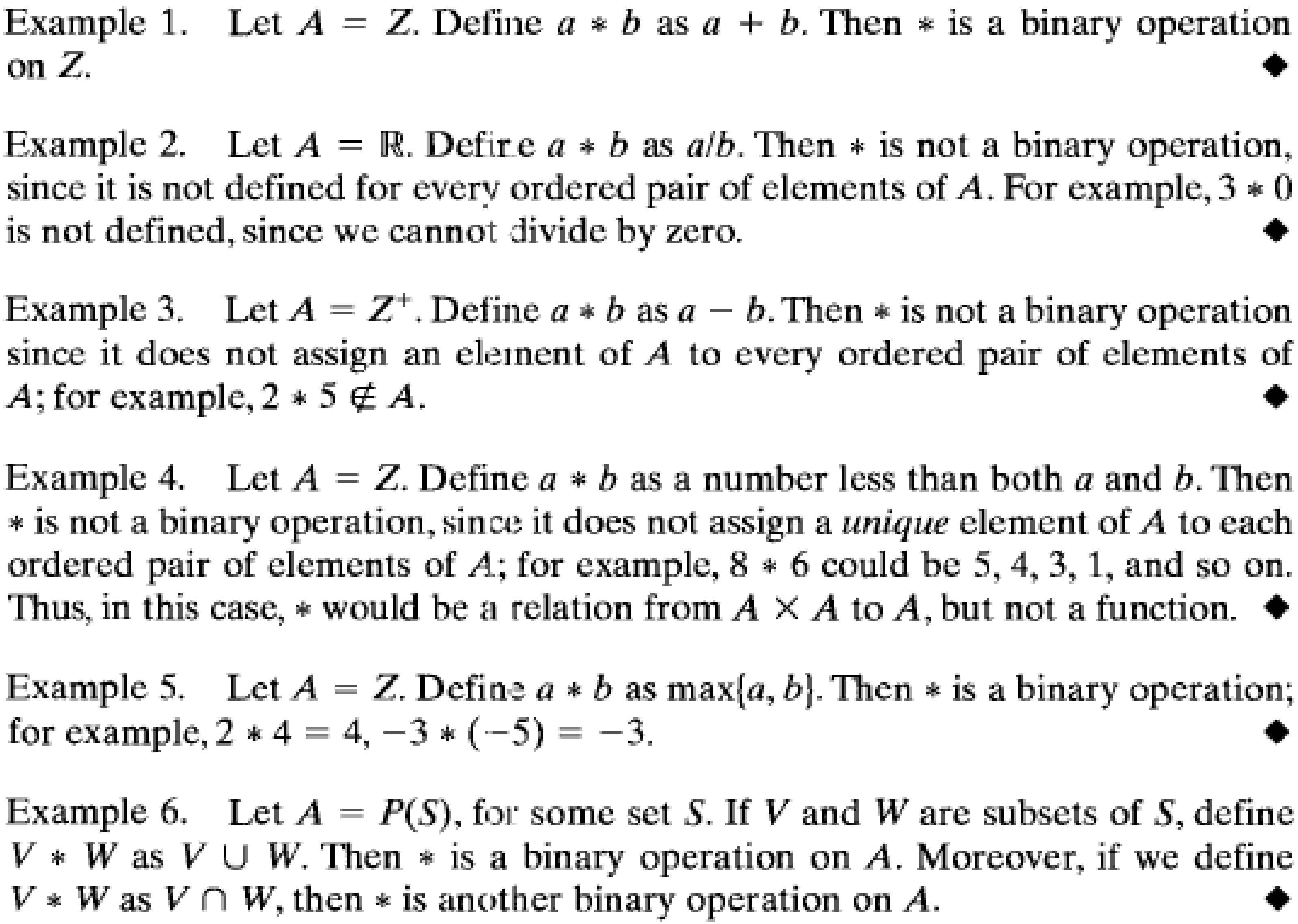


A **binary operation on a set A** is an everywhere defined function $f: A \times A \to A$. Observe the following properties that a binary operation must satisfy:

1. Since $\text{Dom}(f) = A \times A$, f assigns an element $f(a, b)$ of A to each ordered pair (a, b) in $A \times A$. That is, the binary operation must be defined for each ordered pair of elements of A.
2. Since a binary operation is a function, only one element of A is assigned to each ordered pair.

Thus we can say that a binary operation is a rule that assigns to each ordered pair of elements of A a unique element of A. The reader should note that this definition is more restrictive than that given in Chapter 1, but we have made the change to simplify the discussion in this chapter. We shall now turn to a number of examples.

It is customary to denote binary operations by a symbol such as $*$, instead of f, and to denote the element assigned to (a, b) by $a * b$ [instead of $*(a, b)$]. It should be emphasized that if a and b are elements in A, then $a * b \in A$, and this property is often described by saying that A is **closed** under the operation $*$.



Example 1. Let $A = Z$. Define $a * b$ as $a + b$. Then $*$ is a binary operation on Z. ◆

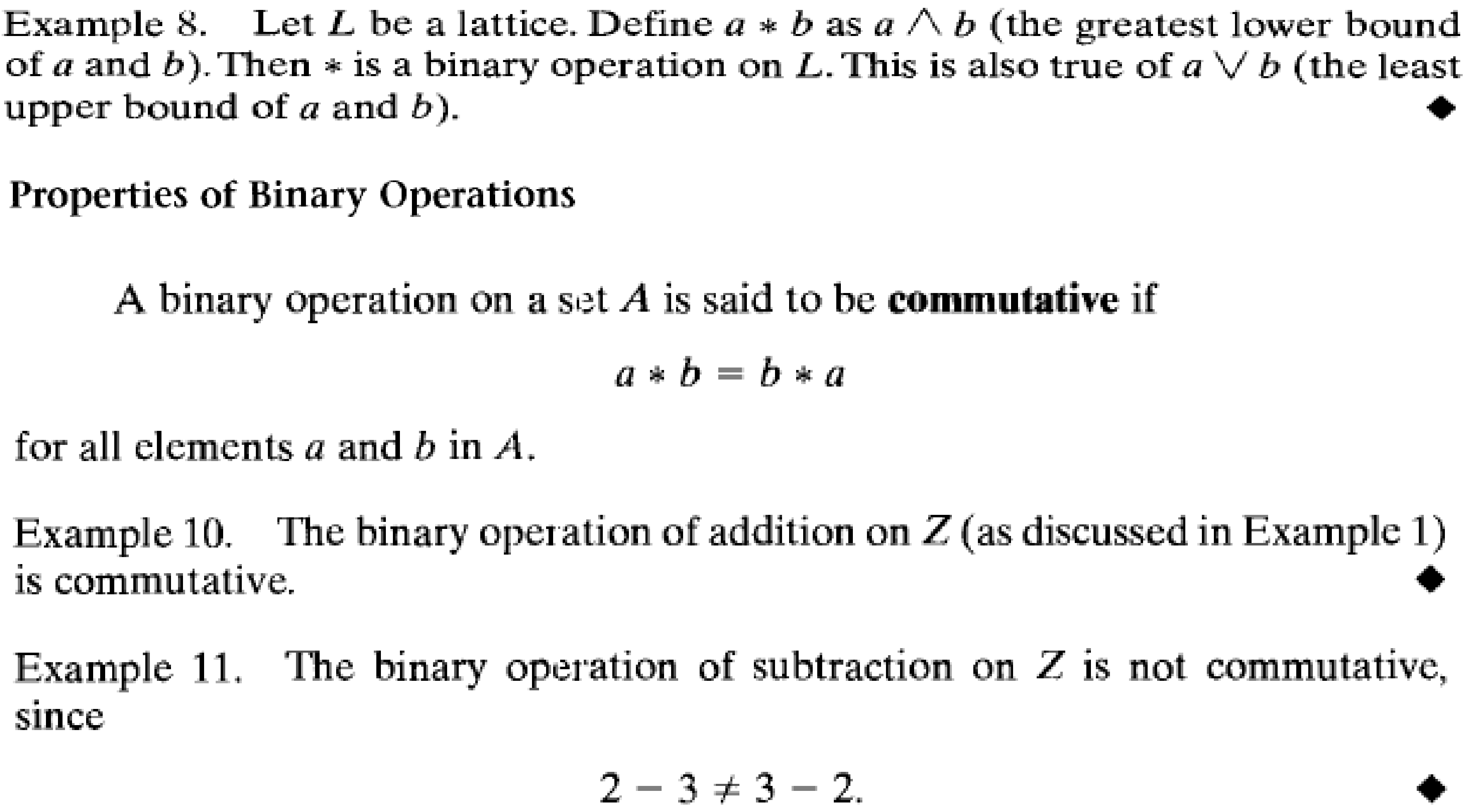
Example 2. Let $A = \mathbb{R}$. Define $a * b$ as a/b. Then $*$ is not a binary operation, since it is not defined for every ordered pair of elements of A. For example, $3 * 0$ is not defined, since we cannot divide by zero. ◆

Example 3. Let $A = Z^+$. Define $a * b$ as $a - b$. Then $*$ is not a binary operation since it does not assign an element of A to every ordered pair of elements of A; for example, $2 * 5 \notin A$. ◆

Example 4. Let $A = Z$. Define $a * b$ as a number less than both a and b. Then $*$ is not a binary operation, since it does not assign a *unique* element of A to each ordered pair of elements of A; for example, $8 * 6$ could be 5, 4, 3, 1, and so on. Thus, in this case, $*$ would be a relation from $A \times A$ to A, but not a function. ◆

Example 5. Let $A = Z$. Define $a * b$ as $\max\{a, b\}$. Then $*$ is a binary operation; for example, $2 * 4 = 4$, $-3 * (-5) = -3$. ◆

Example 6. Let $A = P(S)$, for some set S. If V and W are subsets of S, define $V * W$ as $V \cup W$. Then $*$ is a binary operation on A. Moreover, if we define $V * W$ as $V \cap W$, then $*$ is another binary operation on A. ◆



Example 8. Let L be a lattice. Define $a * b$ as $a \wedge b$ (the greatest lower bound of a and b). Then $*$ is a binary operation on L. This is also true of $a \vee b$ (the least upper bound of a and b). ◆

Properties of Binary Operations

A binary operation on a set A is said to be **commutative** if

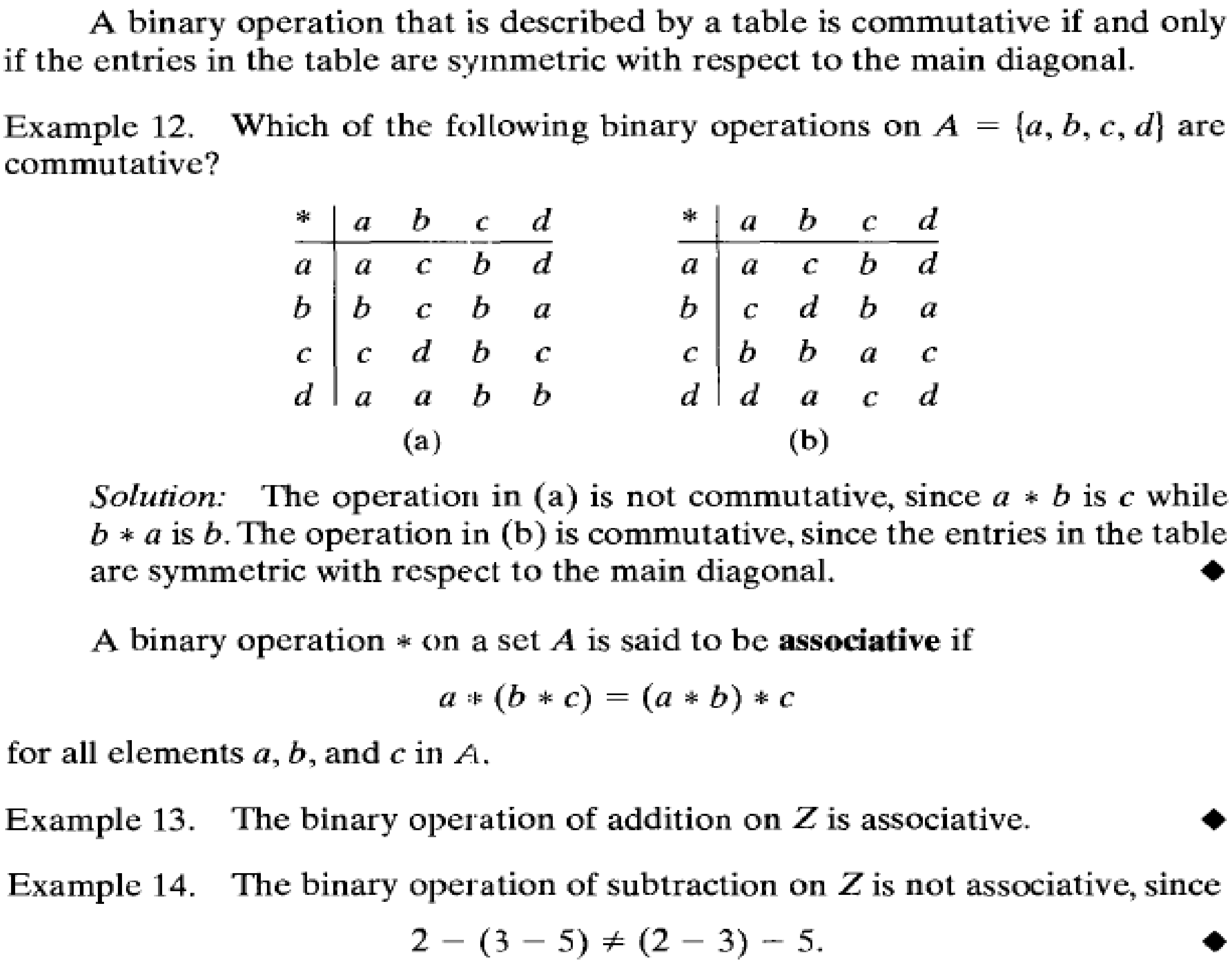
$$a * b = b * a$$

for all elements a and b in A.

Example 10. The binary operation of addition on Z (as discussed in Example 1) is commutative. ◆

Example 11. The binary operation of subtraction on Z is not commutative, since

$$2 - 3 \neq 3 - 2.$$ ◆



A binary operation that is described by a table is commutative if and only if the entries in the table are symmetric with respect to the main diagonal.

Example 12. Which of the following binary operations on $A = \{a, b, c, d\}$ are commutative?

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

(a)

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

(b)

Solution: The operation in (a) is not commutative, since $a * b$ is c while $b * a$ is b. The operation in (b) is commutative, since the entries in the table are symmetric with respect to the main diagonal. ◆

A binary operation $*$ on a set A is said to be **associative** if

$$a * (b * c) = (a * b) * c$$

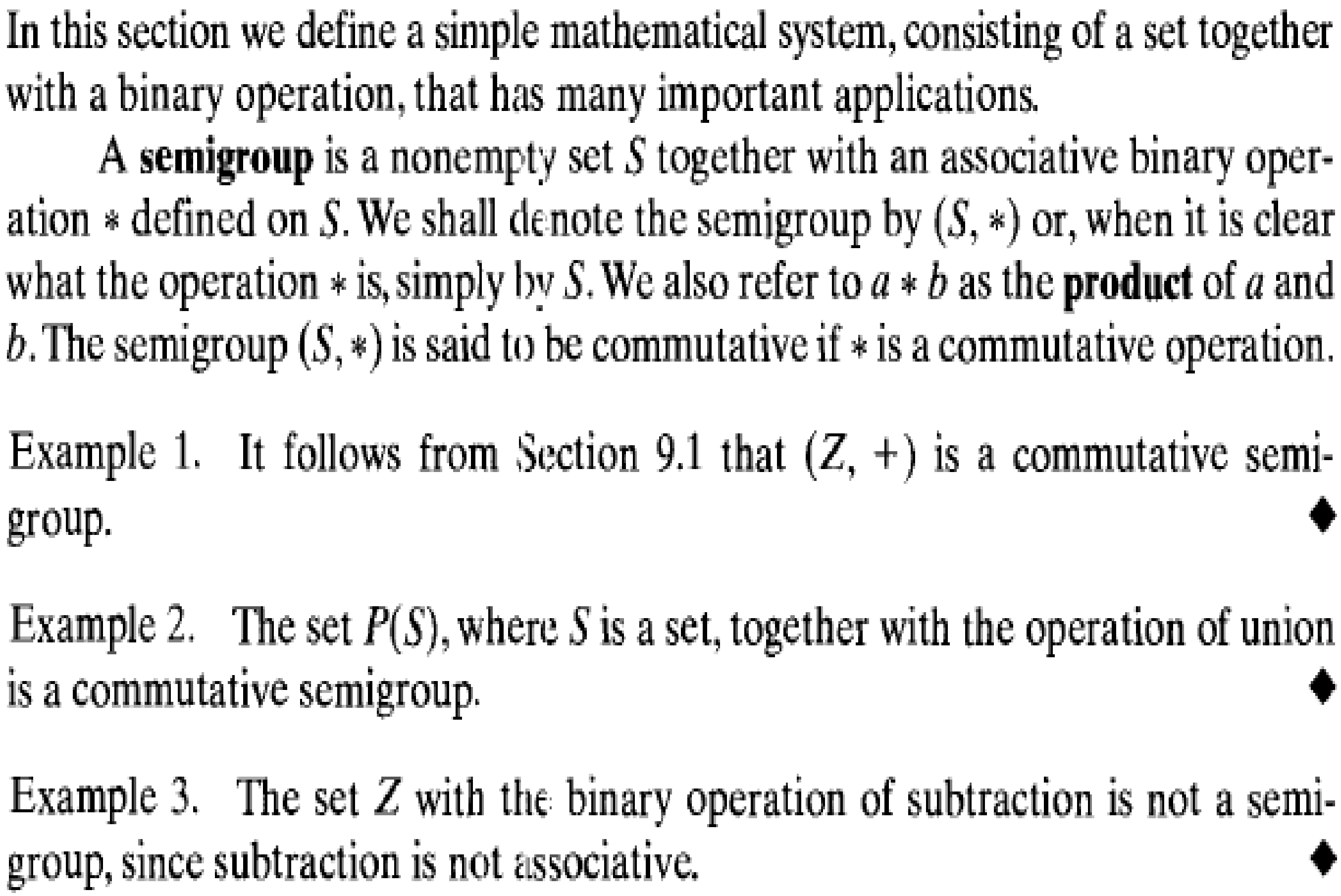
for all elements a, b, and c in A.

Example 13. The binary operation of addition on Z is associative. ◆

Example 14. The binary operation of subtraction on Z is not associative, since

$$2 - (3 - 5) \neq (2 - 3) - 5.$$ ◆

Semigroups



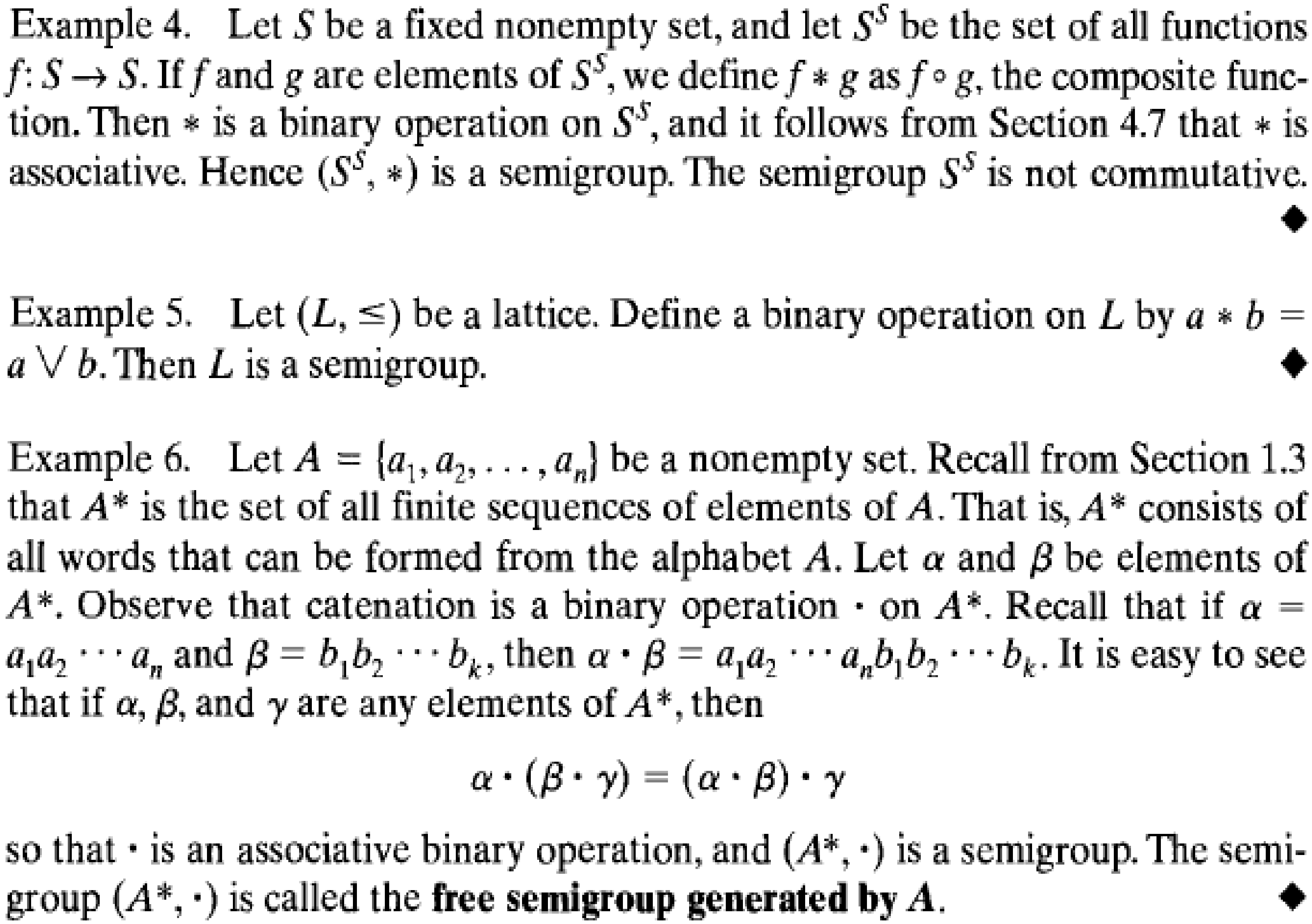
In this section we define a simple mathematical system, consisting of a set together with a binary operation, that has many important applications.

A **semigroup** is a nonempty set S together with an associative binary operation $*$ defined on S. We shall denote the semigroup by $(S, *)$ or, when it is clear what the operation $*$ is, simply by S. We also refer to $a * b$ as the **product** of a and b. The semigroup $(S, *)$ is said to be commutative if $*$ is a commutative operation.

Example 1. It follows from Section 9.1 that $(Z, +)$ is a commutative semigroup. ◆

Example 2. The set $P(S)$, where S is a set, together with the operation of union is a commutative semigroup. ◆

Example 3. The set Z with the binary operation of subtraction is not a semigroup, since subtraction is not associative. ◆



Example 4. Let S be a fixed nonempty set, and let S^S be the set of all functions $f: S \to S$. If f and g are elements of S^S, we define $f * g$ as $f \circ g$, the composite function. Then $*$ is a binary operation on S^S, and it follows from Section 4.7 that $*$ is associative. Hence $(S^S, *)$ is a semigroup. The semigroup S^S is not commutative. ◆

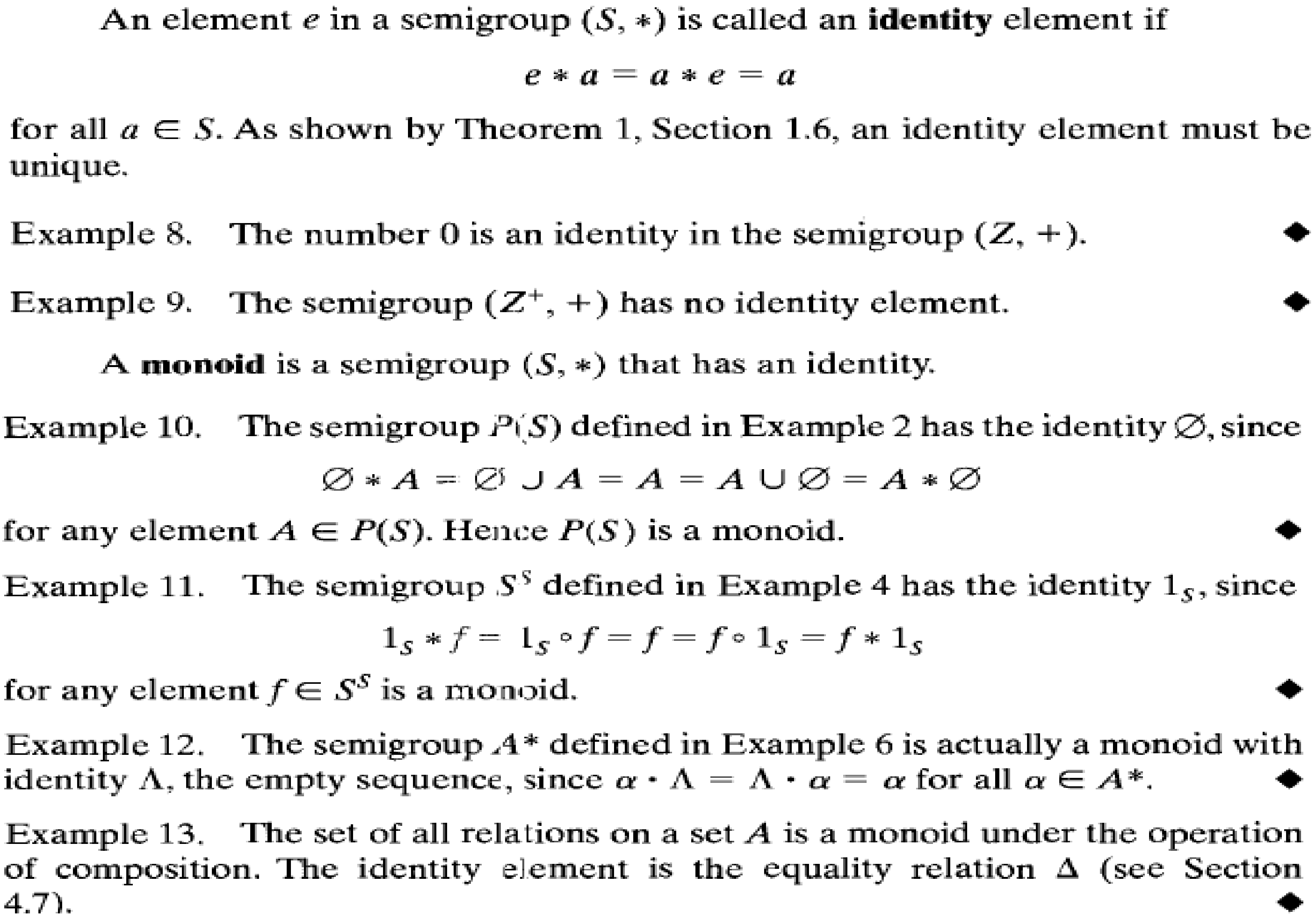
Example 5. Let $(L, \leq)$ be a lattice. Define a binary operation on L by $a * b = a \vee b$. Then L is a semigroup. ◆

Example 6. Let $A = \{a_1, a_2, \ldots, a_n\}$ be a nonempty set. Recall from Section 1.3 that A^* is the set of all finite sequences of elements of A. That is, A^* consists of all words that can be formed from the alphabet A. Let α and β be elements of A^*. Observe that catenation is a binary operation $\cdot$ on A^*. Recall that if $\alpha = a_1a_2 \cdots a_n$ and $\beta = b_1b_2 \cdots b_k$, then $\alpha \cdot \beta = a_1a_2 \cdots a_nb_1b_2 \cdots b_k$. It is easy to see that if α, β, and γ are any elements of A^*, then

$$\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$$

so that $\cdot$ is an associative binary operation, and $(A^*, \cdot)$ is a semigroup. The semigroup $(A^*, \cdot)$ is called the **free semigroup generated by A**. ◆

Monoid



An element e in a semigroup $(S, *)$ is called an **identity** element if

$$e * a = a * e = a$$

for all $a \in S$. As shown by Theorem 1, Section 1.6, an identity element must be unique.

Example 8. The number 0 is an identity in the semigroup $(Z, +)$. ◆

Example 9. The semigroup $(Z^+, +)$ has no identity element. ◆

A **monoid** is a semigroup $(S, *)$ that has an identity.

Example 10. The semigroup $P(S)$ defined in Example 2 has the identity $\varnothing$, since

$$\varnothing * A = \varnothing \cup A = A = A \cup \varnothing = A * \varnothing$$

for any element $A \in P(S)$. Hence $P(S)$ is a monoid. ◆

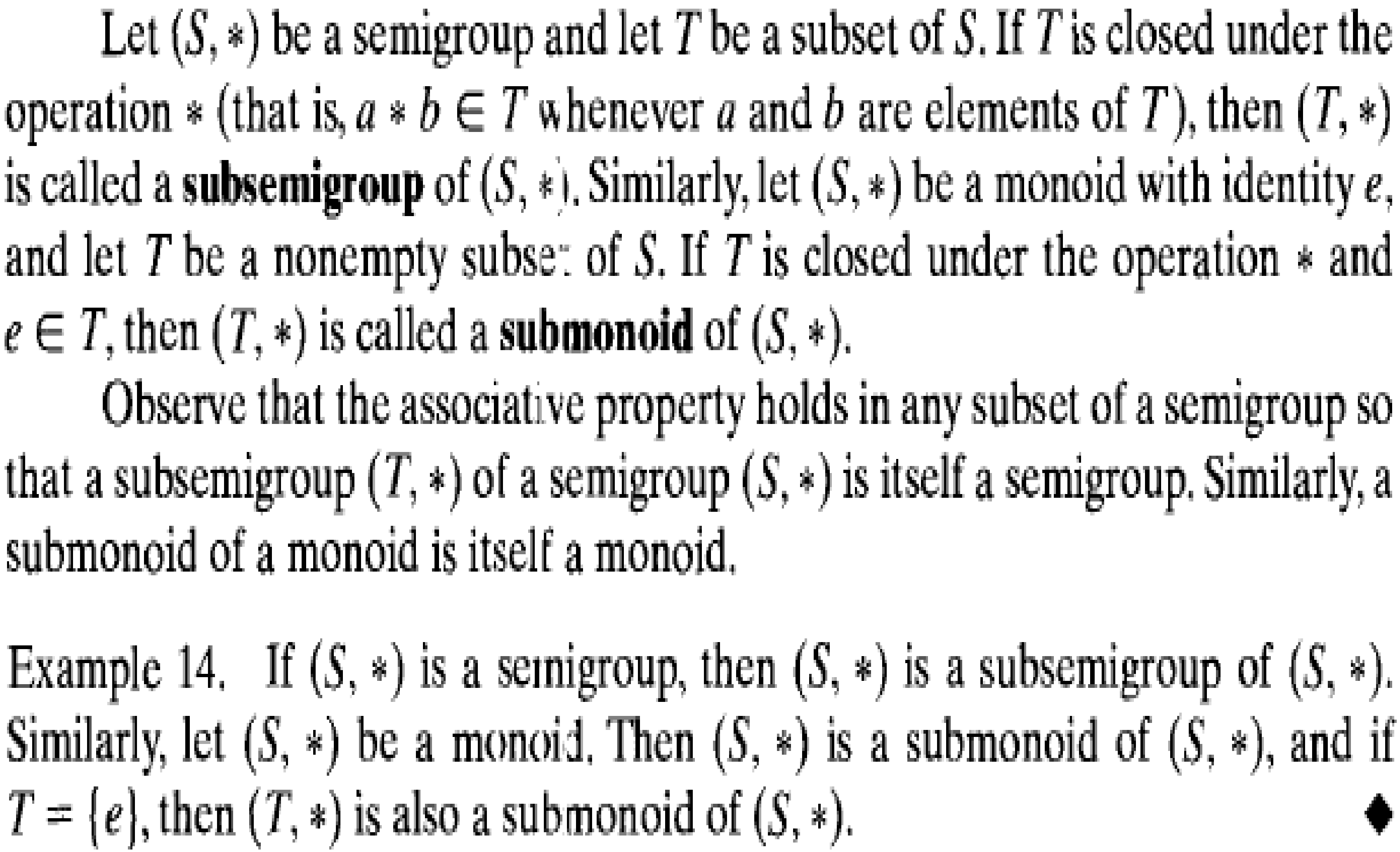
Example 11. The semigroup S^S defined in Example 4 has the identity 1_S, since

$$1_S * f = 1_S \circ f = f = f \circ 1_S = f * 1_S$$

for any element $f \in S^S$ is a monoid. ◆

Example 12. The semigroup A^* defined in Example 6 is actually a monoid with identity Λ, the empty sequence, since $\alpha \cdot \Lambda = \Lambda \cdot \alpha = \alpha$ for all $\alpha \in A^*$. ◆

Example 13. The set of all relations on a set A is a monoid under the operation of composition. The identity element is the equality relation Δ (see Section 4.7). ◆

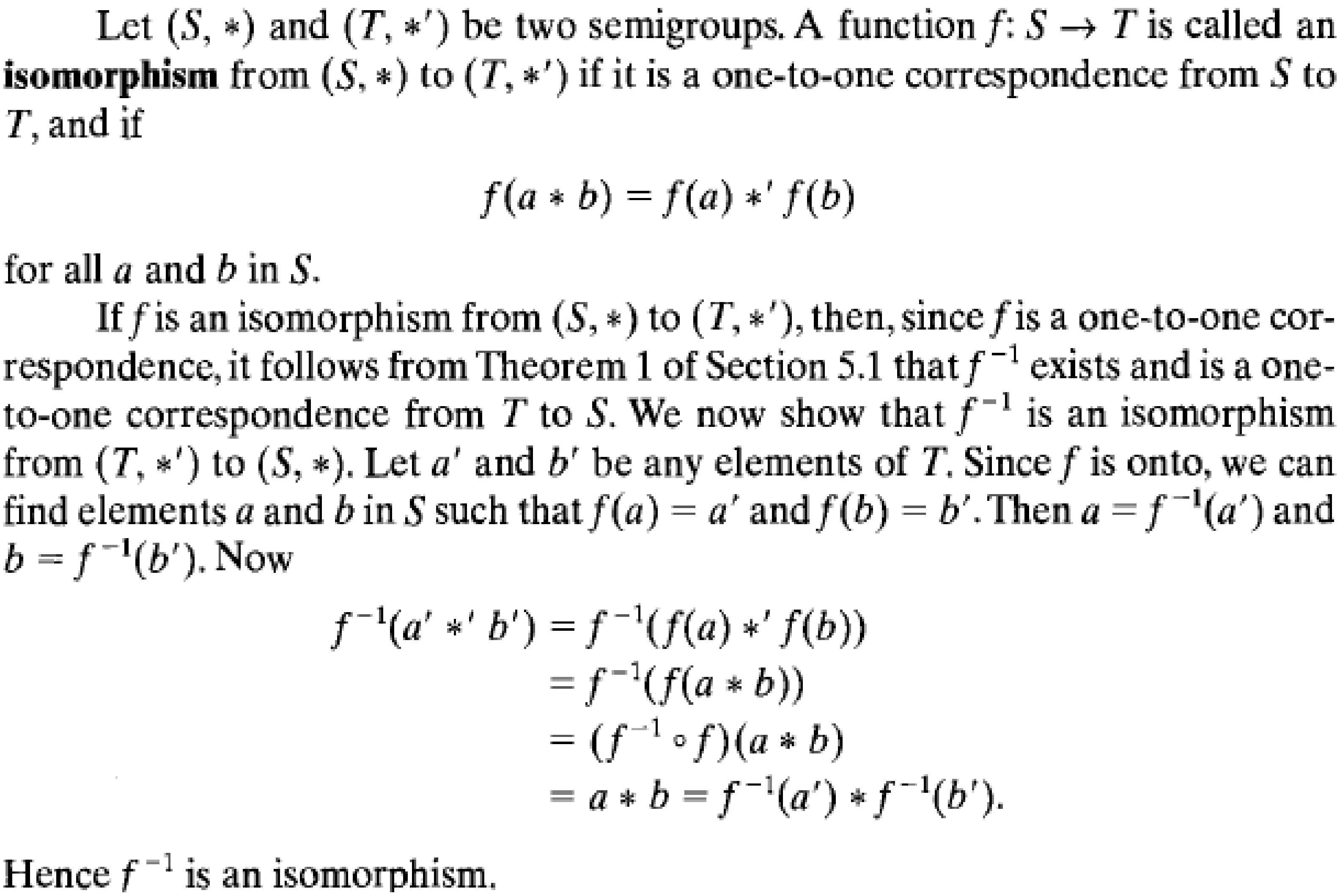


Let $(S, *)$ be a semigroup and let T be a subset of S. If T is closed under the operation $*$ (that is, $a * b \in T$ whenever a and b are elements of T), then $(T, *)$ is called a **subsemigroup** of $(S, *)$. Similarly, let $(S, *)$ be a monoid with identity e, and let T be a nonempty subset of S. If T is closed under the operation $*$ and $e \in T$, then $(T, *)$ is called a **submonoid** of $(S, *)$.

Observe that the associative property holds in any subset of a semigroup so that a subsemigroup $(T, *)$ of a semigroup $(S, *)$ is itself a semigroup. Similarly, a submonoid of a monoid is itself a monoid.

Example 14. If $(S, *)$ is a semigroup, then $(S, *)$ is a subsemigroup of $(S, *)$. Similarly, let $(S, *)$ be a monoid. Then $(S, *)$ is a submonoid of $(S, *)$, and if $T = \{e\}$, then $(T, *)$ is also a submonoid of $(S, *)$. ◆

Isomorphism



Let $(S, *)$ and $(T, *')$ be two semigroups. A function $f \colon S \to T$ is called an **isomorphism** from $(S, *)$ to $(T, *')$ if it is a one-to-one correspondence from S to T, and if

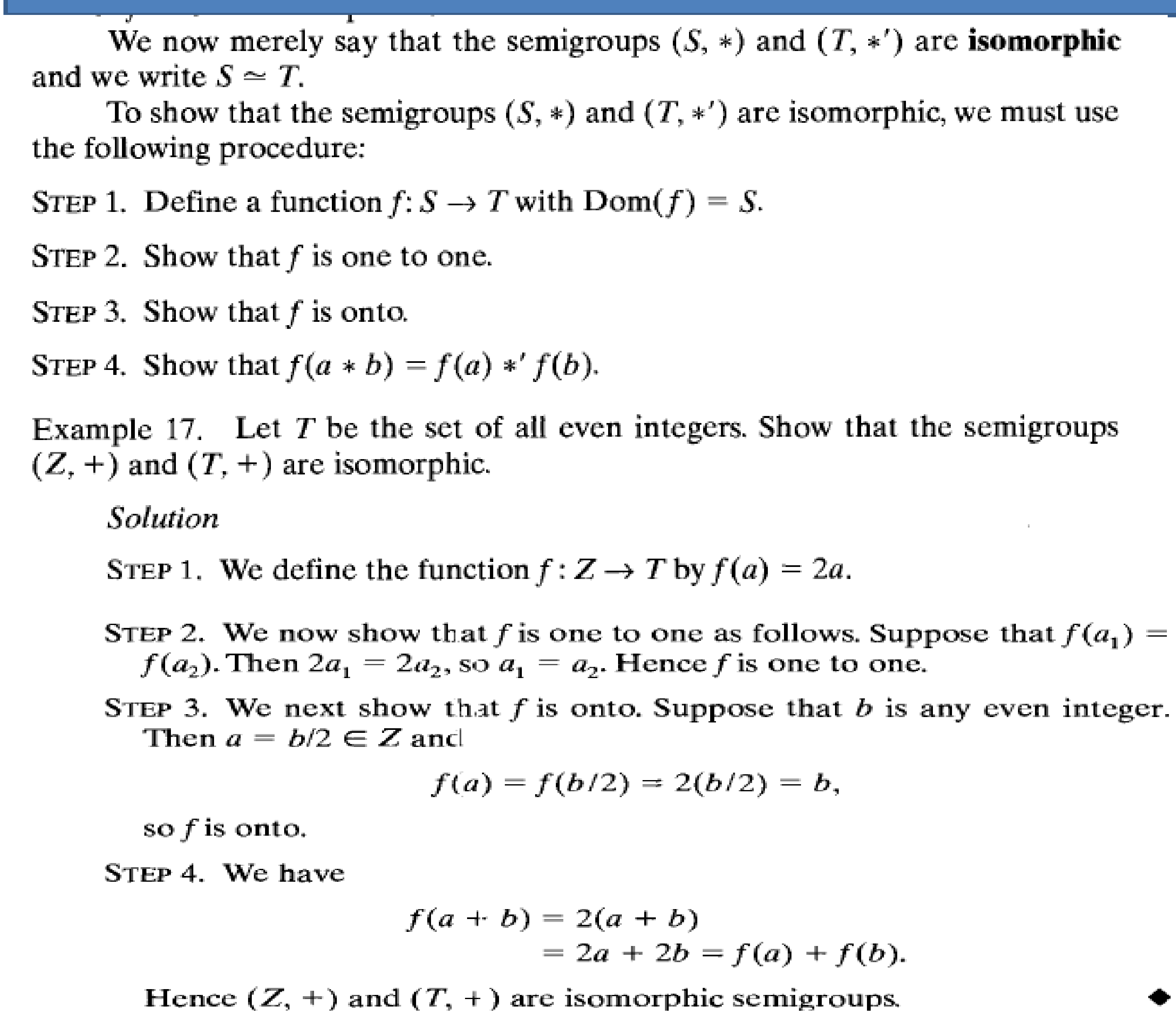
$$f(a * b) = f(a) *' f(b)$$

for all a and b in S.

If f is an isomorphism from $(S, *)$ to $(T, *')$, then, since f is a one-to-one correspondence, it follows from Theorem 1 of Section 5.1 that f^{-1} exists and is a one-to-one correspondence from T to S. We now show that f^{-1} is an isomorphism from $(T, *')$ to $(S, *)$. Let a' and b' be any elements of T. Since f is onto, we can find elements a and b in S such that $f(a) = a'$ and $f(b) = b'$. Then $a = f^{-1}(a')$ and $b = f^{-1}(b')$. Now

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

Hence f^{-1} is an isomorphism.



We now merely say that the semigroups $(S, *)$ and $(T, *')$ are **isomorphic** and we write $S \simeq T$.

To show that the semigroups $(S, *)$ and $(T, *')$ are isomorphic, we must use the following procedure:

STEP 1. Define a function $f\colon S \to T$ with $\text{Dom}(f) = S$.

STEP 2. Show that f is one to one.

STEP 3. Show that f is onto.

STEP 4. Show that $f(a * b) = f(a) *' f(b)$.

Example 17. Let T be the set of all even integers. Show that the semigroups $(Z, +)$ and $(T, +)$ are isomorphic.

Solution

STEP 1. We define the function $f : Z \to T$ by $f(a) = 2a$.

STEP 2. We now show that f is one to one as follows. Suppose that $f(a_1) = f(a_2)$. Then $2a_1 = 2a_2$, so $a_1 = a_2$. Hence f is one to one.

STEP 3. We next show that f is onto. Suppose that b is any even integer. Then $a = b/2 \in Z$ and

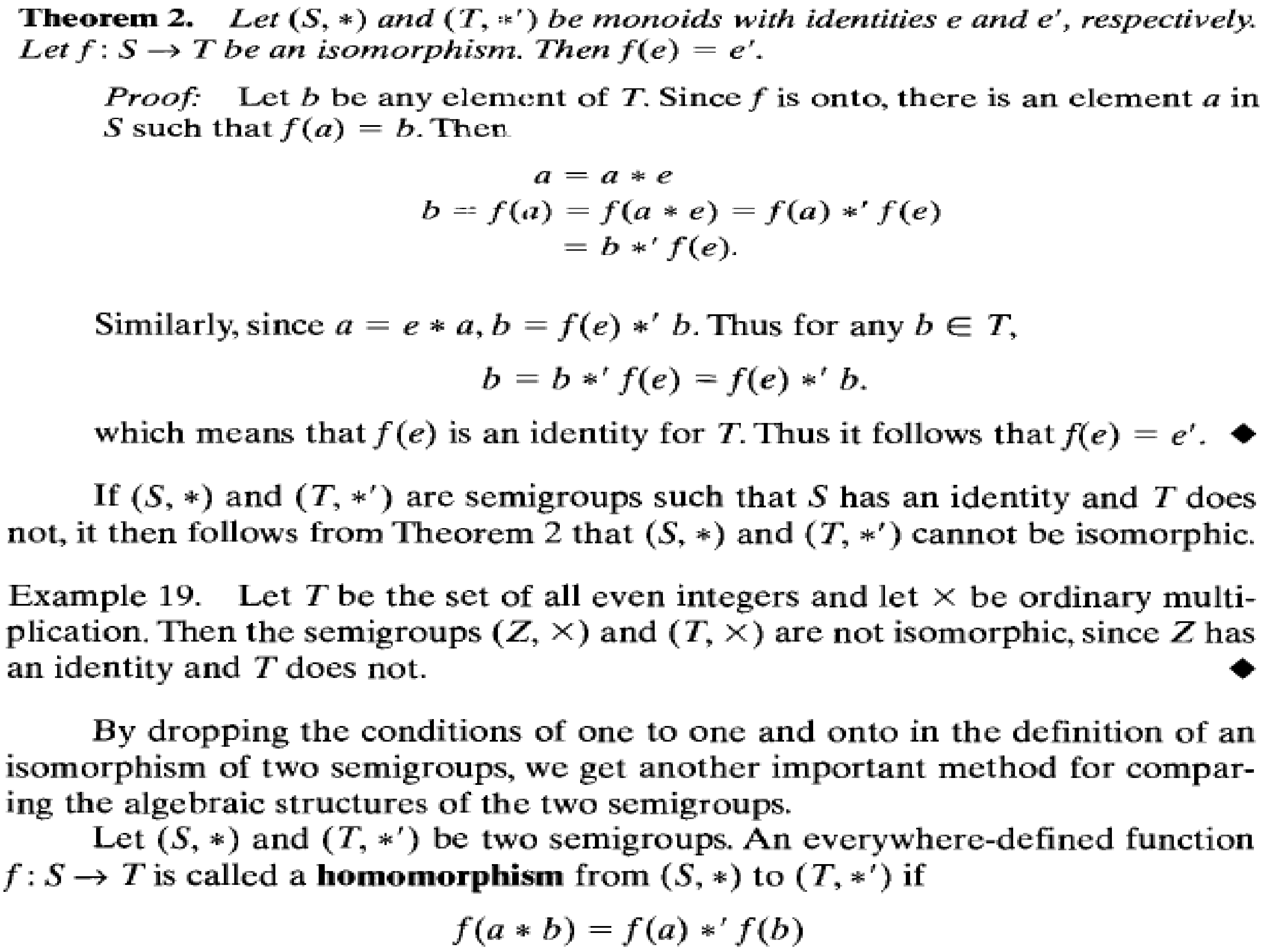
$$f(a) = f(b/2) = 2(b/2) = b,$$

so f is onto.

STEP 4. We have

$$\begin{aligned} f(a + b) &= 2(a + b) \\ &= 2a + 2b = f(a) + f(b). \end{aligned}$$

Hence $(Z, +)$ and $(T, +)$ are isomorphic semigroups. ◆



Theorem 2. *Let $(S, *)$ and $(T, *')$ be monoids with identities e and e', respectively. Let $f : S \to T$ be an isomorphism. Then $f(e) = e'$.*

Proof: Let b be any element of T. Since f is onto, there is an element a in S such that $f(a) = b$. Then

$$\begin{aligned} a &= a * e \\ b = f(a) &= f(a * e) = f(a) *' f(e) \\ &= b *' f(e). \end{aligned}$$

Similarly, since $a = e * a$, $b = f(e) *' b$. Thus for any $b \in T$,

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

which means that $f(e)$ is an identity for T. Thus it follows that $f(e) = e'$. ◆

If $(S, *)$ and $(T, *')$ are semigroups such that S has an identity and T does not, it then follows from Theorem 2 that $(S, *)$ and $(T, *')$ cannot be isomorphic.

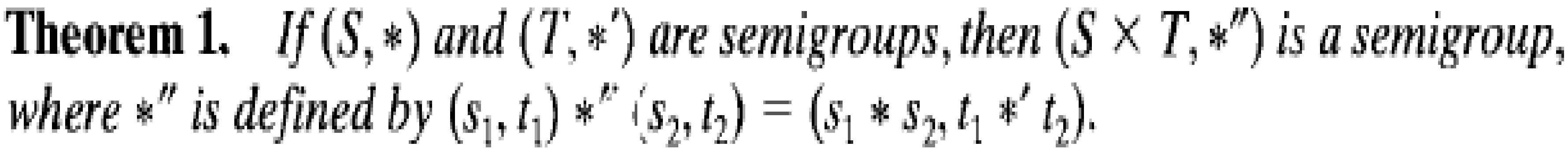
Example 19. Let T be the set of all even integers and let × be ordinary multiplication. Then the semigroups $(Z, \times)$ and $(T, \times)$ are not isomorphic, since Z has an identity and T does not. ◆

By dropping the conditions of one to one and onto in the definition of an isomorphism of two semigroups, we get another important method for comparing the algebraic structures of the two semigroups.

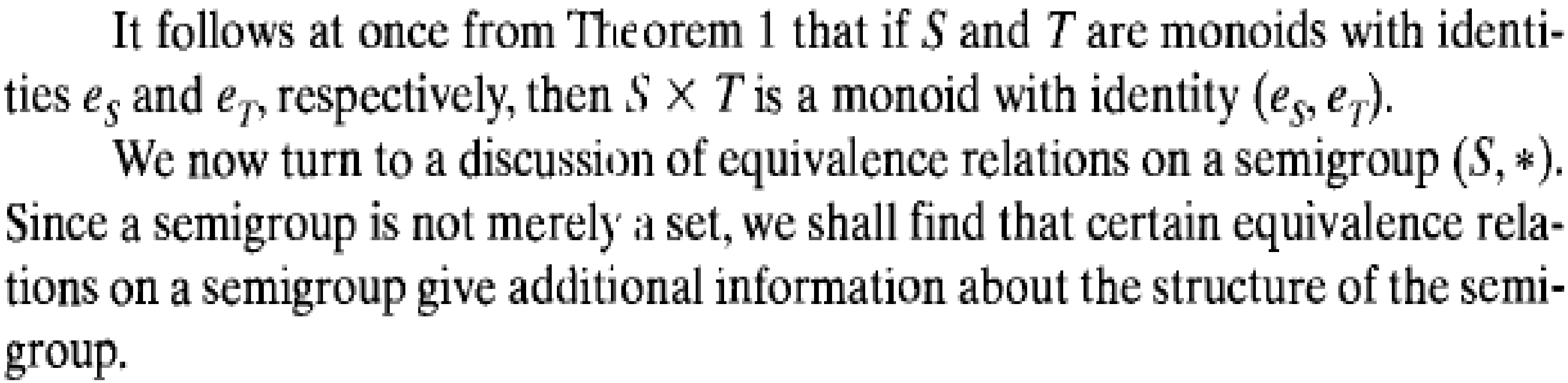
Let $(S, *)$ and $(T, *')$ be two semigroups. An everywhere-defined function $f : S \to T$ is called a **homomorphism** from $(S, *)$ to $(T, *')$ if

$$f(a * b) = f(a) *' f(b)$$

Products and Quotients of Semigroups



Theorem 1. *If $(S, *)$ and $(T, *')$ are semigroups, then $(S \times T, *'')$ is a semigroup, where $*''$ is defined by $(s_1, t_1) *'' (s_2, t_2) = (s_1 * s_2, t_1 *' t_2)$.*



It follows at once from Theorem 1 that if S and T are monoids with identities e_S and e_T, respectively, then $S \times T$ is a monoid with identity (e_S, e_T).

We now turn to a discussion of equivalence relations on a semigroup $(S, *)$. Since a semigroup is not merely a set, we shall find that certain equivalence relations on a semigroup give additional information about the structure of the semigroup.

An equivalence relation R on the semigroup $(S, *)$ is called a **congruence relation** if

$$a \; R \; a' \quad \text{and} \quad b \; R \; b' \quad \text{imply} \quad (a * b) \; R \; (a' * b').$$

Example 1. Consider the semigroup $(Z, +)$ and the equivalence relation R on Z defined by

$$a \; R \; b \quad \text{if and only if} \quad a \equiv b \pmod{2}.$$

Recall that we discussed this equivalence relation in Section 4.5. Note that if a and b yield the same remainder when divided by 2, then $2 \mid (a - b)$. We now show that this relation is a congruence relation as follows.

If

$$a \equiv b \pmod{2} \quad \text{and} \quad c \equiv d \pmod{2},$$

then 2 divides $a - b$ and 2 divides $c - d$, so

$$a - b = 2m \quad \text{and} \quad c - d = 2n,$$

where m and n are in Z. Adding, we have

$$(a - b) + (c - d) = 2m + 2n$$

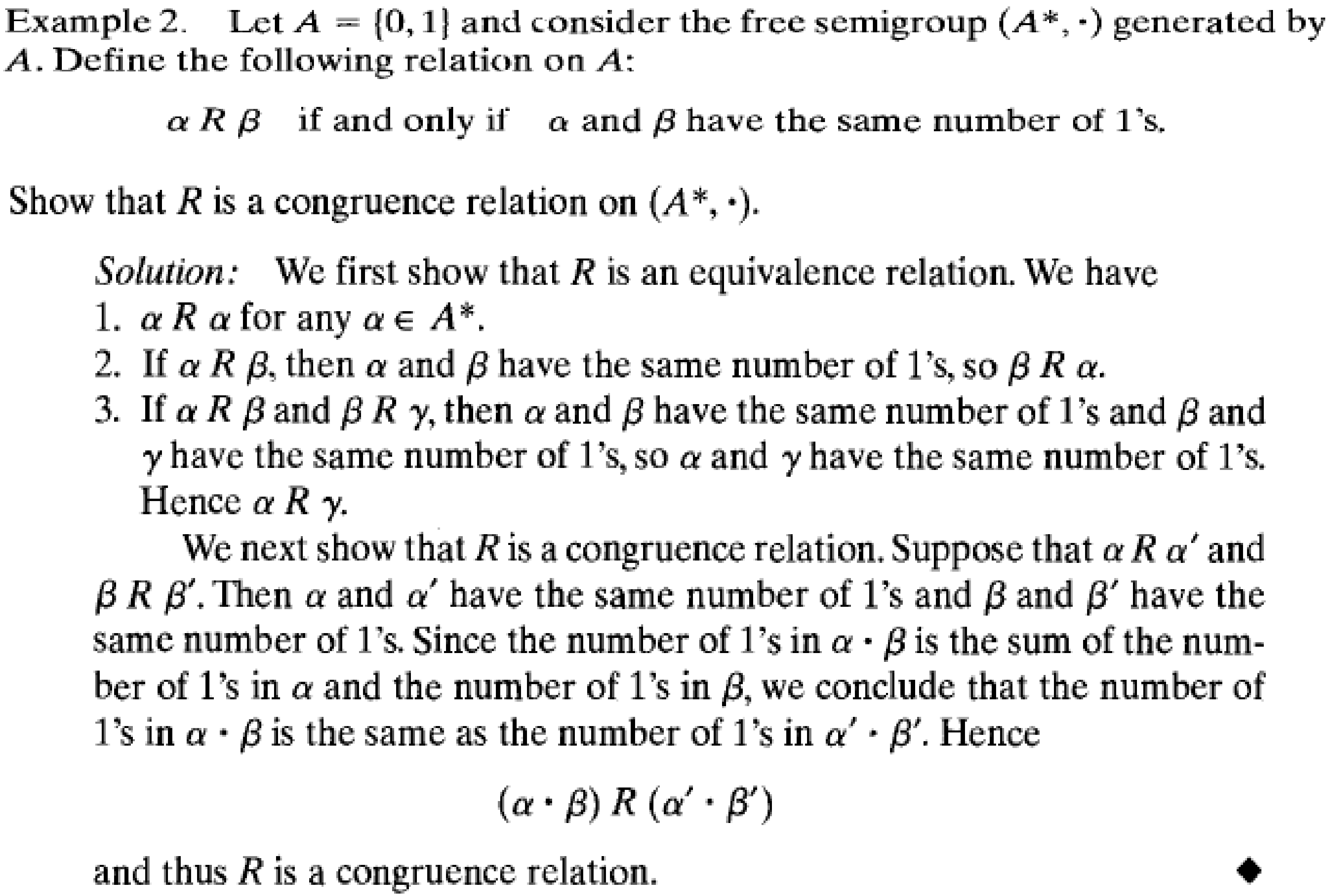
or

$$(a + c) - (b + d) = 2(m + n),$$

so

$$a + c \equiv b + d \pmod{2}.$$

Hence the relation is a congruence relation. ◆



Example 2. Let $A = \{0, 1\}$ and consider the free semigroup $(A^*, \cdot)$ generated by A. Define the following relation on A:

$$\alpha \; R \; \beta \quad \text{if and only if} \quad \alpha \text{ and } \beta \text{ have the same number of 1's.}$$

Show that R is a congruence relation on $(A^*, \cdot)$.

Solution: We first show that R is an equivalence relation. We have

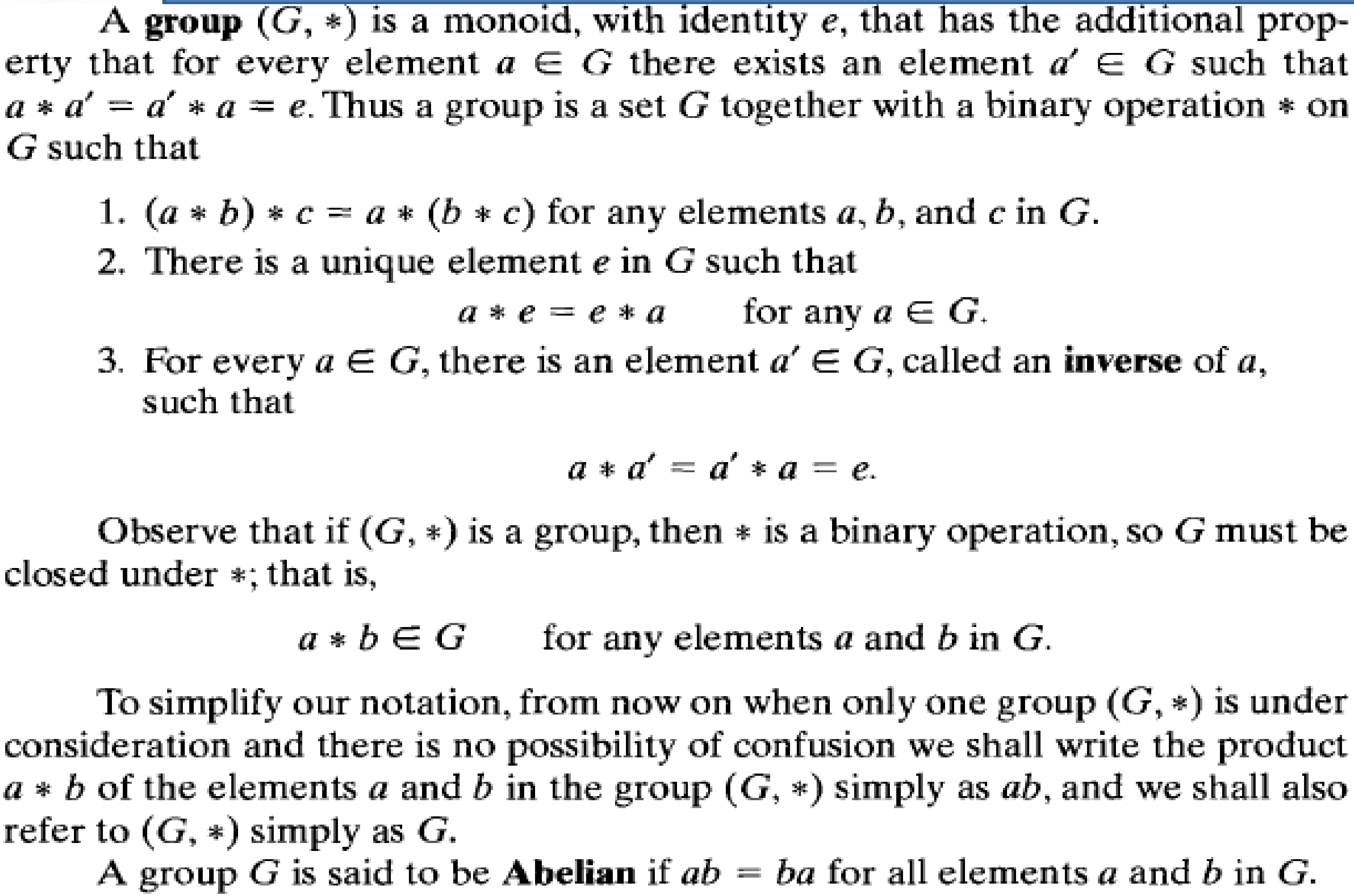
1. $\alpha \; R \; \alpha$ for any $\alpha \in A^*$.
2. If $\alpha \; R \; \beta$, then α and β have the same number of 1's, so $\beta \; R \; \alpha$.
3. If $\alpha \; R \; \beta$ and $\beta \; R \; \gamma$, then α and β have the same number of 1's and β and γ have the same number of 1's, so α and γ have the same number of 1's. Hence $\alpha \; R \; \gamma$.

We next show that R is a congruence relation. Suppose that $\alpha \; R \; \alpha'$ and $\beta \; R \; \beta'$. Then α and α' have the same number of 1's and β and β' have the same number of 1's. Since the number of 1's in $\alpha \cdot \beta$ is the sum of the number of 1's in α and the number of 1's in β, we conclude that the number of 1's in $\alpha \cdot \beta$ is the same as the number of 1's in $\alpha' \cdot \beta'$. Hence

$$(\alpha \cdot \beta) \; R \; (\alpha' \cdot \beta')$$

and thus R is a congruence relation. ◆

Groups



A **group** $(G, *)$ is a monoid, with identity e, that has the additional property that for every element $a \in G$ there exists an element $a' \in G$ such that $a * a' = a' * a = e$. Thus a group is a set G together with a binary operation $*$ on G such that

1. $(a * b) * c = a * (b * c)$ for any elements a, b, and c in G.
2. There is a unique element e in G such that
$$a * e = e * a \qquad \text{for any } a \in G.$$
3. For every $a \in G$, there is an element $a' \in G$, called an **inverse** of a, such that
$$a * a' = a' * a = e.$$

Observe that if $(G, *)$ is a group, then $*$ is a binary operation, so G must be closed under $*$; that is,

$$a * b \in G \qquad \text{for any elements } a \text{ and } b \text{ in } G.$$

To simplify our notation, from now on when only one group $(G, *)$ is under consideration and there is no possibility of confusion we shall write the product $a * b$ of the elements a and b in the group $(G, *)$ simply as ab, and we shall also refer to $(G, *)$ simply as G.

A group G is said to be **Abelian** if $ab = ba$ for all elements a and b in G.

Example 1. The set of all integers Z with the operation of ordinary addition is an Abelian group. If $a \in Z$, then an inverse of a is its negative $-a$. ◆

Example 2. The set Z^+ under the operation of ordinary multiplication is not a group since the element 2 in Z^+ has no inverse. However, this set together with the given operation is a monoid. ◆

Example 3. The set of all nonzero real numbers under the operation of ordinary multiplication is a group. An inverse of $a \neq 0$ is $1/a$. ◆

Example 4. Let G be the set of all nonzero real numbers and let

$$a * b = \frac{ab}{2}.$$

Show that $(G, *)$ is an Abelian group.

Solution: We first verify that $*$ is a binary operation. If a and b are elements of G, then $ab/2$ is a nonzero real number and hence is in G. We next verify associativity. Since

$$(a * b) * c = \left(\frac{ab}{2}\right) * c = \frac{(ab)c}{4}$$

and since

and since

$$a * (b * c) = a * \left(\frac{bc}{2}\right) = \frac{a(bc)}{4} = \frac{(ab)c}{4},$$

the operation $*$ is associative.

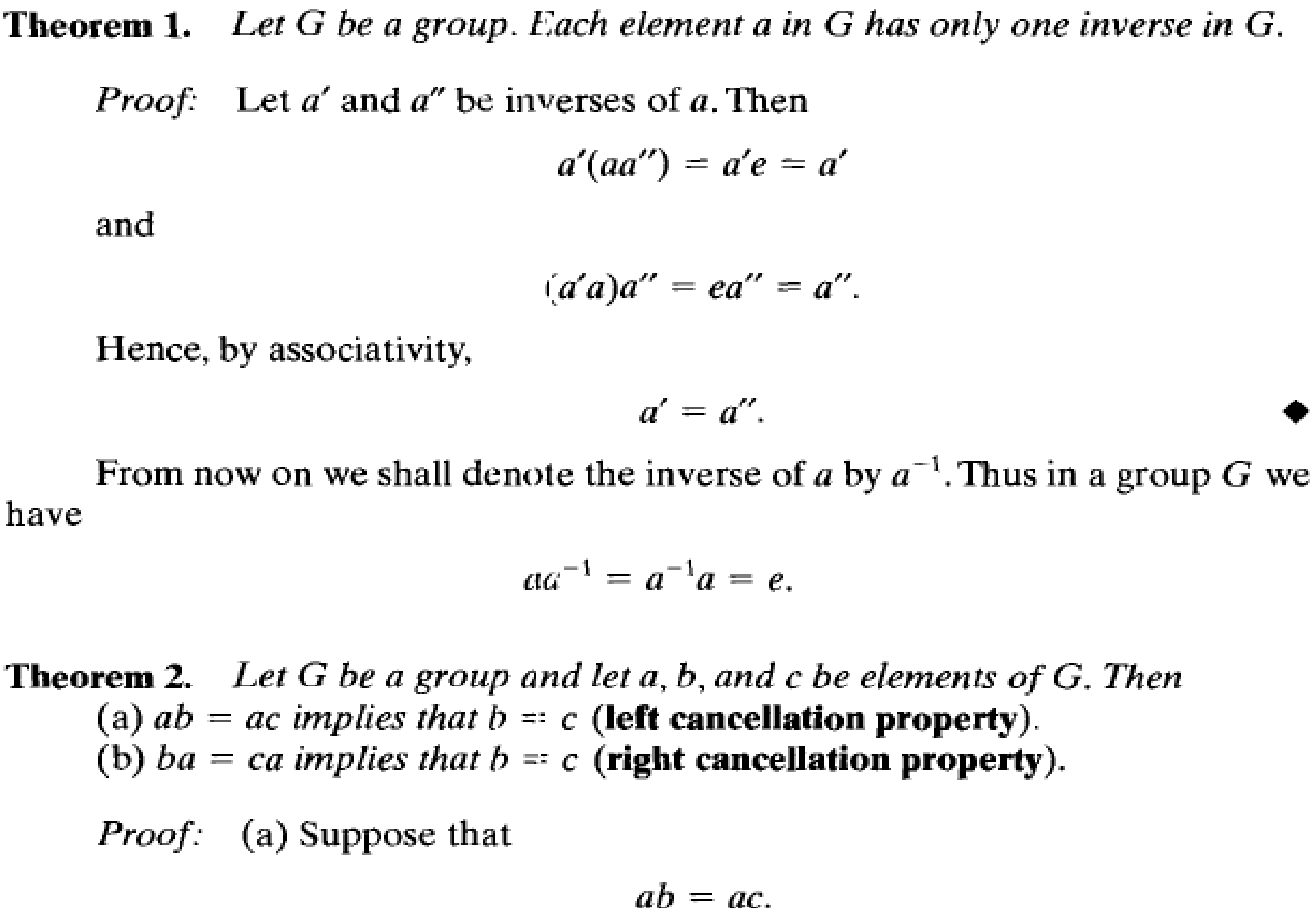
The number 2 is the identity in G, for if $a \in G$, then

$$a * 2 = \frac{(a)(2)}{2} = a = \frac{(2)(a)}{2} = 2 * a.$$

Finally, if $a \in G$, then $a' = 4/a$ is an inverse of a, since

$$a * a' = a * \frac{4}{a} = \frac{a(4/a)}{2} = 2 = \frac{(4/a)(a)}{2} = \frac{4}{a} * a = a' * a.$$

Since $a * b = b * a$ for all a and b in G, we conclude that G is an Abelian group. ◆



Theorem 1. *Let G be a group. Each element a in G has only one inverse in G.*

Proof: Let a' and a'' be inverses of a. Then

$$a'(aa'') = a'e = a'$$

and

$$(a'a)a'' = ea'' = a''.$$

Hence, by associativity,

$$a' = a''. \qquad \blacklozenge$$

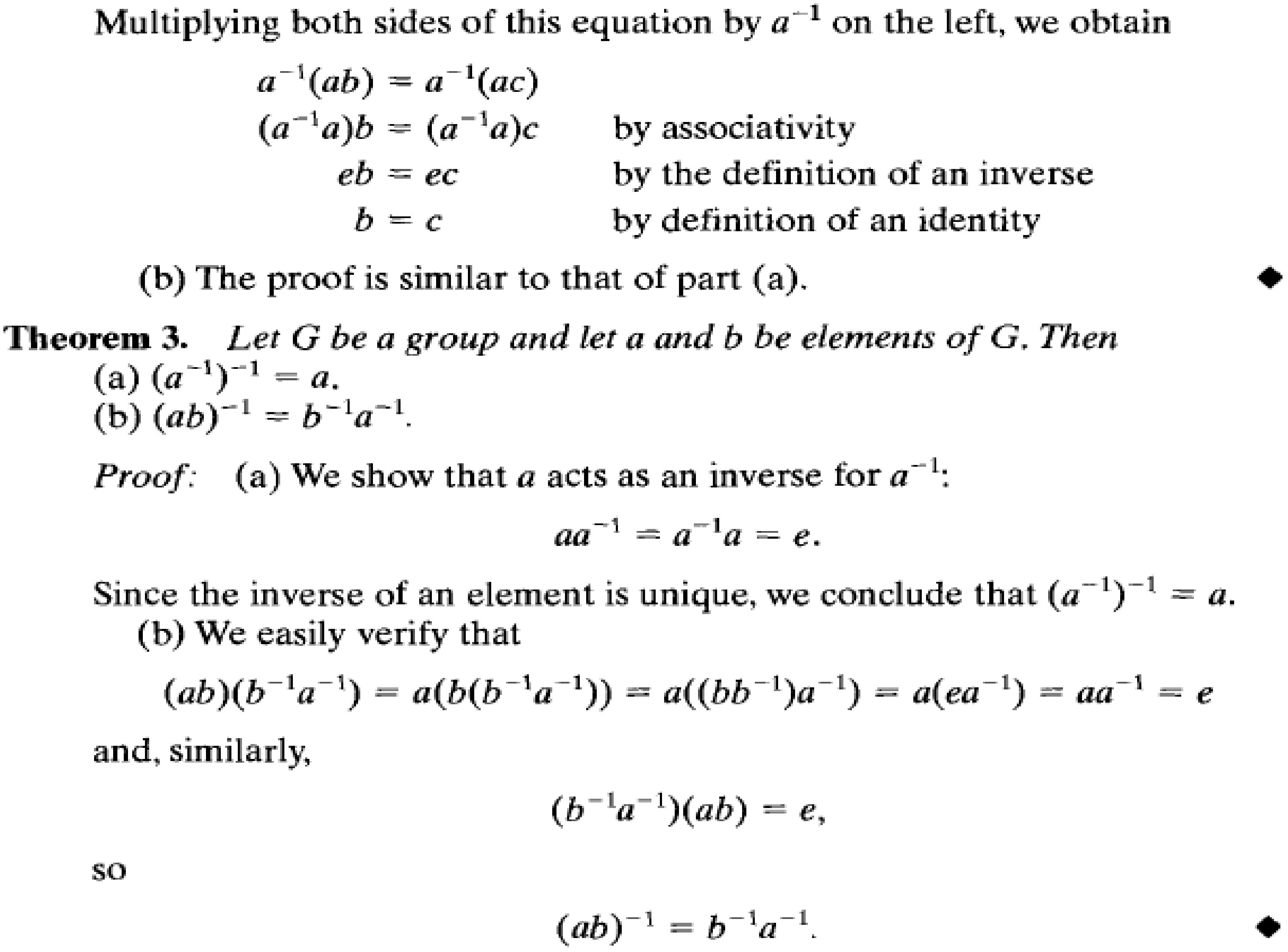
From now on we shall denote the inverse of a by a^{-1}. Thus in a group G we have

$$aa^{-1} = a^{-1}a = e.$$

Theorem 2. *Let G be a group and let a, b, and c be elements of G. Then*
(a) *$ab = ac$ implies that $b = c$* (**left cancellation property**).
(b) *$ba = ca$ implies that $b = c$* (**right cancellation property**).

Proof: (a) Suppose that

$$ab = ac.$$



Multiplying both sides of this equation by a^{-1} on the left, we obtain

$$\begin{aligned} a^{-1}(ab) &= a^{-1}(ac) && \\ (a^{-1}a)b &= (a^{-1}a)c && \text{by associativity} \\ eb &= ec && \text{by the definition of an inverse} \\ b &= c && \text{by definition of an identity} \end{aligned}$$

(b) The proof is similar to that of part (a). ◆

Theorem 3. *Let G be a group and let a and b be elements of G. Then*
(a) $(a^{-1})^{-1} = a$.
(b) $(ab)^{-1} = b^{-1}a^{-1}$.

Proof: (a) We show that a acts as an inverse for a^{-1}:

$$aa^{-1} = a^{-1}a = e.$$

Since the inverse of an element is unique, we conclude that $(a^{-1})^{-1} = a$.
(b) We easily verify that

$$(ab)(b^{-1}a^{-1}) = a(b(b^{-1}a^{-1})) = a((bb^{-1})a^{-1}) = a(ea^{-1}) = aa^{-1} = e$$

and, similarly,

$$(b^{-1}a^{-1})(ab) = e,$$

so

$$(ab)^{-1} = b^{-1}a^{-1}.$$ ◆

Theorem 4. *Let G be a group, and let a and b be elements of G. Then*

(a) *The equation $ax = b$ has a unique solution in G.*

(b) *The equation $ya = b$ has a unique solution in G.*

Proof: (a) The element $x = a^{-1}b$ is a solution of the equation $ax = b$, since

$$a(a^{-1}b) = (aa^{-1})b = eb = b.$$

Suppose now that x_1 and x_2 are two solutions of the equation $ax = b$. Then

$$ax_1 = b \quad \text{and} \quad ax_2 = b.$$

Hence

$$ax_1 = ax_2.$$

Theorem 2 implies that $x_1 = x_2$.

If G is a group that has a finite number of elements, we say that G is a **finite group**, and the **order** of G is the number of elements $|G|$ in G. We shall now determine the multiplication tables of all nonisomorphic groups of orders 1, 2, 3, and 4.

If G is a group of order 1, then $G = \{e\}$, and we have $ee = e$. Now let $G = \{e, a\}$ be a group of order 2. Then we obtain a multiplication table (Table 9.1) where we need to fill in the blank.

Table 9.1

	e	a
e	e	a
a	a	

Example 6. Consider the equilateral triangle shown in Figure 9.3 with vertices 1, 2, and 3. A **symmetry** of the triangle (or of any geometrical figure) is a one-to-one correspondence from the set of points forming the triangle (the geometrical figure) to itself that preserves the distance between adjacent points. Since the triangle is determined by its vertices, a symmetry of the triangle is merely a permutation of the vertices that preserves the distance between adjacent points. Let l_1, l_2, and l_3 be the angle bisectors of the corresponding angles as shown in Figure 9.3, and let O be their point of intersection.

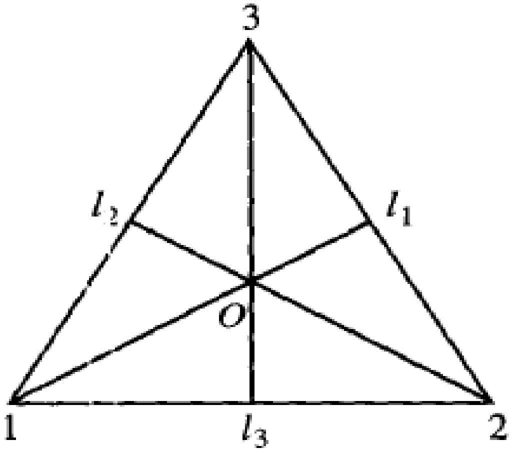


Figure 9.3

We now describe the symmetries of this triangle. First, there is a counterclockwise rotation f_2 of the triangle abou: O through 120°. Then f_2 can be written (see Section 5.3) as the permutation

$$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

We next obtain a counterclockwise rotation f_3 about O through 240°, which can be written as the permutation

$$f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

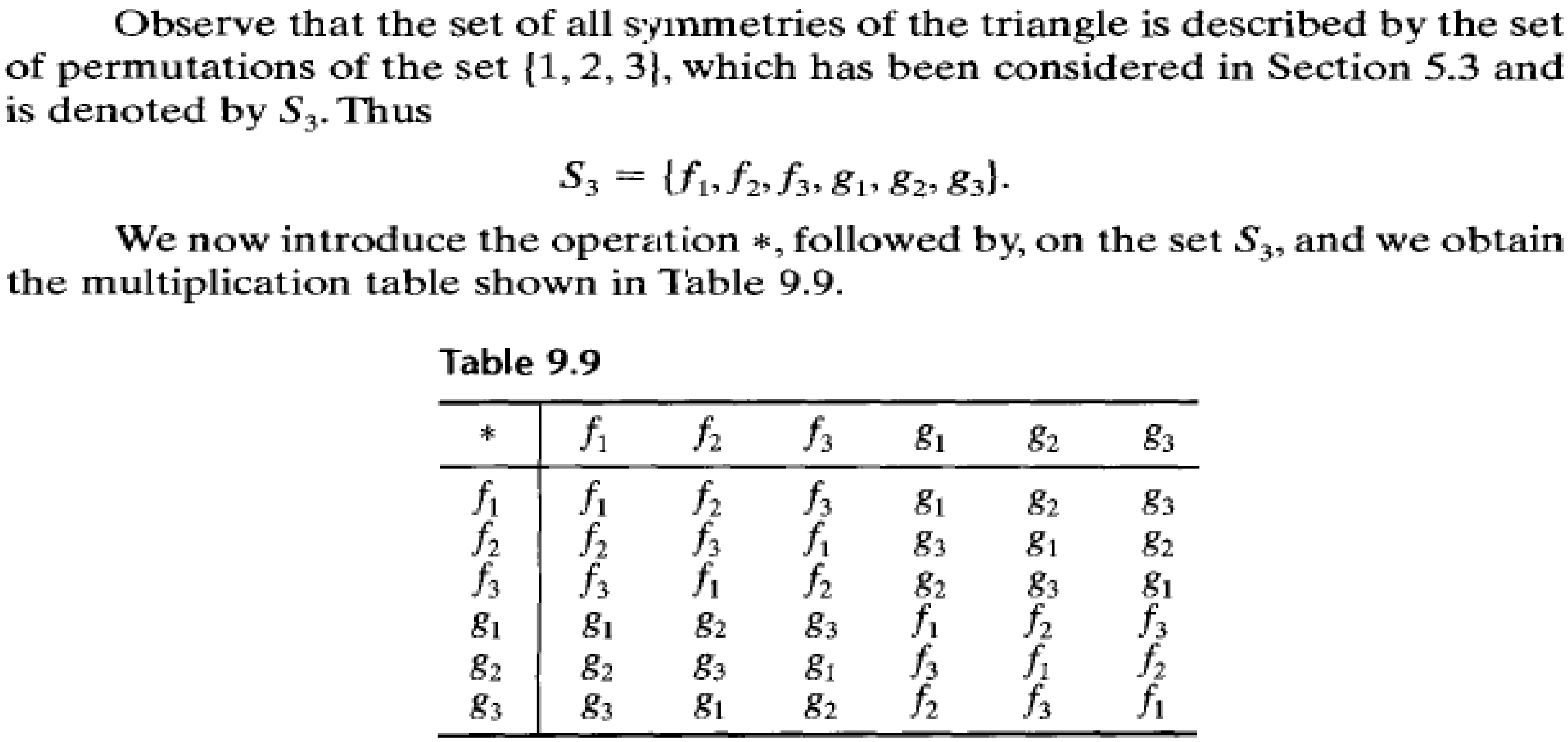
Finally, there is a counterclockwise rotation f_1 about O through 360°, which can be written as the permutation

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}.$$

Of course, f_1 can also be viewed as the result of rotating the triangle about O through 0°.

We may also obtain three additional symmetries of the triangle, g_1, g_2, and g_3, by reflecting about the lines l_1, l_2, and l_3, respectively. We may denote these reflections as the following permutations:

$$g_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \qquad g_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \qquad g_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$



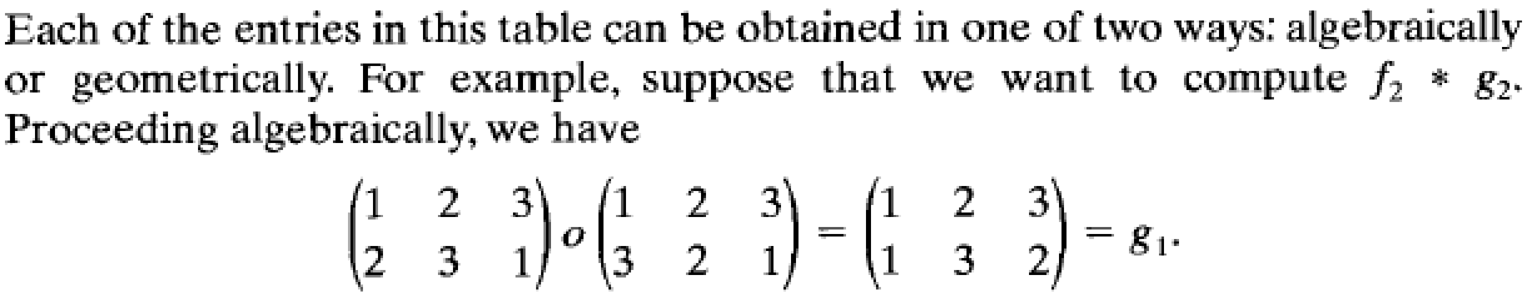
Observe that the set of all symmetries of the triangle is described by the set of permutations of the set {1, 2, 3}, which has been considered in Section 5.3 and is denoted by S_3. Thus

$$S_3 = \{f_1, f_2, f_3, g_1, g_2, g_3\}.$$

We now introduce the operation $*$, followed by, on the set S_3, and we obtain the multiplication table shown in Table 9.9.

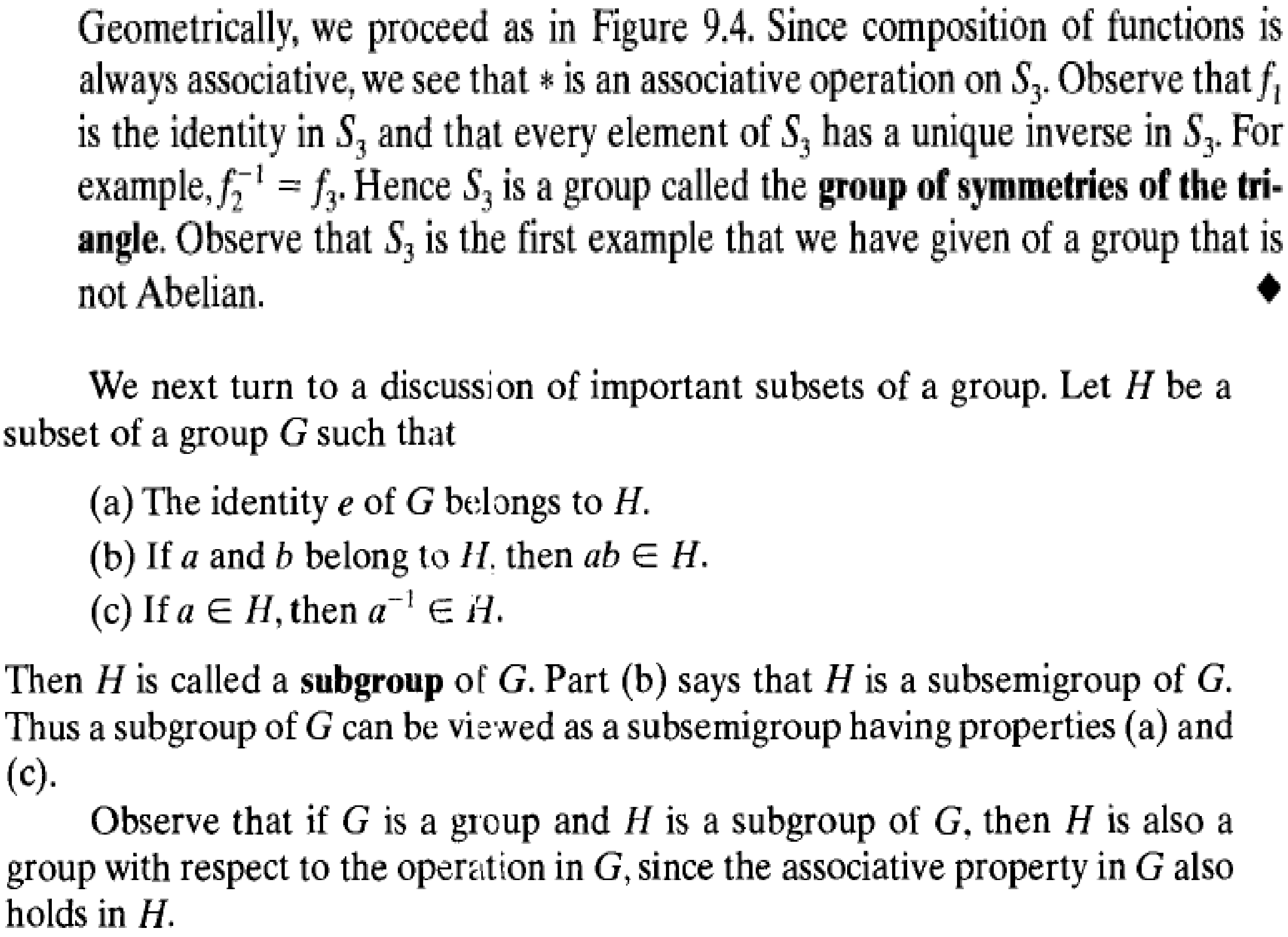
Table 9.9

$*$	f_1	f_2	f_3	g_1	g_2	g_3
f_1	f_1	f_2	f_3	g_1	g_2	g_3
f_2	f_2	f_3	f_1	g_3	g_1	g_2
f_3	f_3	f_1	f_2	g_2	g_3	g_1
g_1	g_1	g_2	g_3	f_1	f_2	f_3
g_2	g_2	g_3	g_1	f_3	f_1	f_2
g_3	g_3	g_1	g_2	f_2	f_3	f_1



Each of the entries in this table can be obtained in one of two ways: algebraically or geometrically. For example, suppose that we want to compute $f_2 * g_2$. Proceeding algebraically, we have

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} o \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = g_1.$$



Geometrically, we proceed as in Figure 9.4. Since composition of functions is always associative, we see that $*$ is an associative operation on S_3. Observe that f_1 is the identity in S_3 and that every element of S_3 has a unique inverse in S_3. For example, $f_2^{-1} = f_3$. Hence S_3 is a group called the **group of symmetries of the triangle**. Observe that S_3 is the first example that we have given of a group that is not Abelian. ◆

We next turn to a discussion of important subsets of a group. Let H be a subset of a group G such that

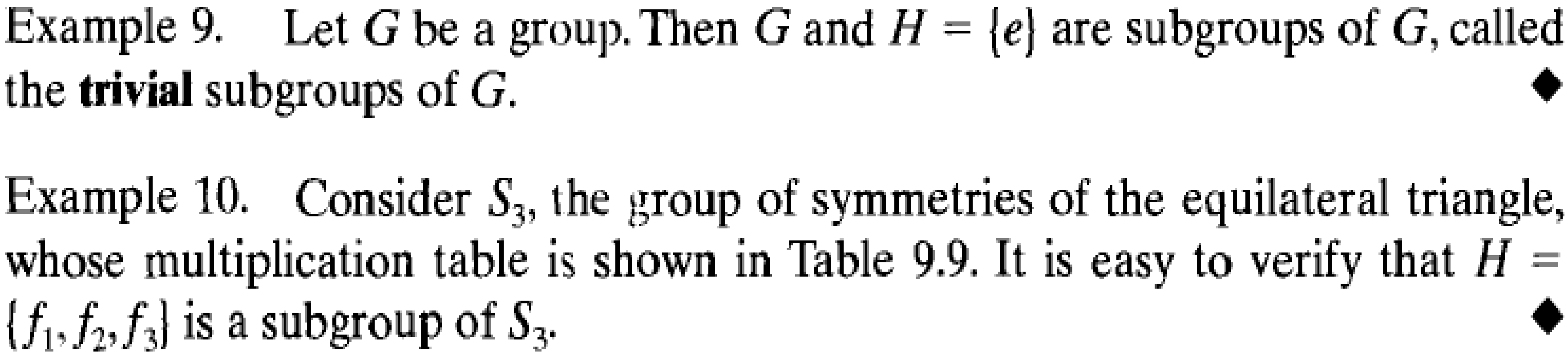
(a) The identity e of G belongs to H.

(b) If a and b belong to H, then $ab \in H$.

(c) If $a \in H$, then $a^{-1} \in H$.

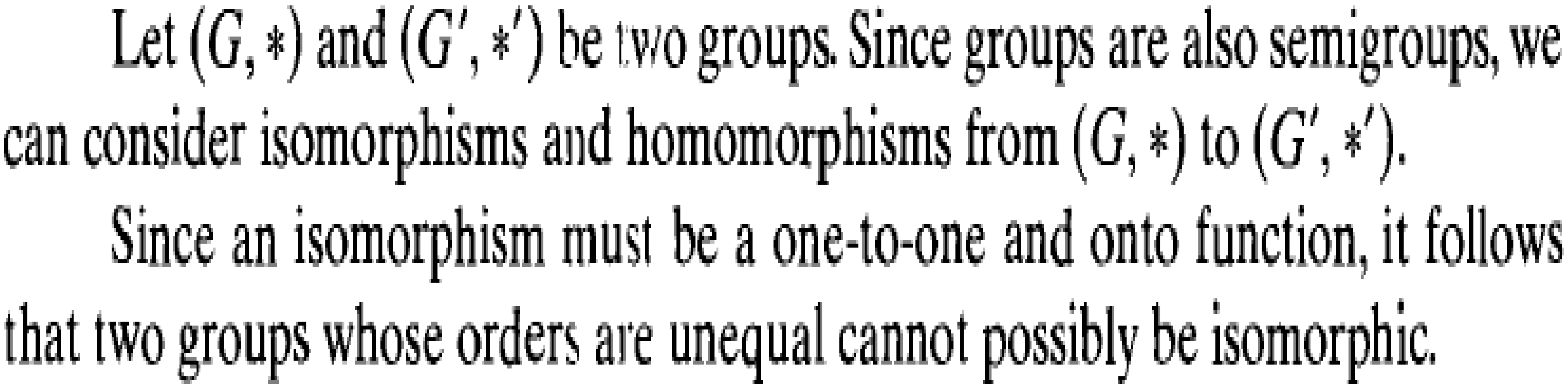
Then H is called a **subgroup** of G. Part (b) says that H is a subsemigroup of G. Thus a subgroup of G can be viewed as a subsemigroup having properties (a) and (c).

Observe that if G is a group and H is a subgroup of G, then H is also a group with respect to the operation in G, since the associative property in G also holds in H.



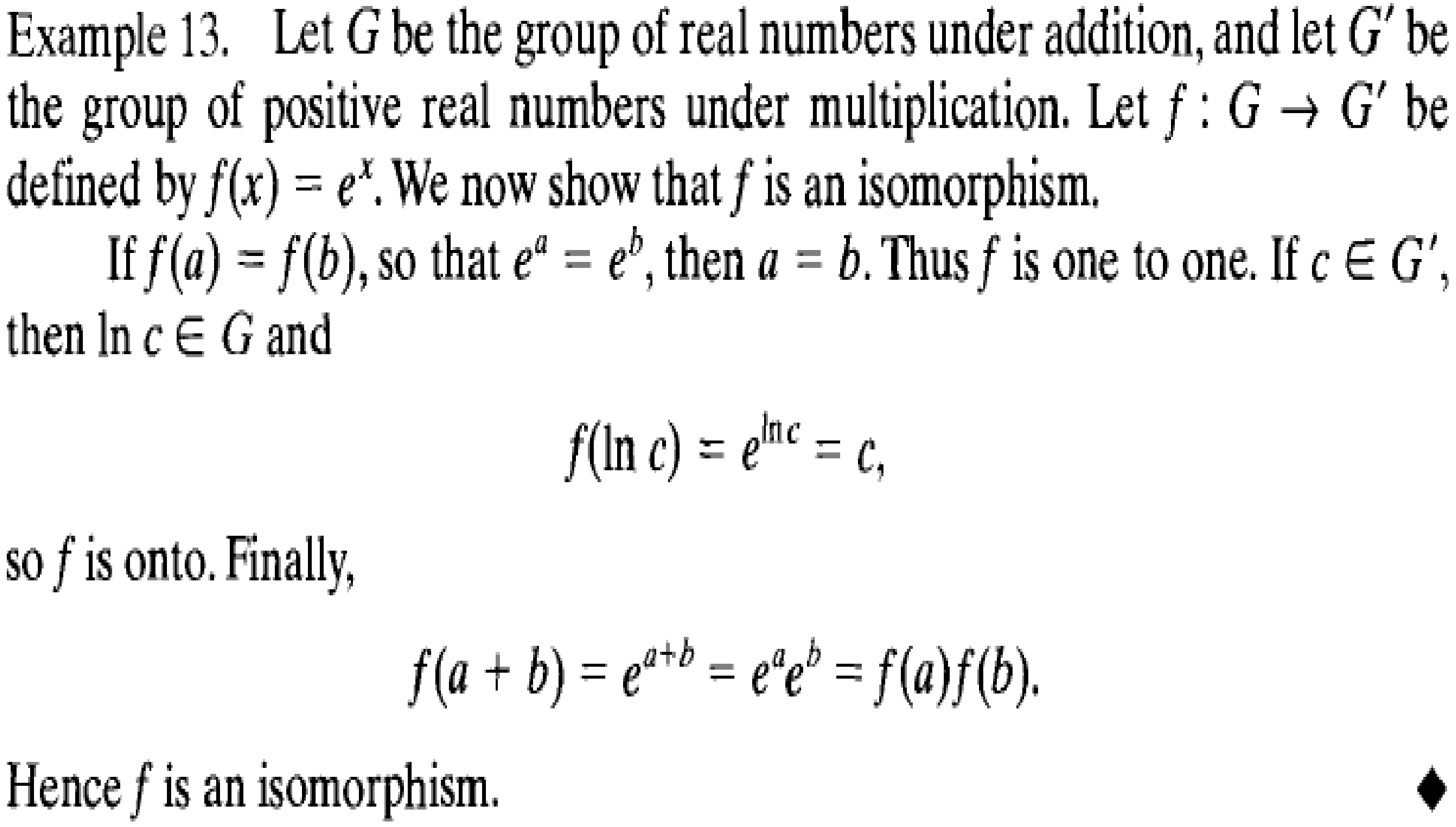
Example 9. Let G be a group. Then G and $H = \{e\}$ are subgroups of G, called the **trivial** subgroups of G. ◆

Example 10. Consider S_3, the group of symmetries of the equilateral triangle, whose multiplication table is shown in Table 9.9. It is easy to verify that $H = \{f_1, f_2, f_3\}$ is a subgroup of S_3. ◆



Let $(G, *)$ and $(G', *')$ be two groups. Since groups are also semigroups, we can consider isomorphisms and homomorphisms from $(G, *)$ to $(G', *')$.

Since an isomorphism must be a one-to-one and onto function, it follows that two groups whose orders are unequal cannot possibly be isomorphic.



Example 13. Let G be the group of real numbers under addition, and let G' be the group of positive real numbers under multiplication. Let $f : G \to G'$ be defined by $f(x) = e^x$. We now show that f is an isomorphism.

If $f(a) = f(b)$, so that $e^a = e^b$, then $a = b$. Thus f is one to one. If $c \in G'$, then $\ln c \in G$ and

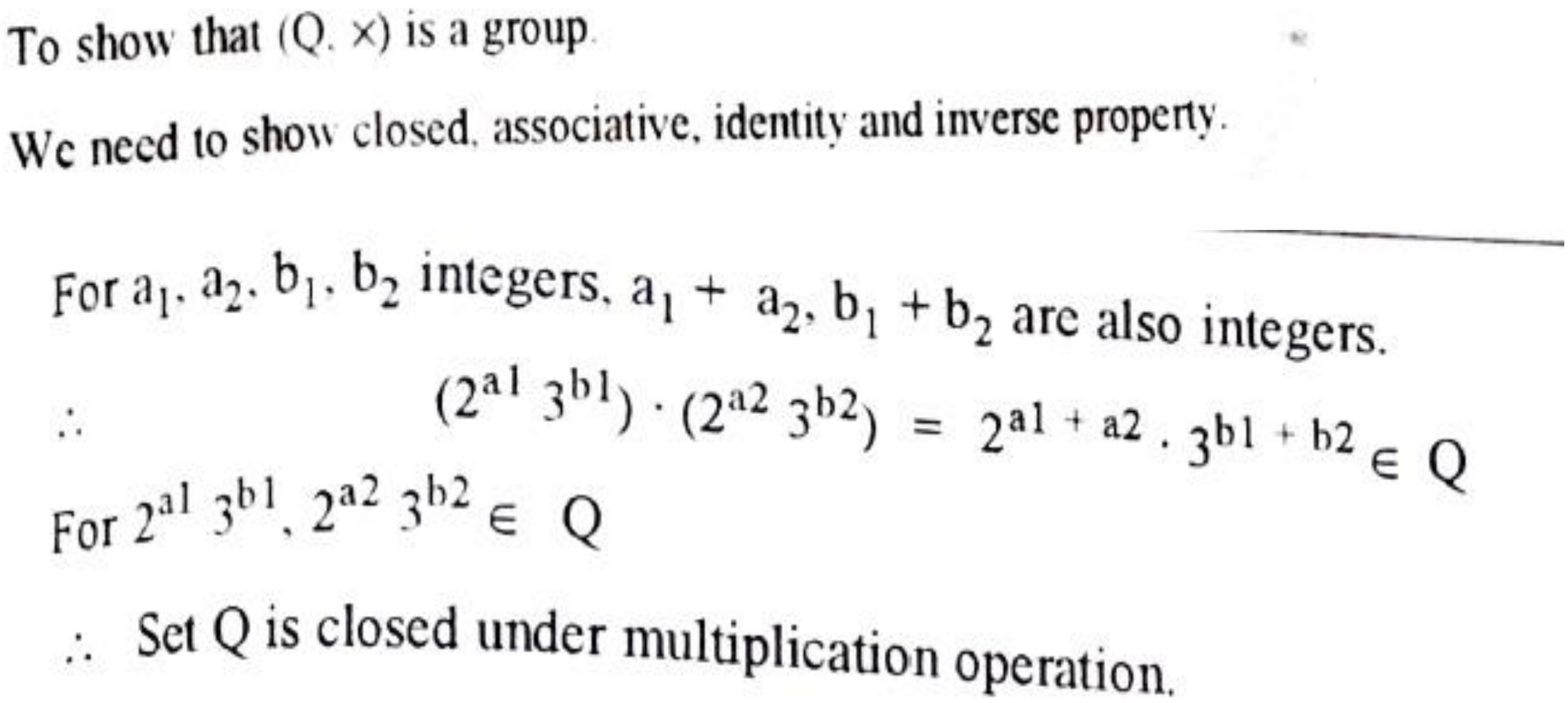
$$f(\ln c) = e^{\ln c} = c,$$

so f is onto. Finally,

$$f(a + b) = e^{a+b} = e^a e^b = f(a)f(b).$$

Hence f is an isomorphism. ♦

Example: Let Q be the set of positive rational numbers which can be expressed as $2^a 3^b$, where a and b are integers. Prove that algebraic structure (Q, ·) is a group. Where · is multiplication operation.



To show that (Q. ×) is a group.

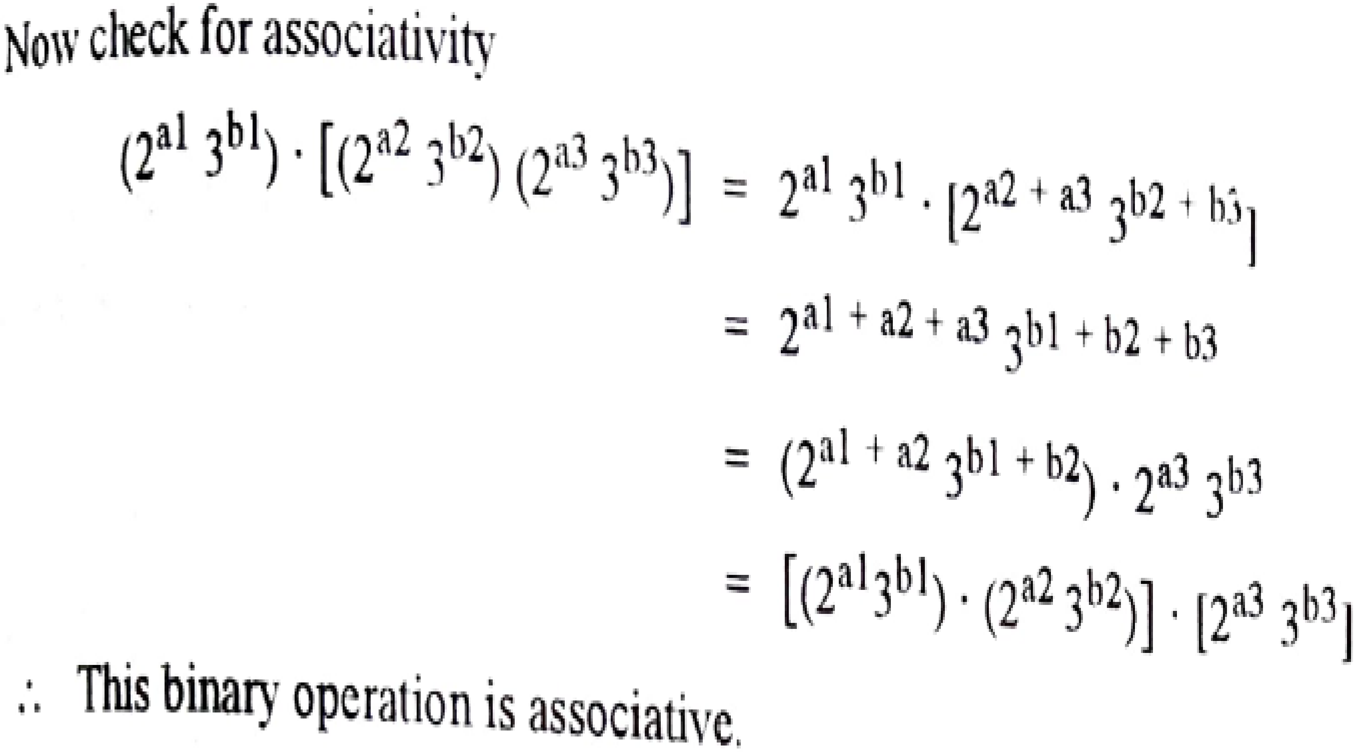
We need to show closed, associative, identity and inverse property.

For a_1. a_2. b_1. b_2 integers, $a_1 + a_2$, $b_1 + b_2$ are also integers.

$$\therefore \quad (2^{a1} 3^{b1}) \cdot (2^{a2} 3^{b2}) = 2^{a1 + a2} . 3^{b1 + b2} \in Q$$

For $2^{a1} 3^{b1}, 2^{a2} 3^{b2} \in Q$

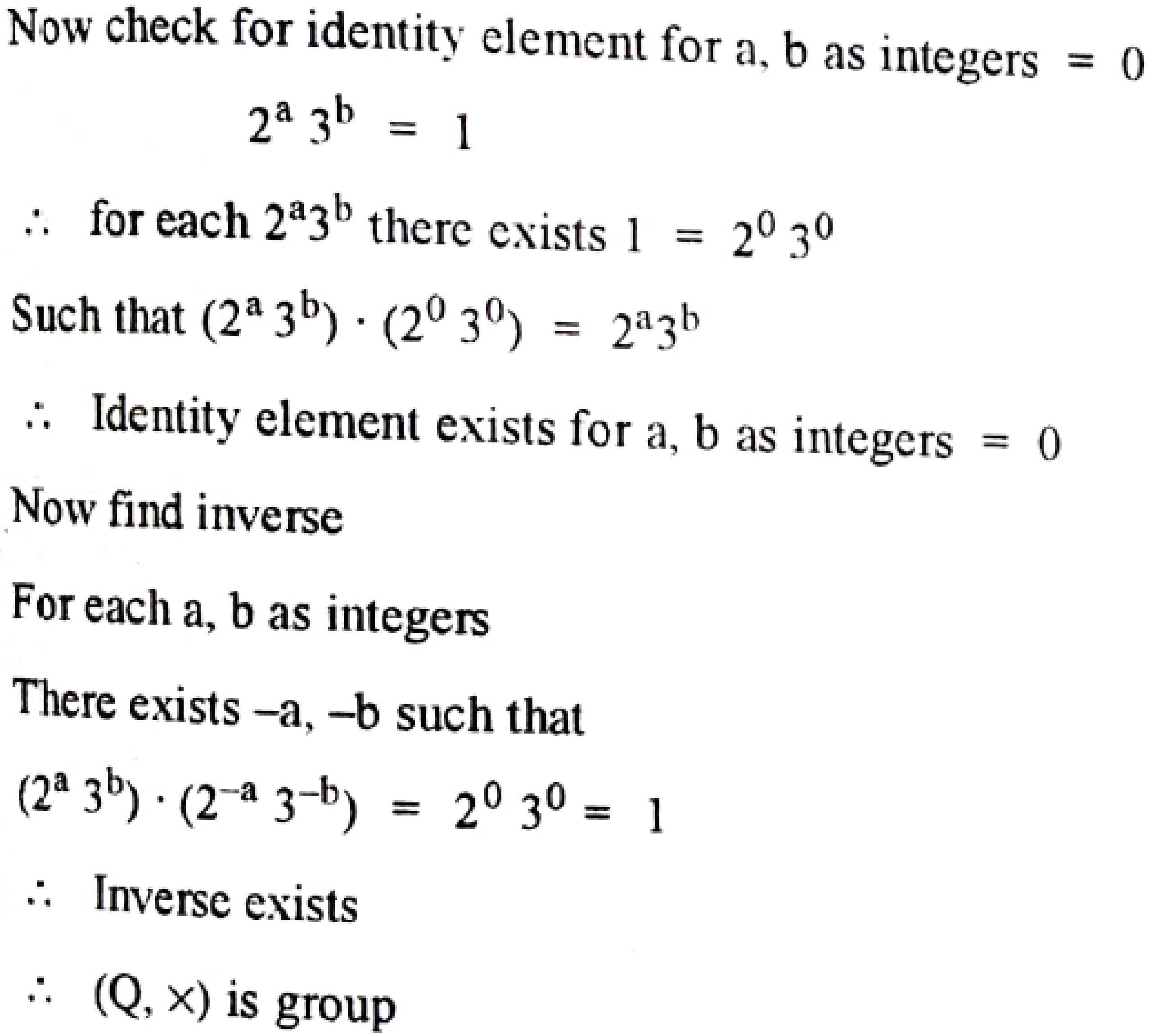
∴ Set Q is closed under multiplication operation.



Now check for associativity

$$
\begin{aligned}
(2^{a1}\,3^{b1})\cdot[(2^{a2}\,3^{b2})\,(2^{a3}\,3^{b3})] &= 2^{a1}\,3^{b1}\cdot[2^{a2+a3}\,3^{b2+b3}] \\
&= 2^{a1+a2+a3}\,3^{b1+b2+b3} \\
&= (2^{a1+a2}\,3^{b1+b2})\cdot 2^{a3}\,3^{b3} \\
&= [(2^{a1}3^{b1})\cdot(2^{a2}\,3^{b2})]\cdot[2^{a3}\,3^{b3}]
\end{aligned}
$$

$\therefore$ This binary operation is associative.



Now check for identity element for a, b as integers = 0

$$2^a 3^b = 1$$

$\therefore$ for each $2^a 3^b$ there exists $1 = 2^0 3^0$

Such that $(2^a 3^b) \cdot (2^0 3^0) = 2^a 3^b$

$\therefore$ Identity element exists for a, b as integers = 0

Now find inverse

For each a, b as integers

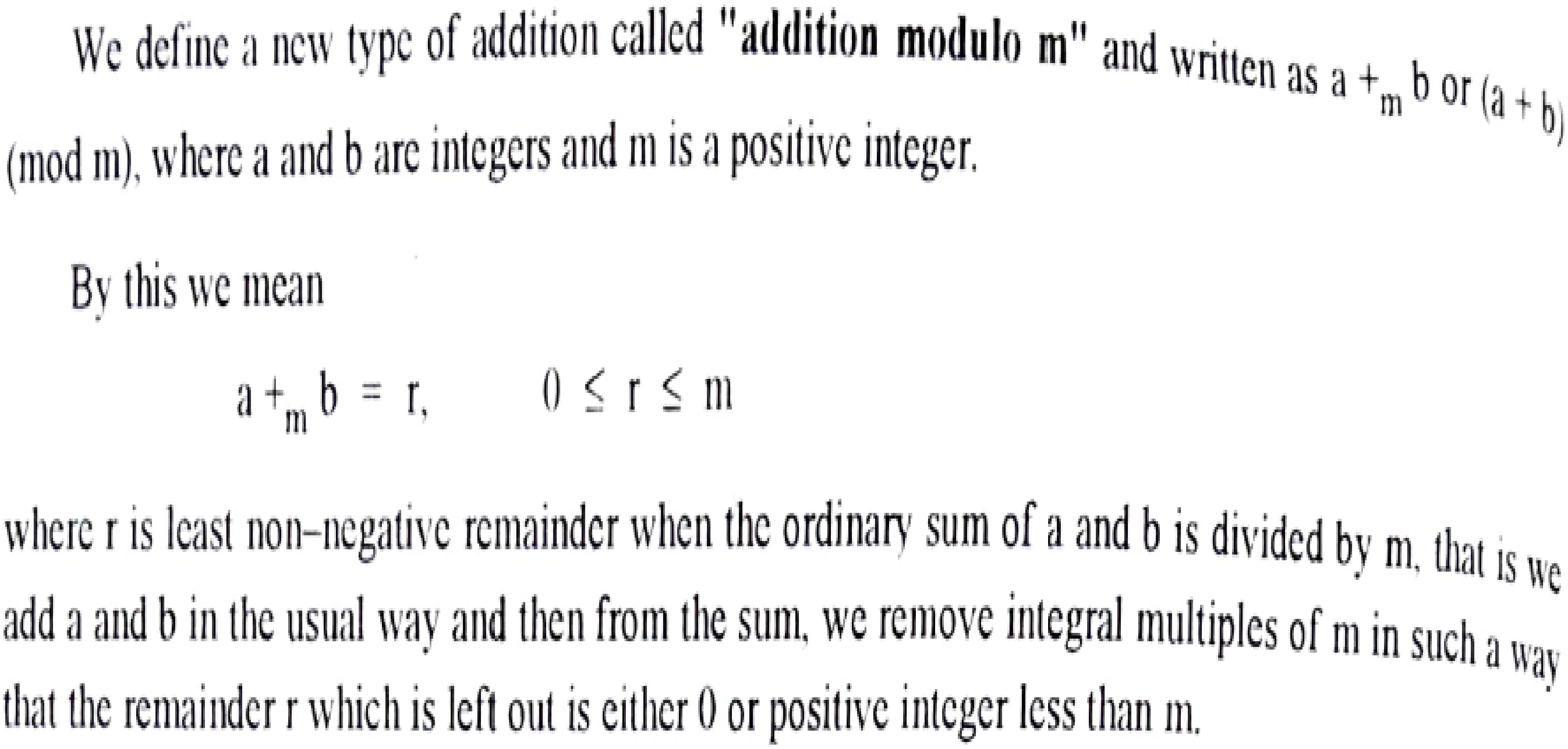
There exists –a, –b such that

$(2^a 3^b) \cdot (2^{-a} 3^{-b}) = 2^0 3^0 = 1$

$\therefore$ Inverse exists

$\therefore$ $(Q, \times)$ is group

Additive Modulo M



We define a new type of addition called "**addition modulo m**" and written as $a +_m b$ or $(a + b) \pmod{m}$, where a and b are integers and m is a positive integer.

By this we mean

$$a +_m b = r, \qquad 0 \leq r \leq m$$

where r is least non–negative remainder when the ordinary sum of a and b is divided by m, that is we add a and b in the usual way and then from the sum, we remove integral multiples of m in such a way that the remainder r which is left out is either 0 or positive integer less than m.

For e.g.

(i) $14 +_6 8 = 22 \% 6 = 4$

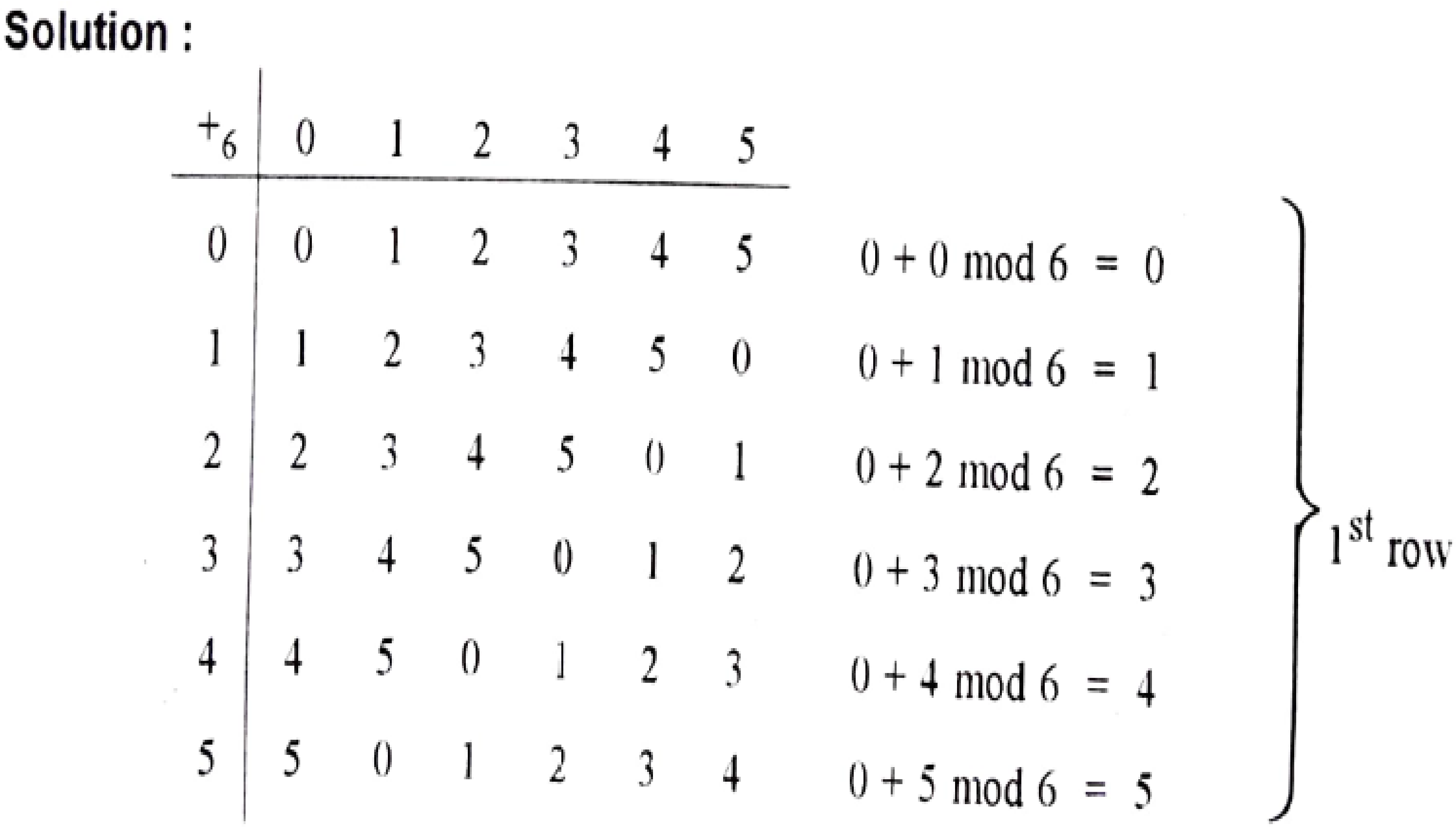
(ii) $5 +_6 3 = 8 \% 6 = 2$

(iii) $9 +_{12} 3 = 12 \% 12 = 0$

(iv) $3 +_3 1 = 4 \% 3 = 1$

(v) $-23 +_3 3 = -20 \% 3 = (-3) \times 7 + 1 = 1$

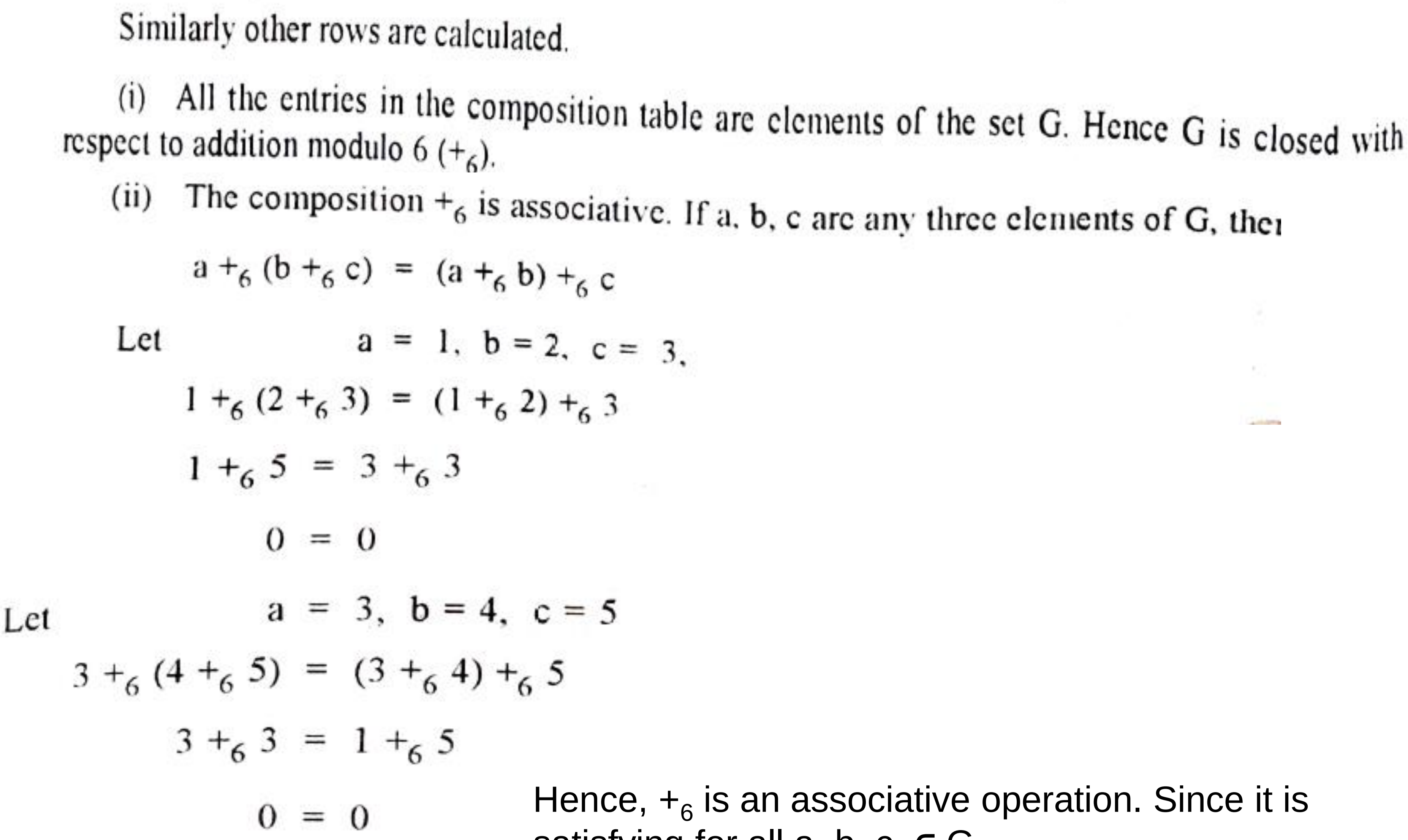
Example: Prove that the set G= {0, 1, 2, 3, 4, 5} is an Abelian group of order 6 with respect to addition modulo 6.



Solution :

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$$\left.\begin{aligned} 0 + 0 \bmod 6 &= 0 \\ 0 + 1 \bmod 6 &= 1 \\ 0 + 2 \bmod 6 &= 2 \\ 0 + 3 \bmod 6 &= 3 \\ 0 + 4 \bmod 6 &= 4 \\ 0 + 5 \bmod 6 &= 5 \end{aligned}\right\} 1^{st} \text{ row}$$



Similarly other rows are calculated.

(i) All the entries in the composition table are elements of the set G. Hence G is closed with respect to addition modulo 6 ($+_6$).

(ii) The composition $+_6$ is associative. If a, b, c are any three elements of G, thei

$$a +_6 (b +_6 c) = (a +_6 b) +_6 c$$

Let $a = 1,\ b = 2,\ c = 3,$

$$1 +_6 (2 +_6 3) = (1 +_6 2) +_6 3$$

$$1 +_6 5 = 3 +_6 3$$

$$0 = 0$$

Let $a = 3,\ b = 4,\ c = 5$

$$3 +_6 (4 +_6 5) = (3 +_6 4) +_6 5$$

$$3 +_6 3 = 1 +_6 5$$

$$0 = 0$$

Hence, $+_6$ is an associative operation. Since it is satisfying for all a, b, c, ∈ G.

(iii) If a is any element of G, then from the composition table we see that

$$0 +_6 a = a = a +_6 0 = 0$$

that is, $0 +_6 0 = 0 +_6 0 = 0$

$$0 +_6 1 = 1 +_6 0 = 1$$

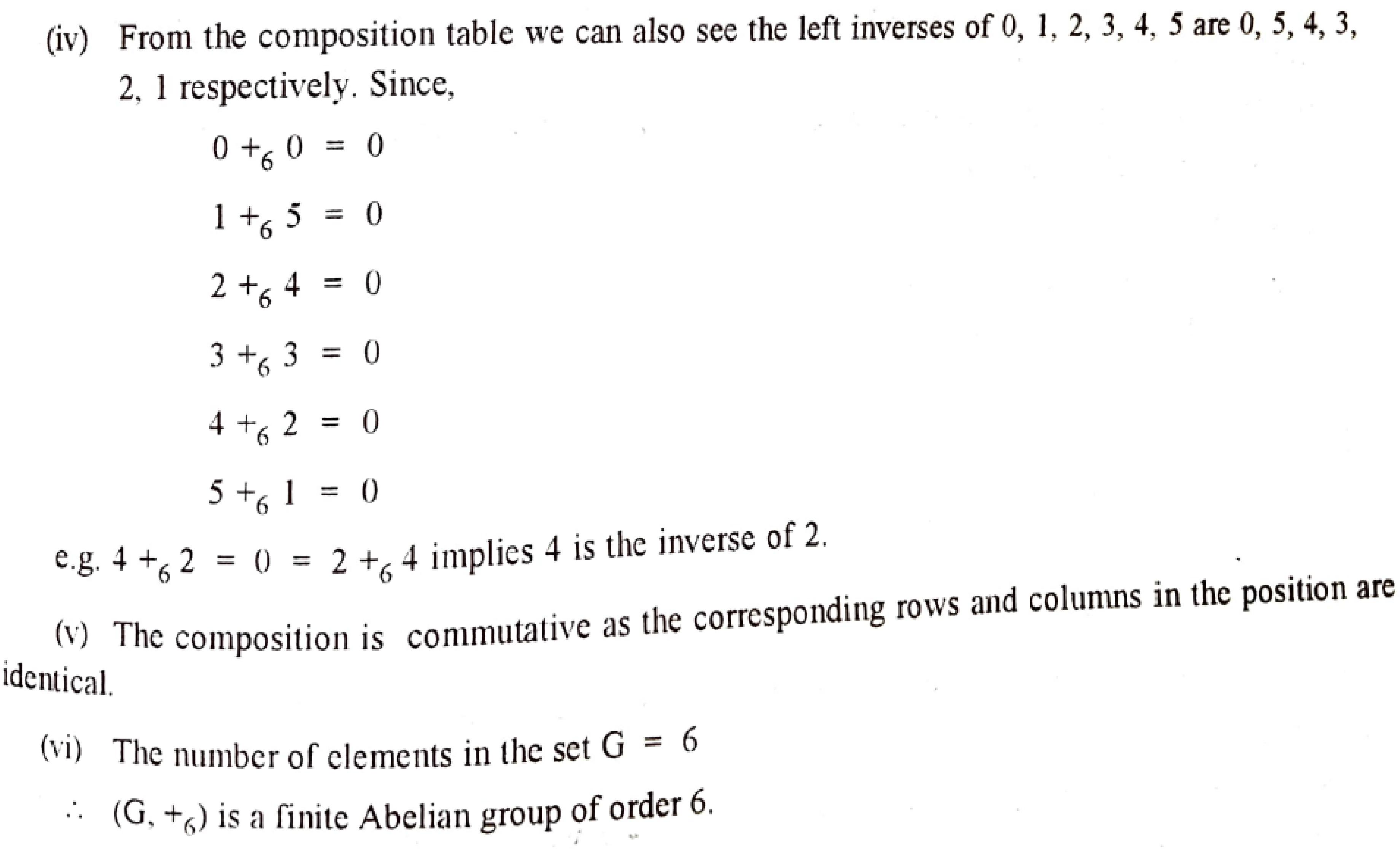
$$0 +_6 2 = 2 +_6 0 = 2$$

$$0 +_6 3 = 3 +_6 0 = 3$$

$$0 +_6 4 = 4 +_6 0 = 4$$

$$0 +_6 5 = 5 +_6 0 = 5$$

$\therefore$ 0 is identity element.



(iv) From the composition table we can also see the left inverses of 0, 1, 2, 3, 4, 5 are 0, 5, 4, 3, 2, 1 respectively. Since,

$$0 +_6 0 = 0$$

$$1 +_6 5 = 0$$

$$2 +_6 4 = 0$$

$$3 +_6 3 = 0$$

$$4 +_6 2 = 0$$

$$5 +_6 1 = 0$$

e.g. $4 +_6 2 = 0 = 2 +_6 4$ implies 4 is the inverse of 2.

(v) The composition is commutative as the corresponding rows and columns in the position are identical.

(vi) The number of elements in the set $G = 6$

$\therefore$ $(G, +_6)$ is a finite Abelian group of order 6.

Multiplication Modulo P

A new type of multiplication known as "multiplication modulo P" and written as a X_P b where a and b are any integers and p is fixed positive integer is defined as:

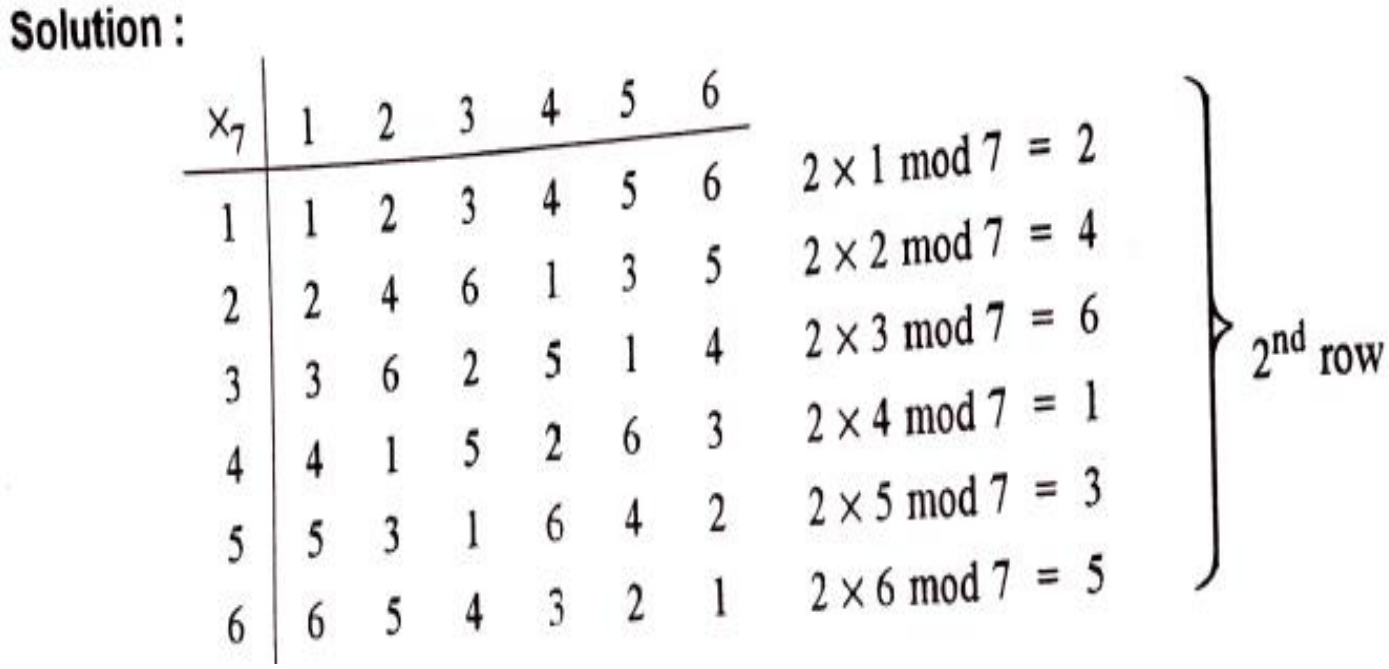
$$a \times_p b = r$$

, $0 \leq r < p$ where, r is the least non-negative remainder when ab (ordinary product of a and b) divided by p.

e.g. (i) $8 \times_5 3 = 24 \bmod 5 = 4$

(ii) $4 \times_7 2 = 8 \bmod 7 = 1$

Example: Prove that the set G= {1, 2, 3, 4, 5, 6} is an Abelian group of order 6 with respect to multiplication modulo 7.



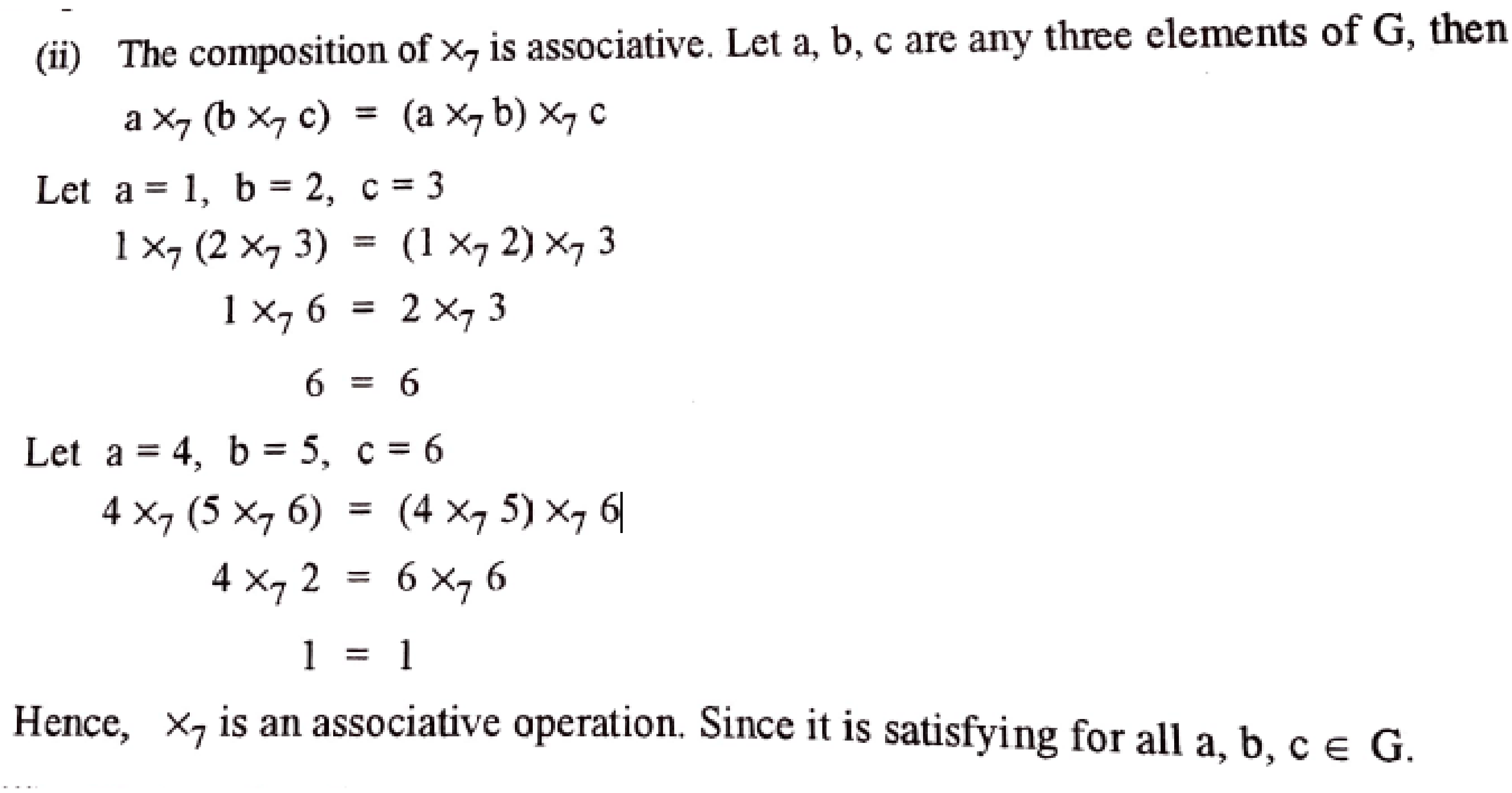
Solution :

$\times_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

$$\left.\begin{aligned} 2 \times 1 \bmod 7 &= 2 \\ 2 \times 2 \bmod 7 &= 4 \\ 2 \times 3 \bmod 7 &= 6 \\ 2 \times 4 \bmod 7 &= 1 \\ 2 \times 5 \bmod 7 &= 3 \\ 2 \times 6 \bmod 7 &= 5 \end{aligned}\right\} 2^{nd} \text{ row}$$

Similarly row 1, row 3, row 4, row 5, and row 6 are calculated.

(i) All the entries in the composition table are elements of G. Hence G is closed under multiplication modulo 7 (X_7)



(ii) The composition of $\times_7$ is associative. Let a, b, c are any three elements of G, then

$$a \times_7 (b \times_7 c) = (a \times_7 b) \times_7 c$$

Let $a = 1$, $b = 2$, $c = 3$

$$1 \times_7 (2 \times_7 3) = (1 \times_7 2) \times_7 3$$

$$1 \times_7 6 = 2 \times_7 3$$

$$6 = 6$$

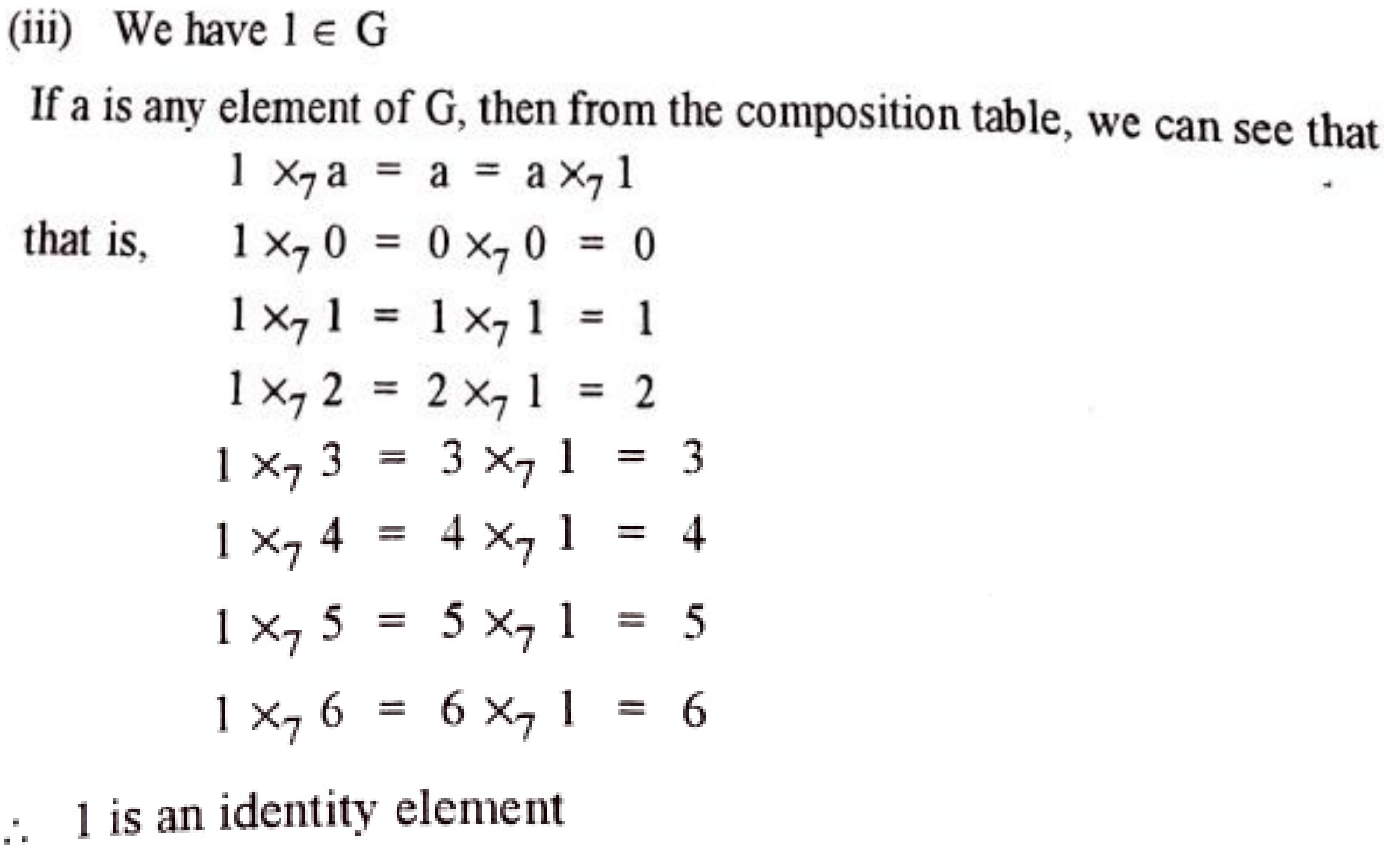
Let $a = 4$, $b = 5$, $c = 6$

$$4 \times_7 (5 \times_7 6) = (4 \times_7 5) \times_7 6$$

$$4 \times_7 2 = 6 \times_7 6$$

$$1 = 1$$

Hence, $\times_7$ is an associative operation. Since it is satisfying for all a, b, c $\in$ G.



(iii) We have $1 \in G$

If a is any element of G, then from the composition table, we can see that

$$1 \times_7 a = a = a \times_7 1$$

that is,

$$1 \times_7 0 = 0 \times_7 0 = 0$$

$$1 \times_7 1 = 1 \times_7 1 = 1$$

$$1 \times_7 2 = 2 \times_7 1 = 2$$

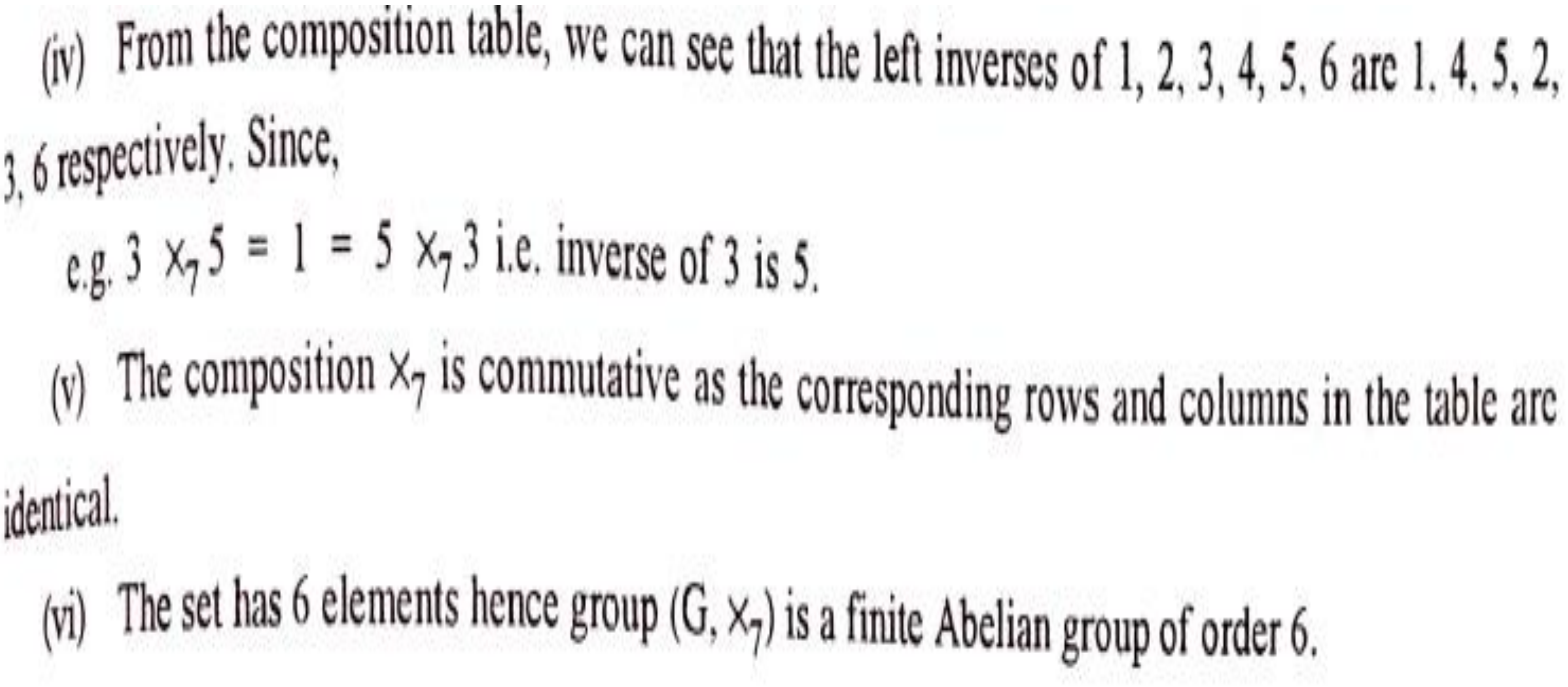
$$1 \times_7 3 = 3 \times_7 1 = 3$$

$$1 \times_7 4 = 4 \times_7 1 = 4$$

$$1 \times_7 5 = 5 \times_7 1 = 5$$

$$1 \times_7 6 = 6 \times_7 1 = 6$$

$\therefore$ 1 is an identity element



(iv) From the composition table, we can see that the left inverses of 1, 2, 3, 4, 5. 6 arc 1. 4. 5, 2, 3, 6 respectively. Since,

e.g. 3 $\times_7$ 5 = 1 = 5 $\times_7$ 3 i.e. inverse of 3 is 5.

(v) The composition $\times_7$ is commutative as the corresponding rows and columns in the table arc identical.

(vi) The set has 6 elements hence group (G, $\times_7$) is a finite Abelian group of order 6.

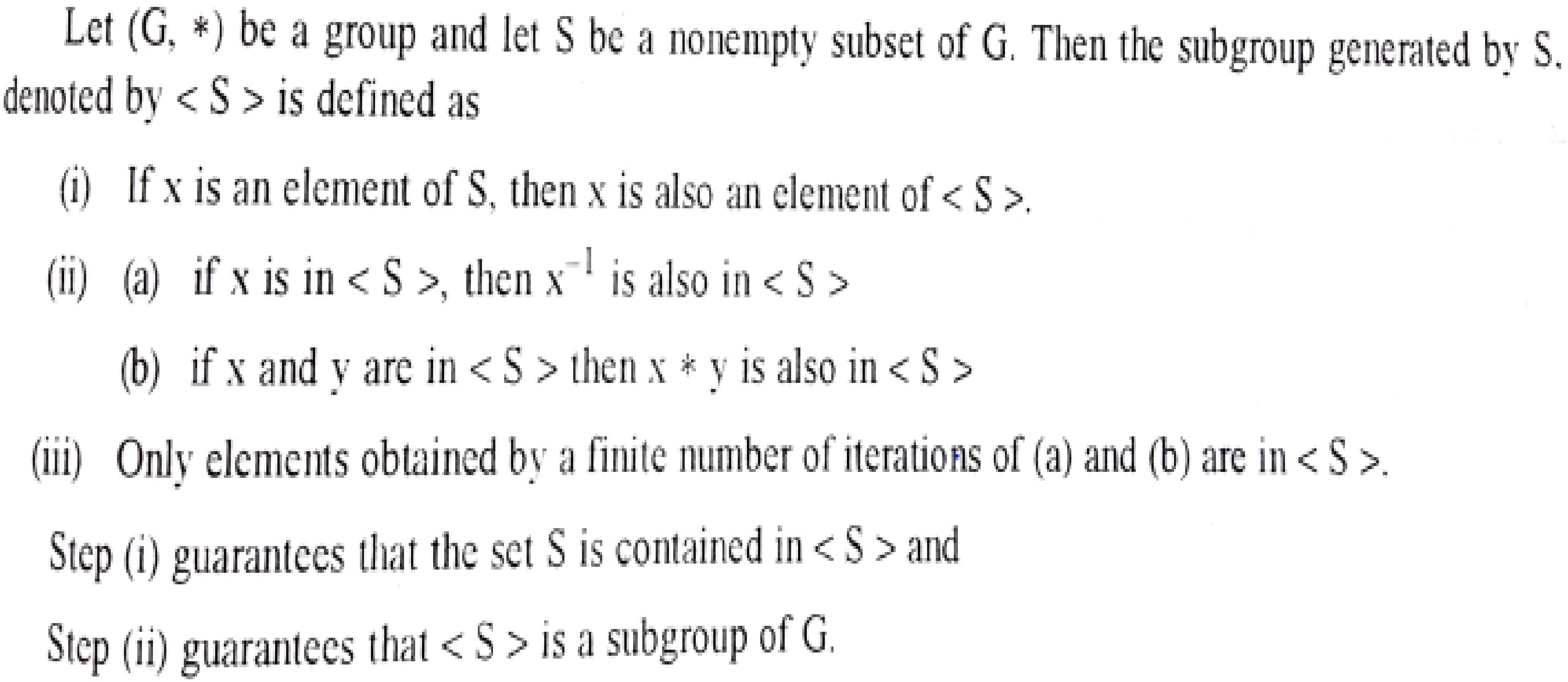
Cyclic Groups

A group (G, *) is said to be a cyclic group if there exists an element $a \in G$ such that every element can be G can be written as some power of a, viz a^k, for some integer k. By a^k, we mean a * a* a.. a (k times). We then say that G is generated by a or a is a generator of G.

A cyclic group is Abelian, since for any two elements $a^r, a^s \in G$,

$$\mathbf{a^r * a^s = a^{r+s} = a* = a^s * a^r}$$

Generation of Subgroups



Let (G, $*$) be a group and let S be a nonempty subset of G. Then the subgroup generated by S, denoted by $< S >$ is defined as

(i) If x is an element of S, then x is also an element of $< S >$.

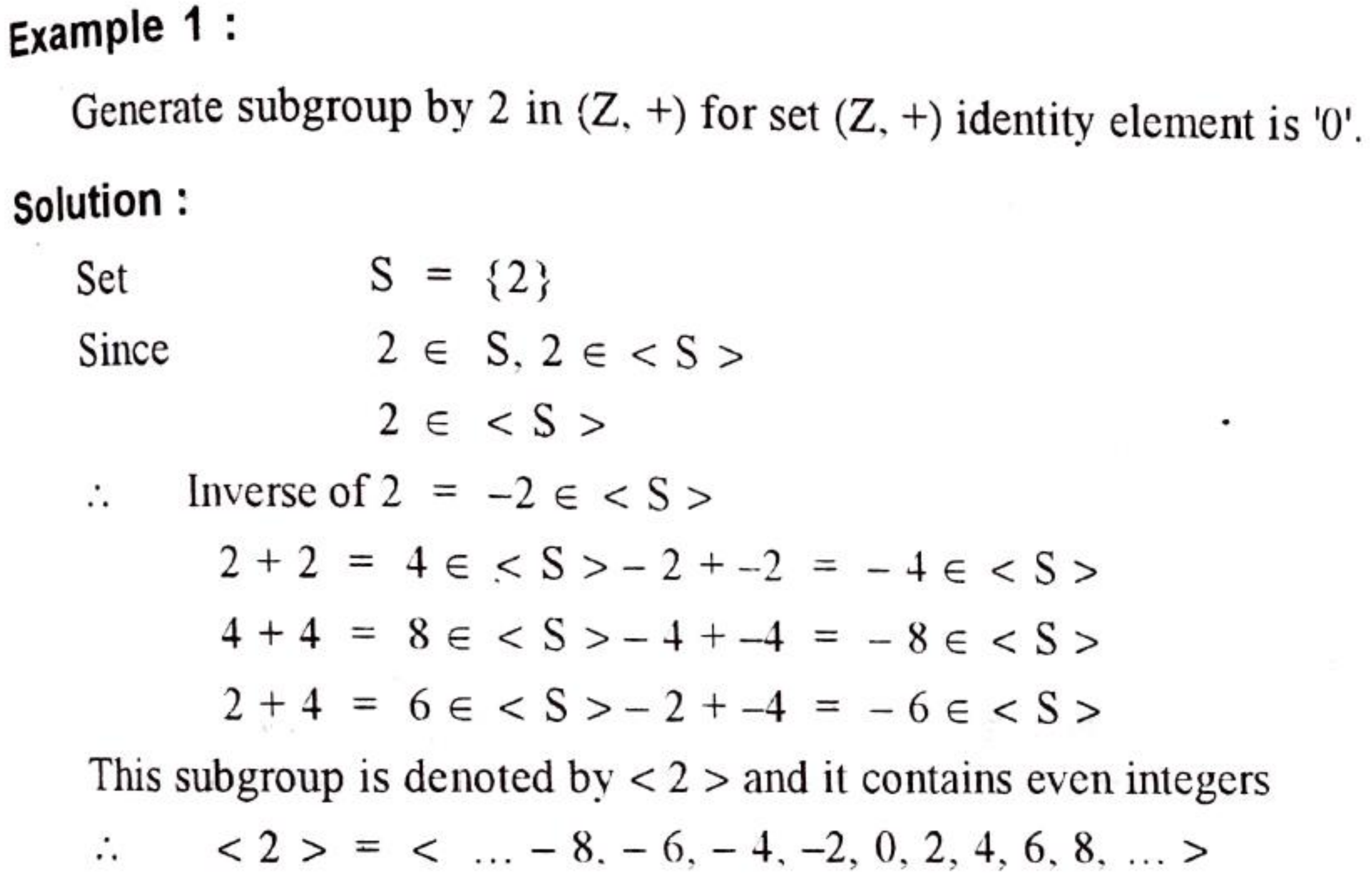
(ii) (a) if x is in $< S >$, then x^{-1} is also in $< S >$

(b) if x and y are in $< S >$ then $x * y$ is also in $< S >$

(iii) Only elements obtained by a finite number of iterations of (a) and (b) are in $< S >$.

Step (i) guarantees that the set S is contained in $< S >$ and

Step (ii) guarantees that $< S >$ is a subgroup of G.



Example 1 :

Generate subgroup by 2 in (Z, +) for set (Z, +) identity element is '0'.

Solution :

Set $S = \{2\}$

Since $2 \in S, 2 \in < S >$

$2 \in < S >$

$\therefore$ Inverse of 2 $= -2 \in < S >$

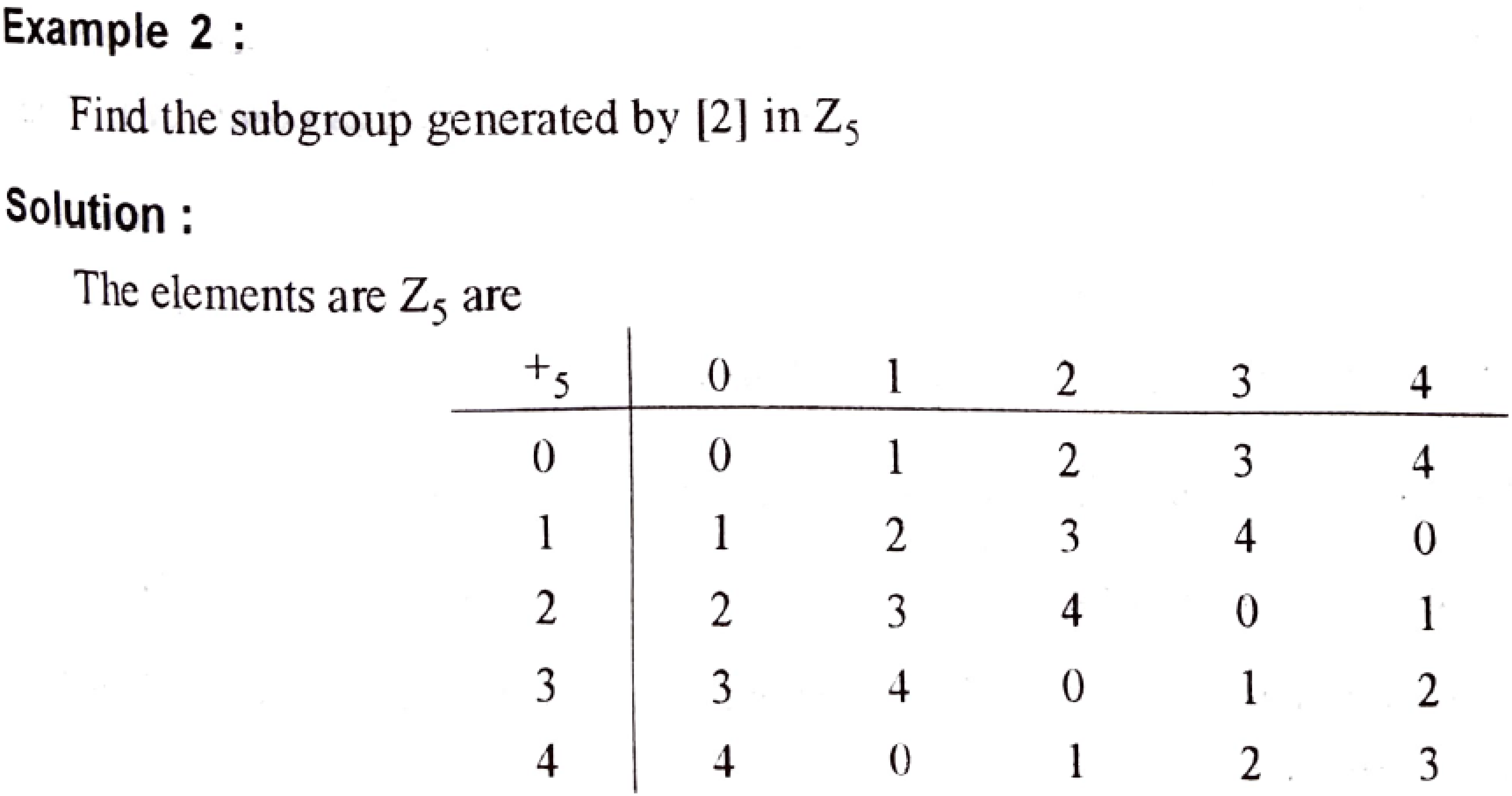
$$2 + 2 = 4 \in < S > - 2 + -2 = -4 \in < S >$$

$$4 + 4 = 8 \in < S > - 4 + -4 = -8 \in < S >$$

$$2 + 4 = 6 \in < S > - 2 + -4 = -6 \in < S >$$

This subgroup is denoted by < 2 > and it contains even integers

$\therefore$ $< 2 > = < \ldots -8, -6, -4, -2, 0, 2, 4, 6, 8, \ldots >$



Example 2 :

Find the subgroup generated by [2] in Z_5

Solution :

The elements are Z_5 are

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

The inverse of [2] in Z_5 is [3]. It must be in $< [2] >$

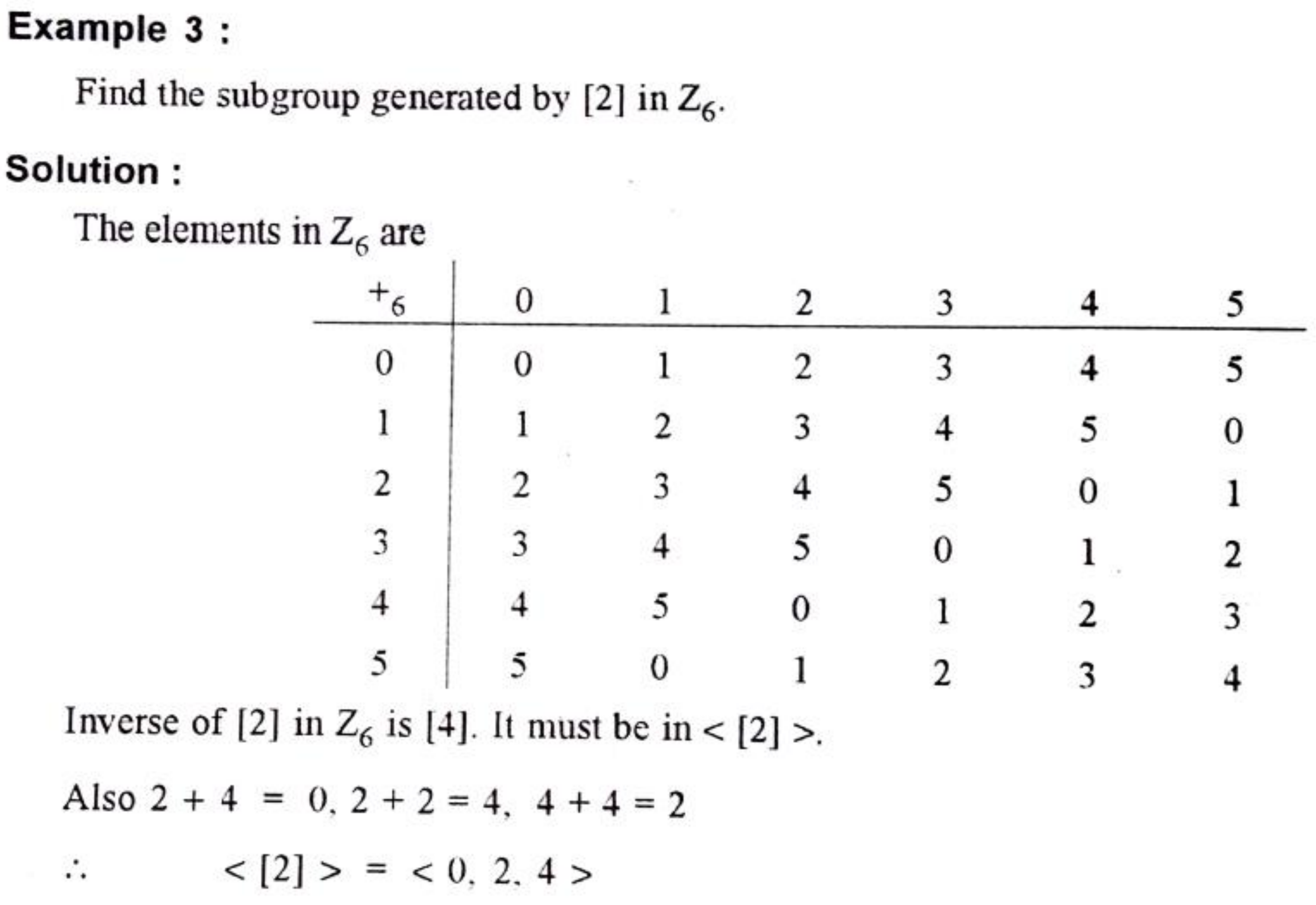
Also $\quad 2 + 3 = 0,$

$2 + 2 = 4,$

$3 + 3 = 1$ must be in $< 2 >$

Thus all the elements of Z_5 are in $< [\ 2\ ] >$.

$\therefore \quad < [2] > \ = \ < 0, 1, 2, 3, 4 >$



Example 3 :

Find the subgroup generated by [2] in Z_6.

Solution :

The elements in Z_6 are

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

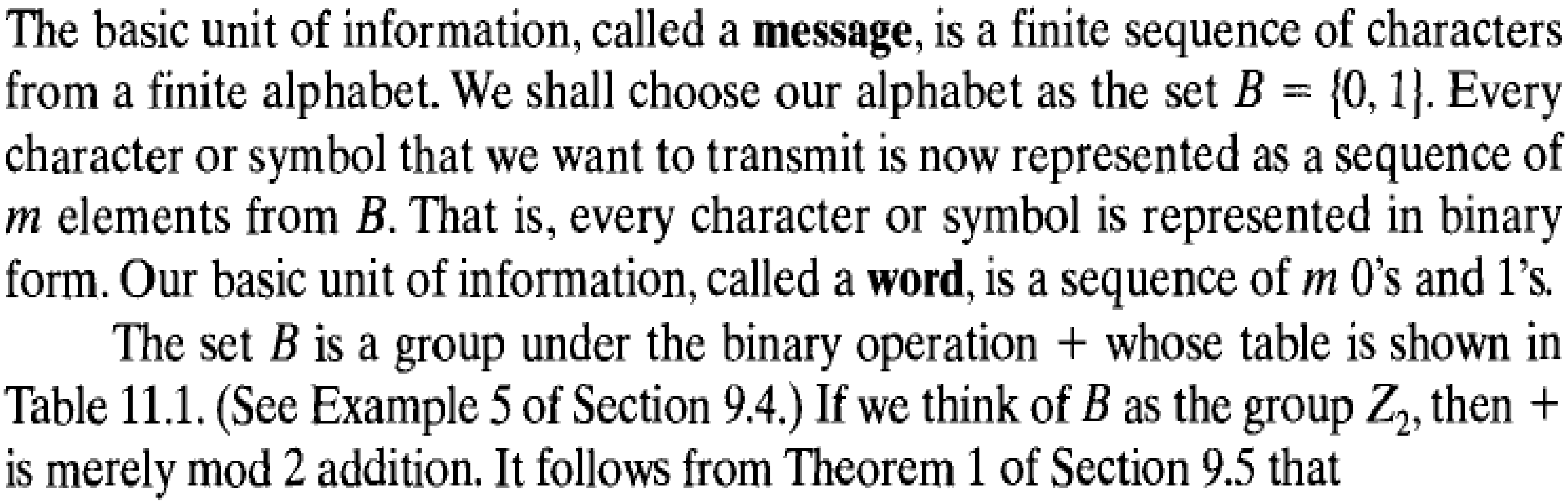
Inverse of [2] in Z_6 is [4]. It must be in $< [2] >$.

Also $2 + 4 = 0$, $2 + 2 = 4$, $4 + 4 = 2$

$\therefore \quad < [2] > = < 0, 2, 4 >$

CODING

Coding of Binary Information and Error detection



The basic unit of information, called a **message**, is a finite sequence of characters from a finite alphabet. We shall choose our alphabet as the set $B = \{0, 1\}$. Every character or symbol that we want to transmit is now represented as a sequence of m elements from B. That is, every character or symbol is represented in binary form. Our basic unit of information, called a **word**, is a sequence of m 0's and 1's.

The set B is a group under the binary operation $+$ whose table is shown in Table 11.1. (See Example 5 of Section 9.4.) If we think of B as the group Z_2, then $+$ is merely mod 2 addition. It follows from Theorem 1 of Section 9.5 that

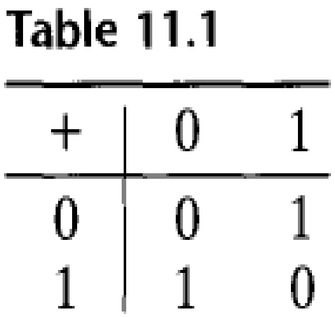
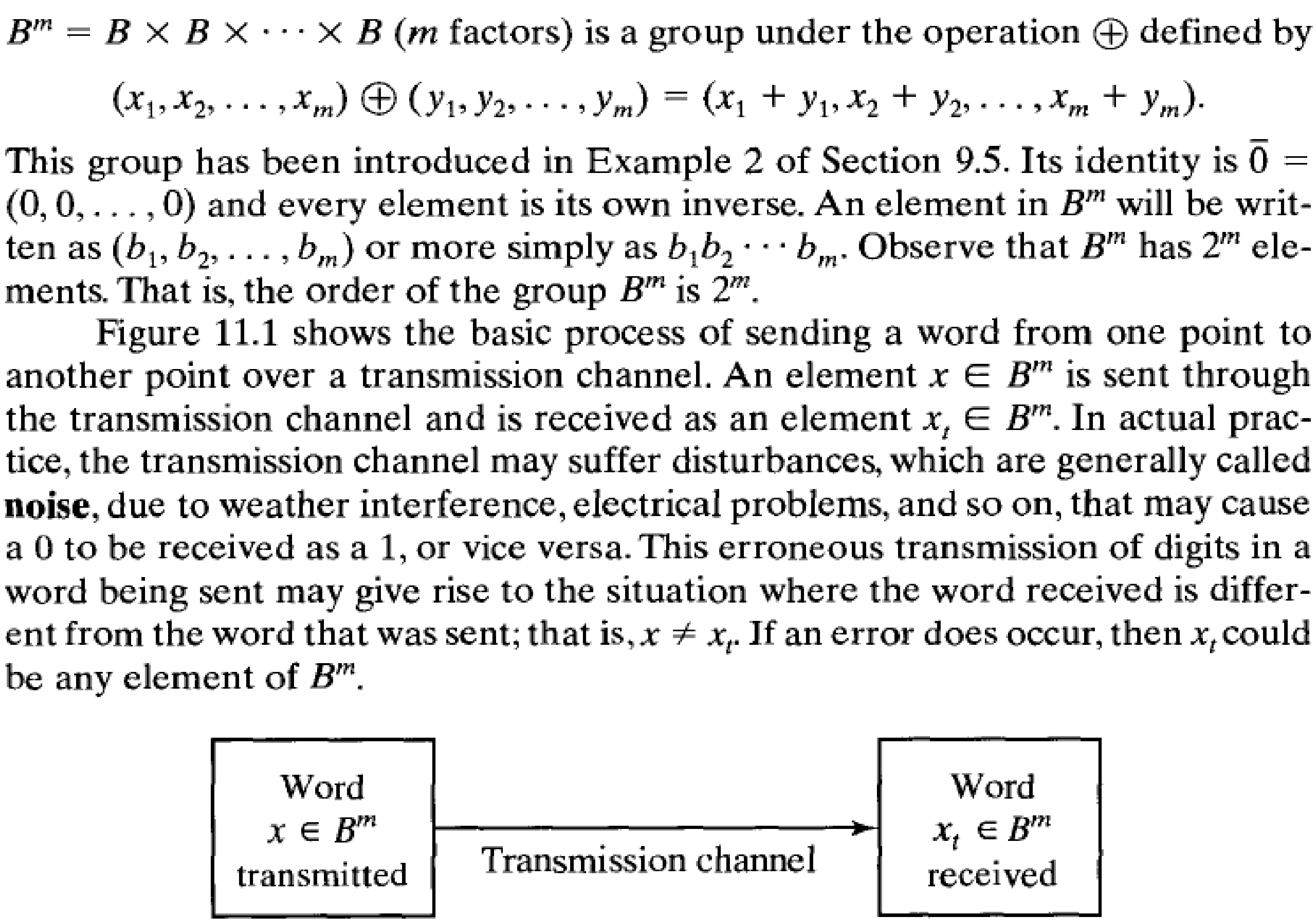


Table 11.1

+	0	1
0	0	1
1	1	0



$B^m = B \times B \times \cdots \times B$ (m factors) is a group under the operation $\oplus$ defined by

$$(x_1, x_2, \ldots, x_m) \oplus (y_1, y_2, \ldots, y_m) = (x_1 + y_1, x_2 + y_2, \ldots, x_m + y_m).$$

This group has been introduced in Example 2 of Section 9.5. Its identity is $\overline{0} = (0, 0, \ldots, 0)$ and every element is its own inverse. An element in B^m will be written as $(b_1, b_2, \ldots, b_m)$ or more simply as $b_1 b_2 \cdots b_m$. Observe that B^m has 2^m elements. That is, the order of the group B^m is 2^m.

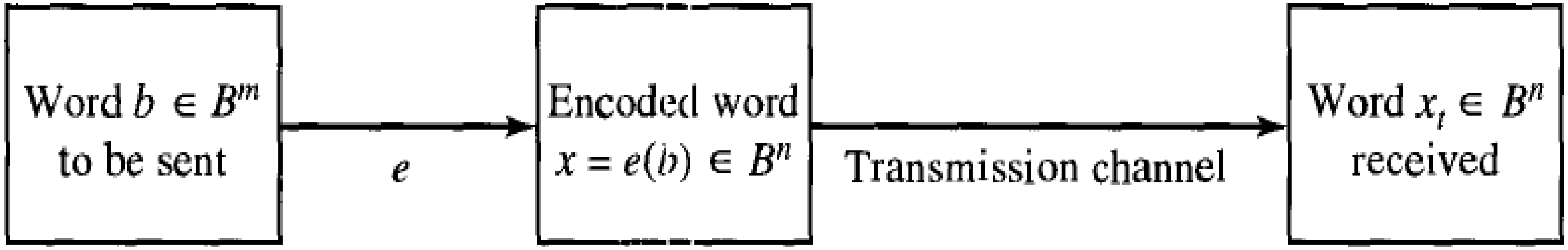
Figure 11.1 shows the basic process of sending a word from one point to another point over a transmission channel. An element $x \in B^m$ is sent through the transmission channel and is received as an element $x_t \in B^m$. In actual practice, the transmission channel may suffer disturbances, which are generally called **noise**, due to weather interference, electrical problems, and so on, that may cause a 0 to be received as a 1, or vice versa. This erroneous transmission of digits in a word being sent may give rise to the situation where the word received is different from the word that was sent; that is, $x \neq x_t$. If an error does occur, then x_t could be any element of B^m.

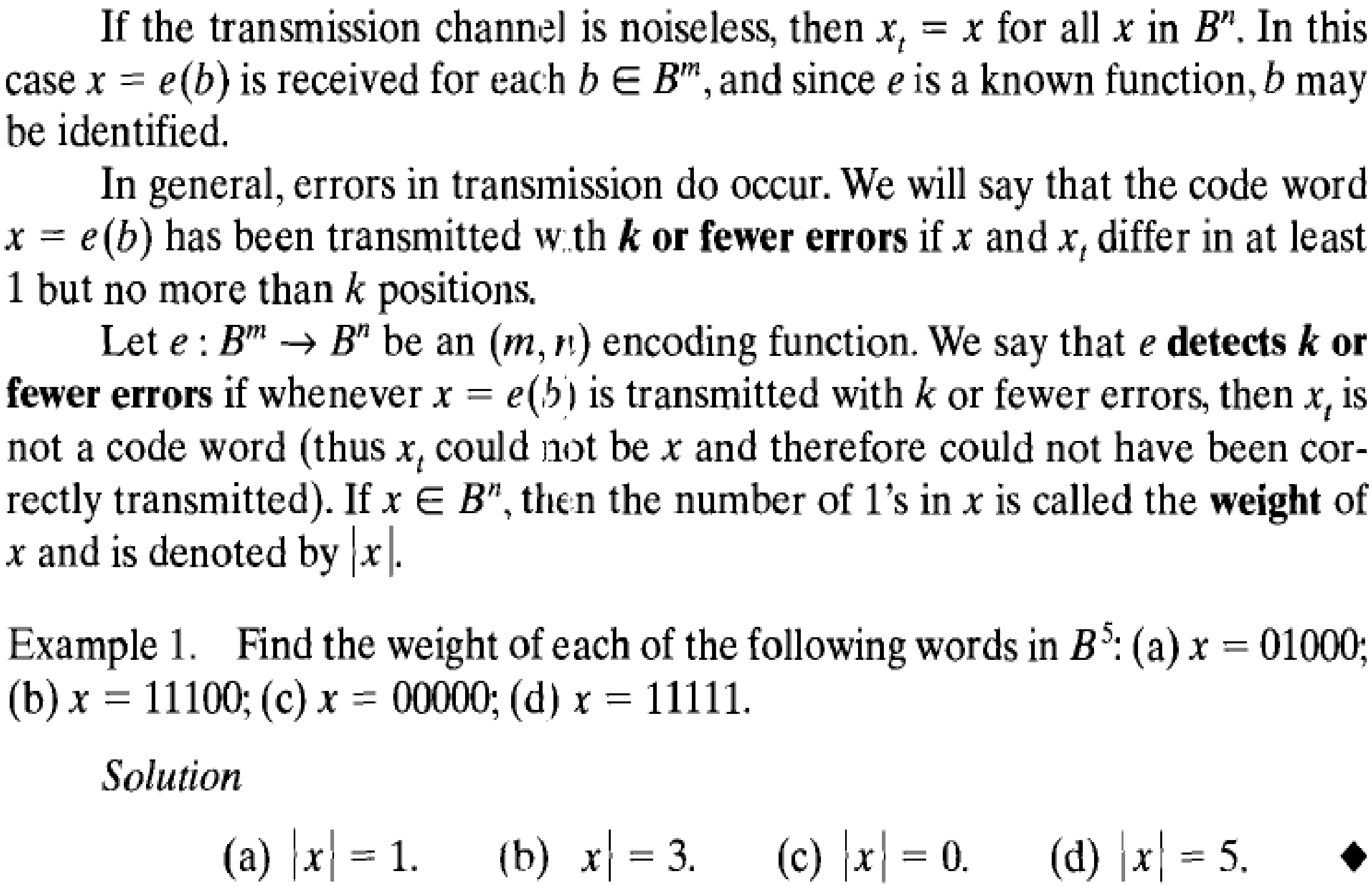
The basic task in the transmission of information is to reduce the likelihood of receiving a word that differs from the word that was sent. This is done as follows. We first choose an integer $n > m$ and a one-to-one function $e : B^m \to B^n$.

The function e is called an (m, n) **encoding function**, and we view it as a means of representing every word in B^m as a word in B^n. If $b \in B^m$, then $e(b)$ is called the **code word** representing b. The additional 0's and 1's can provide the means to detect or correct errors produced in the transmission channel.

We now transmit the code words by means of a transmission channel. Then each code word $x = e(b)$ is received as the word x_t in B^n. This situation is illustrated in Figure 11.2.

Observe that we want an encoding function e to be one to one so that different words in B^m will be assigned different code words.


Word $b \in B^m$ to be sent
e
Encoded word $x = e(b) \in B^n$
Transmission channel
Word $x_t \in B^n$ received



If the transmission channel is noiseless, then $x_t = x$ for all x in B^n. In this case $x = e(b)$ is received for each $b \in B^m$, and since e is a known function, b may be identified.

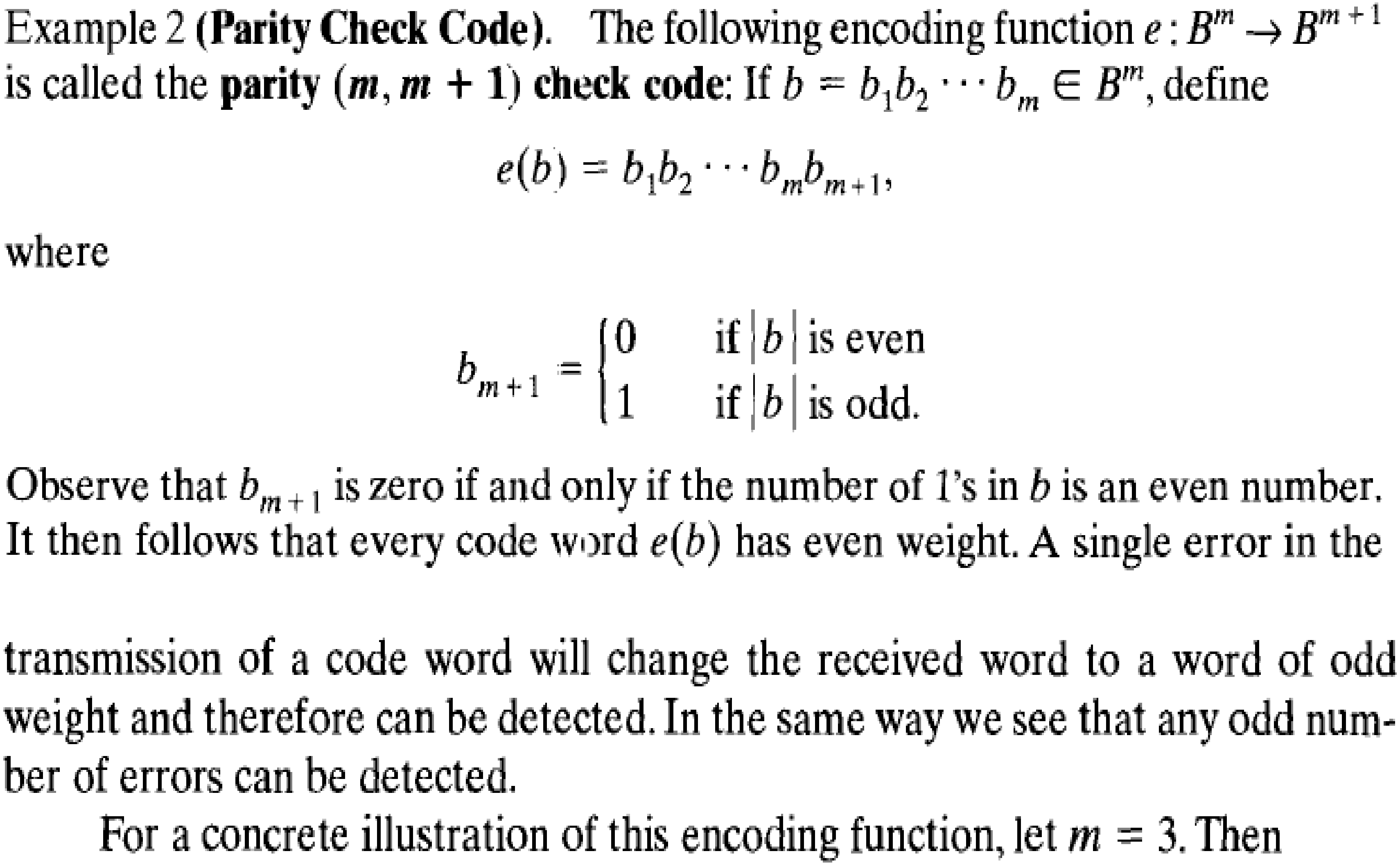
In general, errors in transmission do occur. We will say that the code word $x = e(b)$ has been transmitted with ***k* or fewer errors** if x and x_t differ in at least 1 but no more than k positions.

Let $e : B^m \to B^n$ be an (m, n) encoding function. We say that e **detects *k* or fewer errors** if whenever $x = e(b)$ is transmitted with k or fewer errors, then x_t is not a code word (thus x_t could not be x and therefore could not have been correctly transmitted). If $x \in B^n$, then the number of 1's in x is called the **weight** of x and is denoted by $|x|$.

Example 1. Find the weight of each of the following words in B^5: (a) $x = 01000$; (b) $x = 11100$; (c) $x = 00000$; (d) $x = 11111$.

Solution

(a) $|x| = 1$. (b) $x| = 3$. (c) $|x| = 0$. (d) $|x| = 5$. ◆



Example 2 (**Parity Check Code**). The following encoding function $e : B^m \to B^{m+1}$ is called the **parity $(m, m+1)$ check code**: If $b = b_1 b_2 \cdots b_m \in B^m$, define

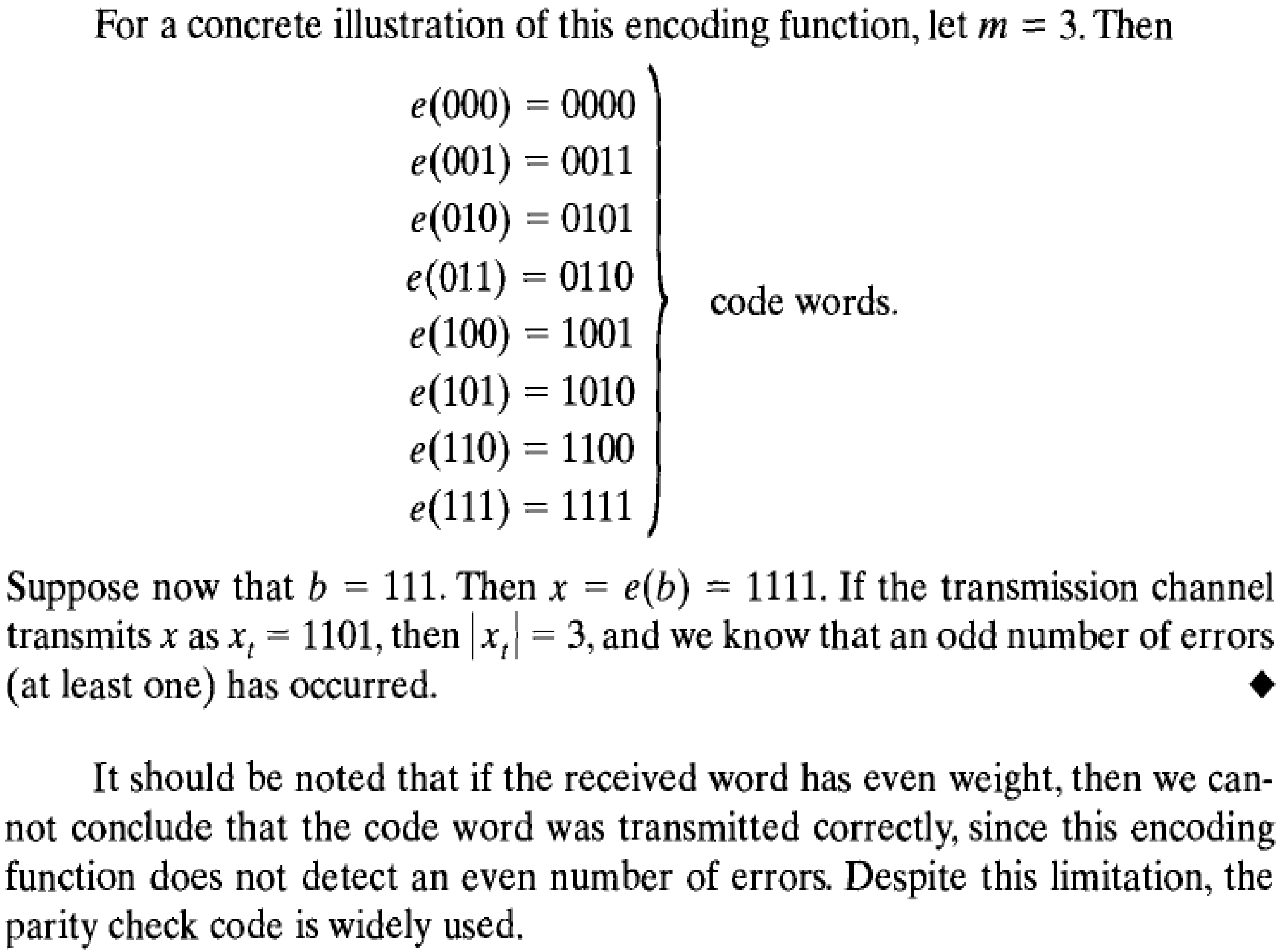
$$e(b) = b_1 b_2 \cdots b_m b_{m+1},$$

where

$$b_{m+1} = \begin{cases} 0 & \text{if } |b| \text{ is even} \\ 1 & \text{if } |b| \text{ is odd.} \end{cases}$$

Observe that b_{m+1} is zero if and only if the number of 1's in b is an even number. It then follows that every code word $e(b)$ has even weight. A single error in the transmission of a code word will change the received word to a word of odd weight and therefore can be detected. In the same way we see that any odd number of errors can be detected.

For a concrete illustration of this encoding function, let $m = 3$. Then

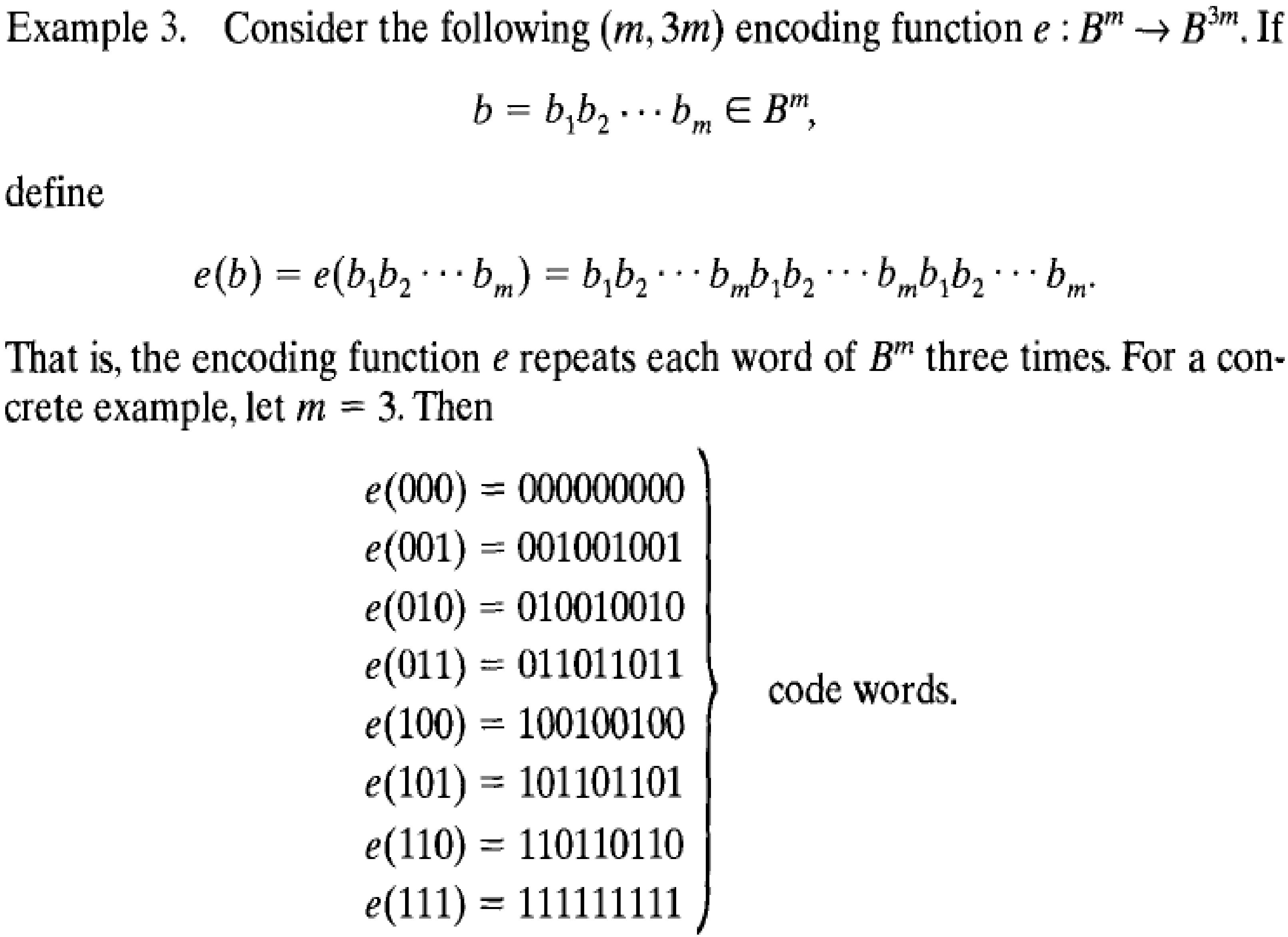


For a concrete illustration of this encoding function, let $m = 3$. Then

$$\left.\begin{aligned} e(000) &= 0000 \\ e(001) &= 0011 \\ e(010) &= 0101 \\ e(011) &= 0110 \\ e(100) &= 1001 \\ e(101) &= 1010 \\ e(110) &= 1100 \\ e(111) &= 1111 \end{aligned}\right\} \text{code words.}$$

Suppose now that $b = 111$. Then $x = e(b) = 1111$. If the transmission channel transmits x as $x_t = 1101$, then $|x_t| = 3$, and we know that an odd number of errors (at least one) has occurred. ◆

It should be noted that if the received word has even weight, then we cannot conclude that the code word was transmitted correctly, since this encoding function does not detect an even number of errors. Despite this limitation, the parity check code is widely used.



Example 3. Consider the following $(m, 3m)$ encoding function $e : B^m \to B^{3m}$. If

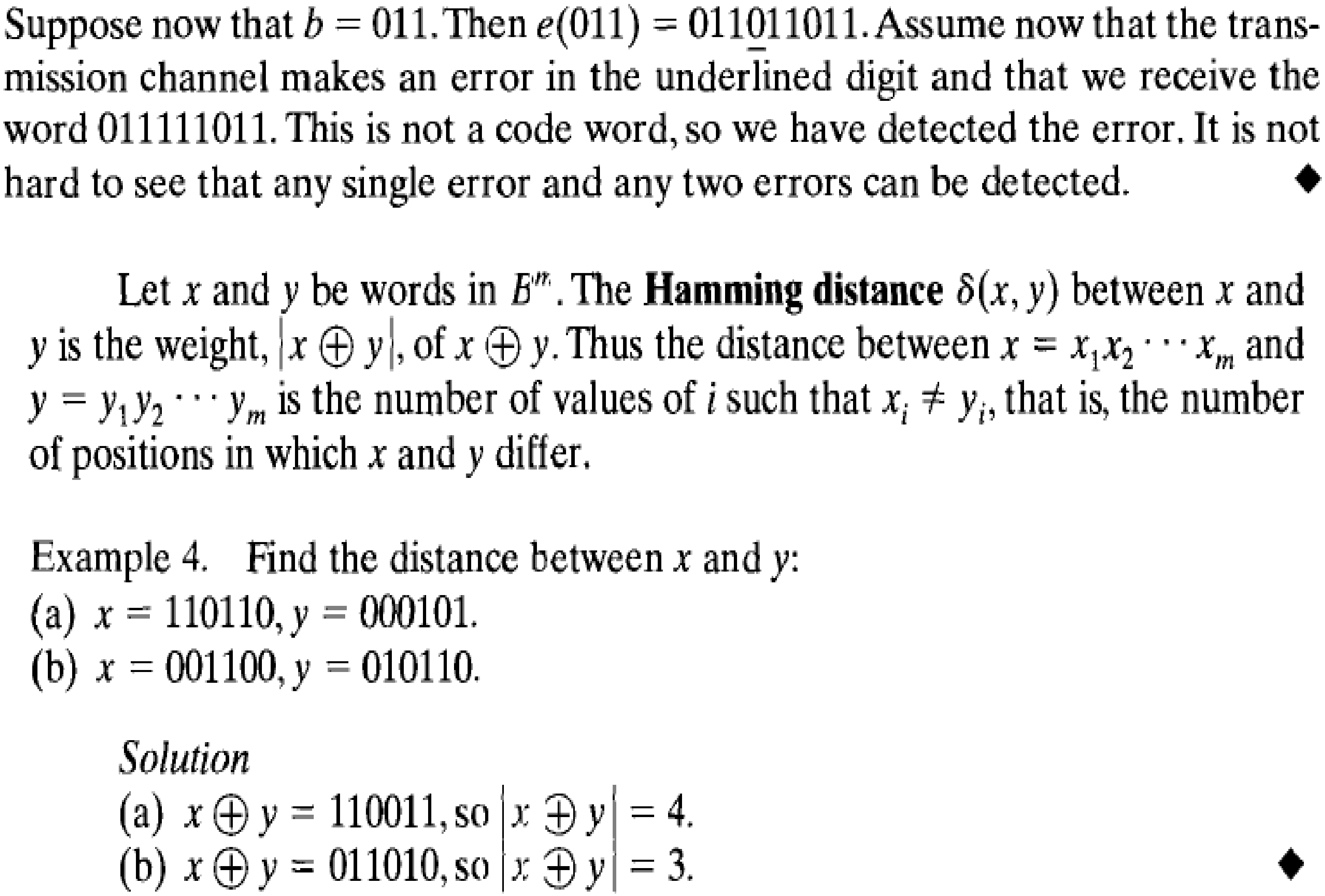
$$b = b_1 b_2 \cdots b_m \in B^m,$$

define

$$e(b) = e(b_1 b_2 \cdots b_m) = b_1 b_2 \cdots b_m b_1 b_2 \cdots b_m b_1 b_2 \cdots b_m.$$

That is, the encoding function e repeats each word of B^m three times. For a concrete example, let $m = 3$. Then

$$\left.\begin{aligned} e(000) &= 000000000 \\ e(001) &= 001001001 \\ e(010) &= 010010010 \\ e(011) &= 011011011 \\ e(100) &= 100100100 \\ e(101) &= 101101101 \\ e(110) &= 110110110 \\ e(111) &= 111111111 \end{aligned}\right\} \quad \text{code words.}$$



Suppose now that $b = 011$. Then $e(011) = 011\underline{0}11011$. Assume now that the transmission channel makes an error in the underlined digit and that we receive the word 011111011. This is not a code word, so we have detected the error. It is not hard to see that any single error and any two errors can be detected. ◆

Let x and y be words in B^m. The **Hamming distance** $\delta(x, y)$ between x and y is the weight, $|x \oplus y|$, of $x \oplus y$. Thus the distance between $x = x_1x_2 \cdots x_m$ and $y = y_1y_2 \cdots y_m$ is the number of values of i such that $x_i \neq y_i$, that is, the number of positions in which x and y differ.

Example 4. Find the distance between x and y:

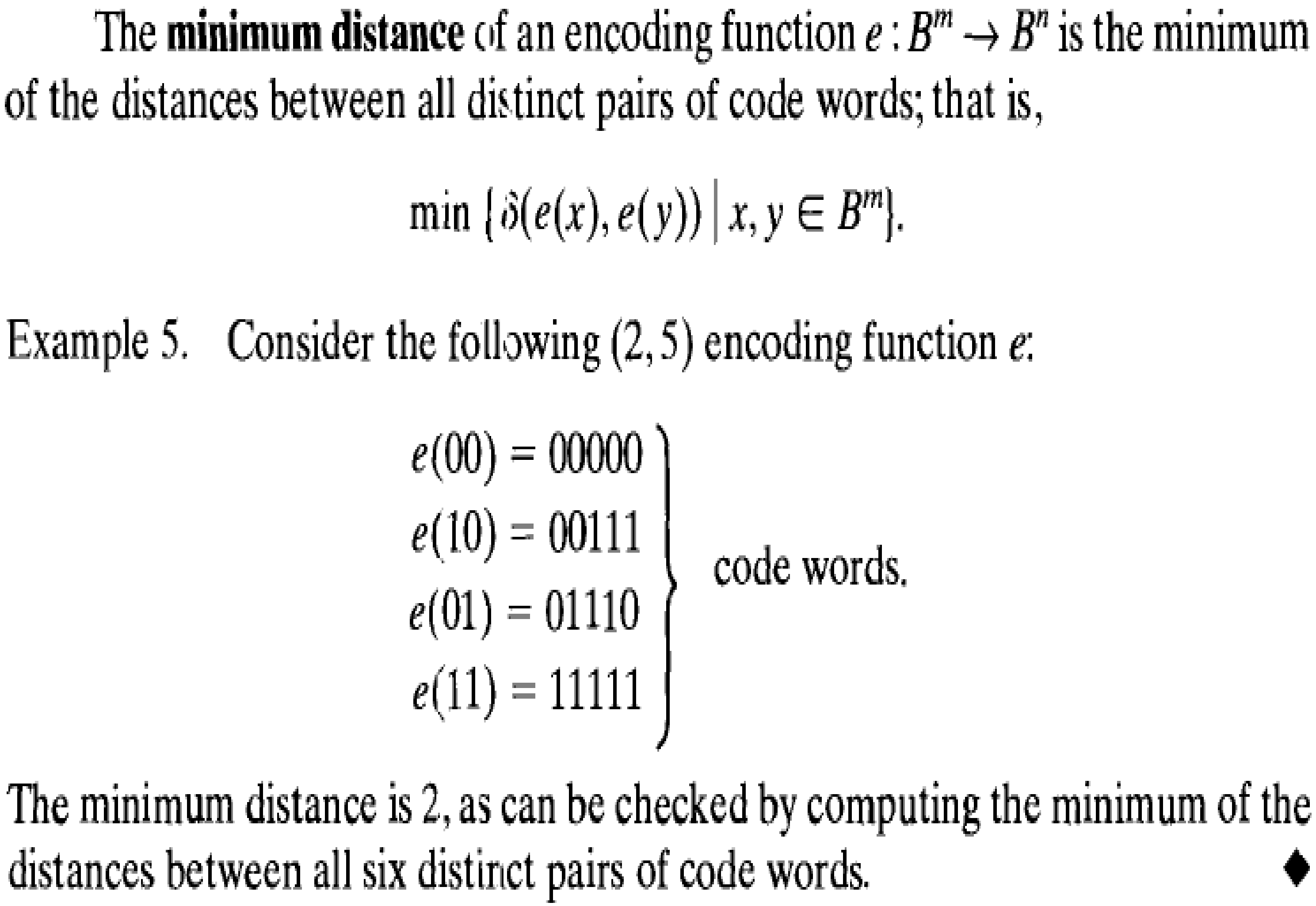
(a) $x = 110110, y = 000101$.

(b) $x = 001100, y = 010110$.

Solution

(a) $x \oplus y = 110011$, so $|x \oplus y| = 4$.

(b) $x \oplus y = 011010$, so $|x \oplus y| = 3$. ◆



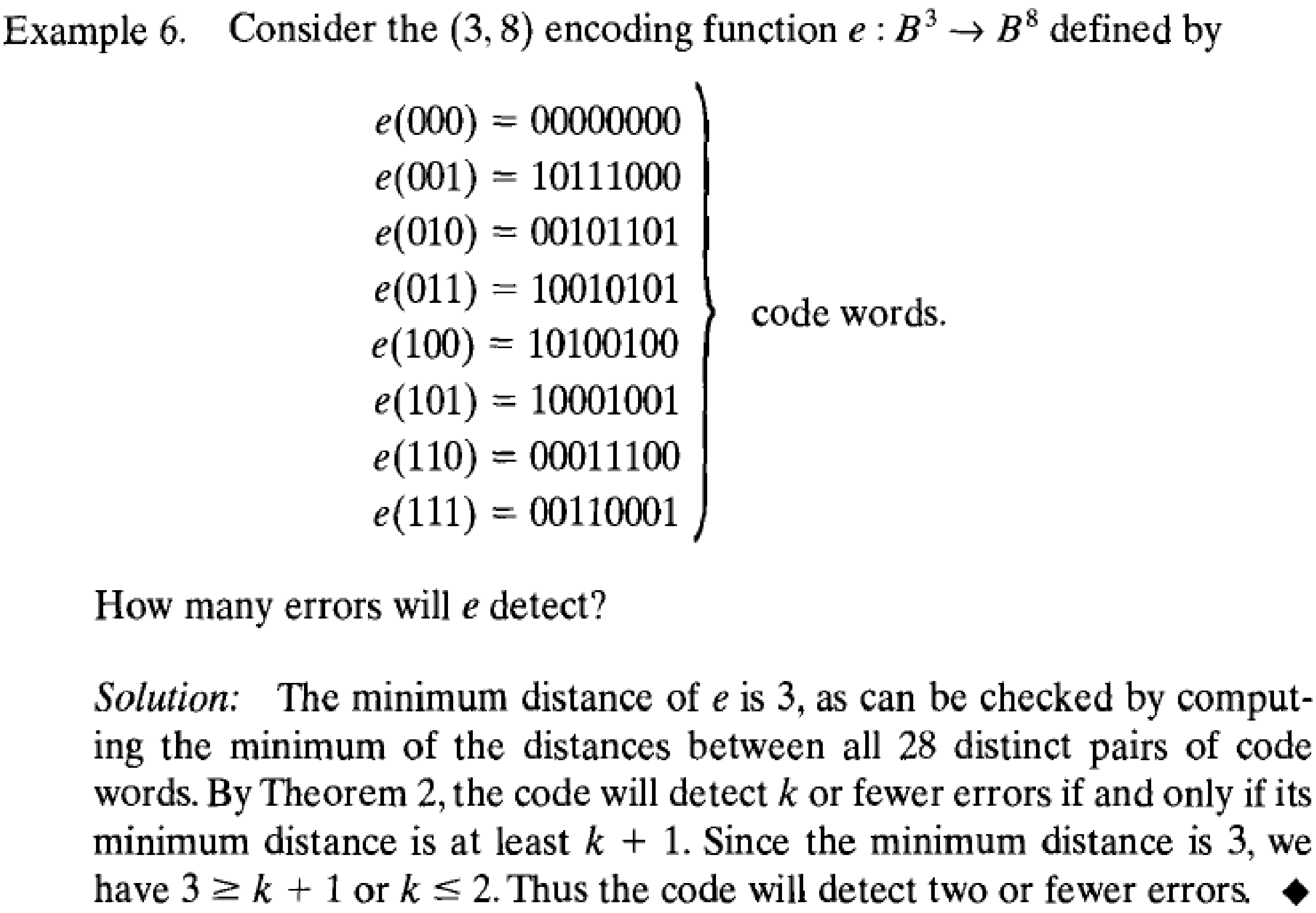
The **minimum distance** of an encoding function $e : B^m \to B^n$ is the minimum of the distances between all distinct pairs of code words; that is,

$$\min \{\delta(e(x), e(y)) \mid x, y \in B^m\}.$$

Example 5. Consider the following $(2, 5)$ encoding function e:

$$\left.\begin{aligned} e(00) &= 00000 \\ e(10) &= 00111 \\ e(01) &= 01110 \\ e(11) &= 11111 \end{aligned}\right\} \text{ code words.}$$

The minimum distance is 2, as can be checked by computing the minimum of the distances between all six distinct pairs of code words. ♦

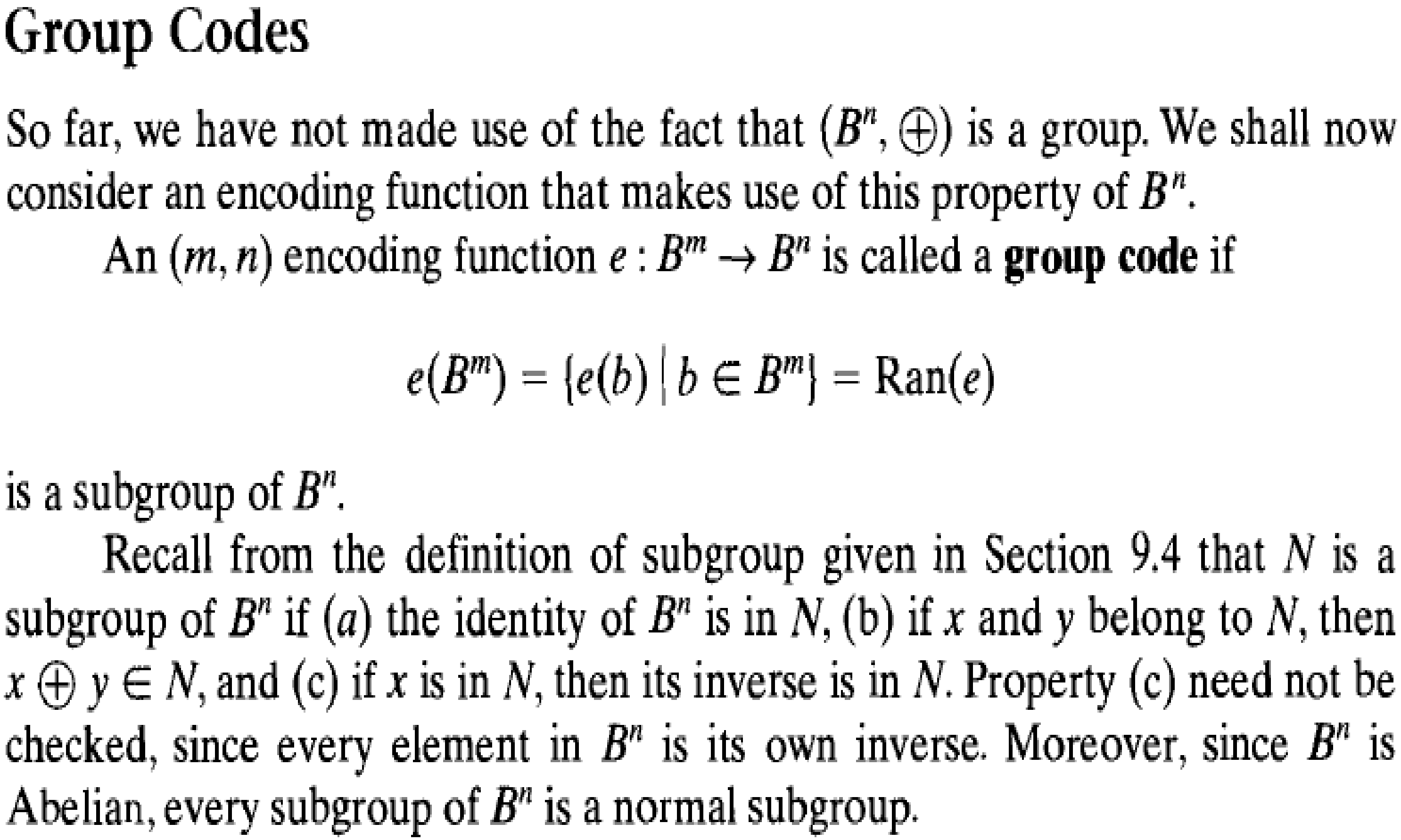


Example 6. Consider the (3, 8) encoding function $e : B^3 \to B^8$ defined by

$$\left.\begin{aligned}
e(000) &= 00000000\\
e(001) &= 10111000\\
e(010) &= 00101101\\
e(011) &= 10010101\\
e(100) &= 10100100\\
e(101) &= 10001001\\
e(110) &= 00011100\\
e(111) &= 00110001
\end{aligned}\right\} \text{code words.}$$

How many errors will e detect?

Solution: The minimum distance of e is 3, as can be checked by computing the minimum of the distances between all 28 distinct pairs of code words. By Theorem 2, the code will detect k or fewer errors if and only if its minimum distance is at least $k + 1$. Since the minimum distance is 3, we have $3 \geq k + 1$ or $k \leq 2$. Thus the code will detect two or fewer errors. ◆



Group Codes

So far, we have not made use of the fact that $(B^n, \oplus)$ is a group. We shall now consider an encoding function that makes use of this property of B^n.

An (m, n) encoding function $e : B^m \to B^n$ is called a **group code** if

$$e(B^m) = \{e(b) \mid b \in B^m\} = \text{Ran}(e)$$

is a subgroup of B^n.

Recall from the definition of subgroup given in Section 9.4 that N is a subgroup of B^n if (a) the identity of B^n is in N, (b) if x and y belong to N, then $x \oplus y \in N$, and (c) if x is in N, then its inverse is in N. Property (c) need not be checked, since every element in B^n is its own inverse. Moreover, since B^n is Abelian, every subgroup of B^n is a normal subgroup.

Example 7. Consider the (3, 6) encoding function $e : B^3 \to B^6$ defined by

$$\left.\begin{aligned} e(000) &= 000000 \\ e(001) &= 001100 \\ e(010) &= 010011 \\ e(011) &= 011111 \\ e(100) &= 100101 \\ e(101) &= 101001 \\ e(110) &= 110110 \\ e(111) &= 111010 \end{aligned}\right\} \text{code words.}$$

Show that this encoding function is a group code.

Solution: We must show that the set of all code words

$$N = \{000000, 001100, 010011, 011111, 100101, 101001, 110110, 111010\}$$

is a subgroup of B^6. This is done by first noting that the identity of B^6 belongs to N. Next we verify, by trying all possibilities, that if x and y are elements in N, then $x \oplus y$ is in N. Hence N is a subgroup of B^6, and the given encoding function is a group code. ◆

Let $m < n$ and $r = n - m$. An $n \times r$ Boolean matrix

$$\mathbf{H} = \begin{array}{r} \begin{matrix} \\ \\ \\ \\ \end{matrix} \\ n - m = r \text{ rows} \left\{ \begin{matrix} \\ \\ \\ \\ \end{matrix} \right. \end{array} \begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1r} \\ h_{21} & h_{22} & \cdots & h_{2r} \\ \vdots & \vdots & & \vdots \\ h_{m1} & h_{m2} & \cdots & h_{mr} \\ 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix},$$

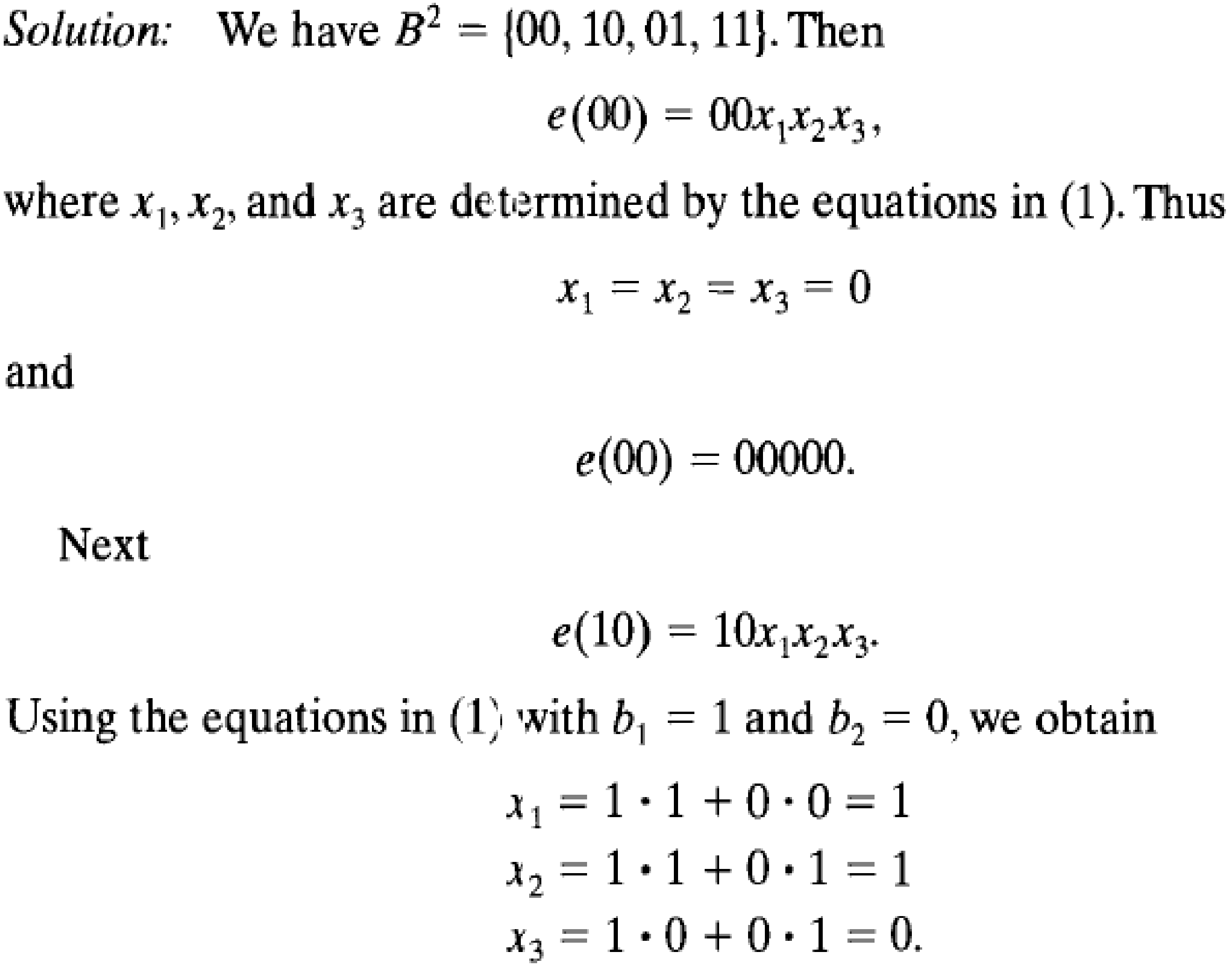
whose last r rows form the $r \times r$ identity matrix, is called a **parity check matrix**. We use $\mathbf{H}$ to define an encoding function $e_H: B^m \to B^n$. If $b = b_1 b_2 \cdots b_m$, let $x = e_H(b) = b_1 b_2 \cdots b_m x_1 x_2 \cdots x_r$, where

$$\begin{aligned} x_1 &= b_1 \cdot h_{11} + b_2 \cdot h_{21} + \cdots + b_m \cdot h_{m1} \\ x_2 &= b_1 \cdot h_{12} + b_2 \cdot h_{22} + \cdots + b_m \cdot h_{m2} \\ &\vdots \\ x_r &= b_1 \cdot h_{1r} + b_2 \cdot h_{2r} + \cdots + b_m \cdot h_{mr}. \end{aligned} \tag{1}$$

Example 11. Let $m = 2, n = 5$, and

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Determine the group code $e_H \colon B^2 \to B^5$.



Solution: We have $B^2 = \{00, 10, 01, 11\}$. Then

$$e(00) = 00x_1x_2x_3,$$

where x_1, x_2, and x_3 are determined by the equations in (1). Thus

$$x_1 = x_2 = x_3 = 0$$

and

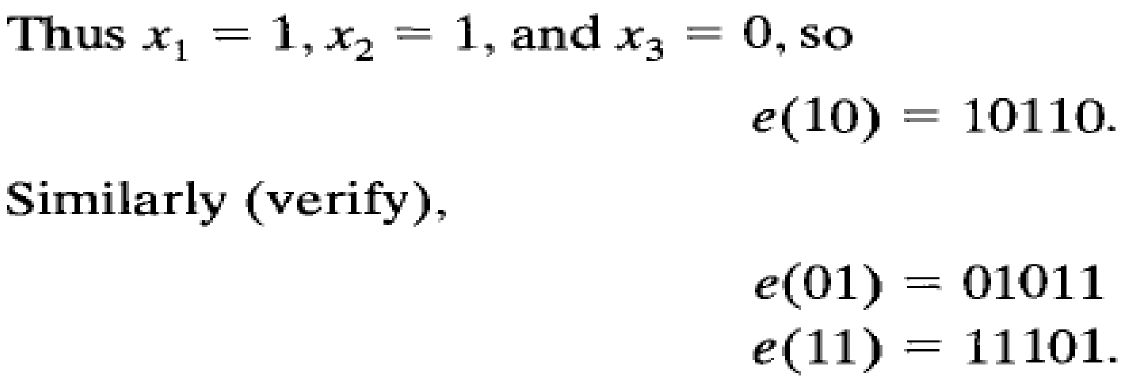
$$e(00) = 00000.$$

Next

$$e(10) = 10x_1x_2x_3.$$

Using the equations in (1) with $b_1 = 1$ and $b_2 = 0$, we obtain

$$x_1 = 1 \cdot 1 + 0 \cdot 0 = 1$$
$$x_2 = 1 \cdot 1 + 0 \cdot 1 = 1$$
$$x_3 = 1 \cdot 0 + 0 \cdot 1 = 0.$$



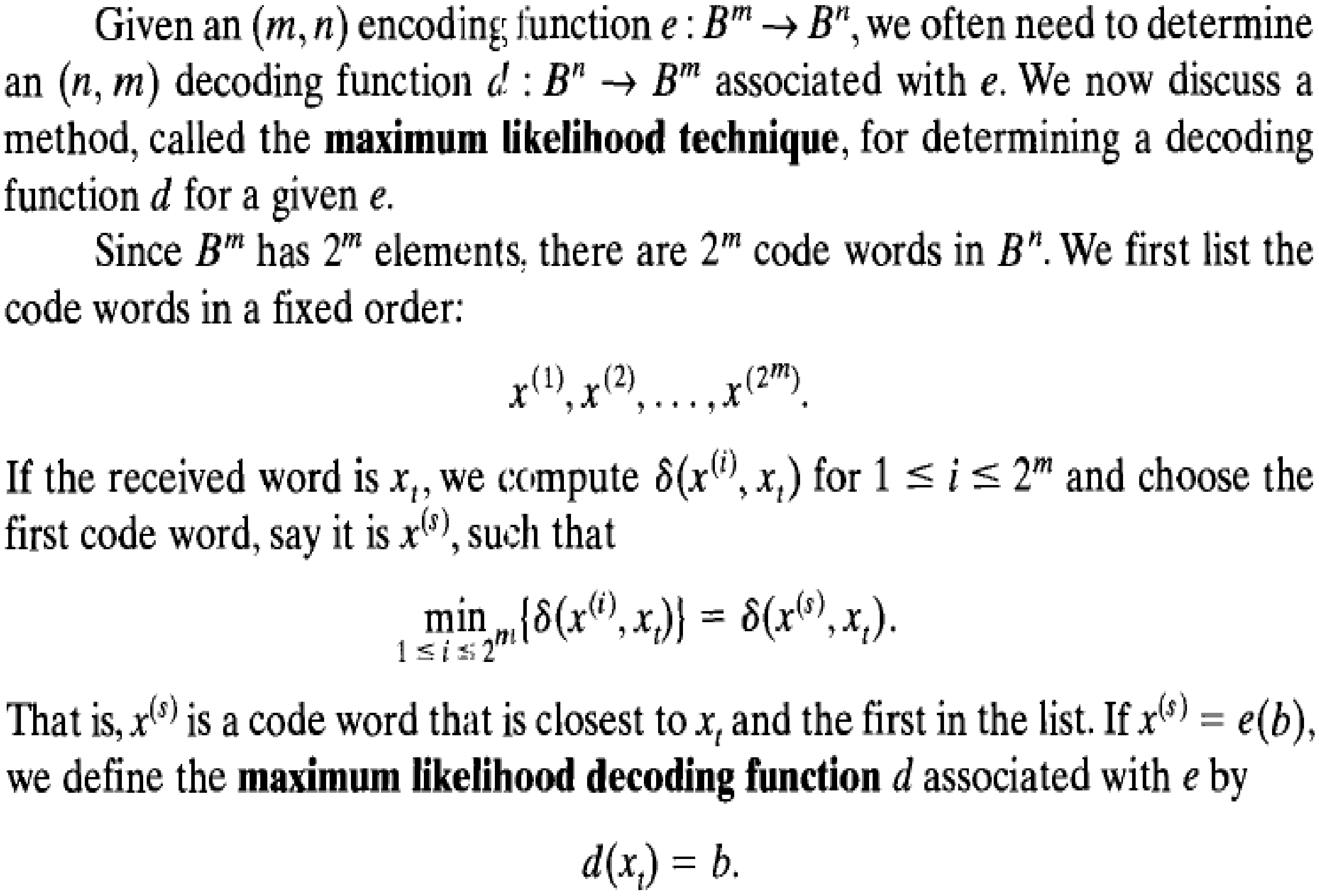
Thus $x_1 = 1, x_2 = 1$, and $x_3 = 0$, so

$$e(10) = 10110.$$

Similarly (verify),

$$e(01) = 01011$$
$$e(11) = 11101.$$

Decoding and Error Correction



Given an (m, n) encoding function $e : B^m \to B^n$, we often need to determine an (n, m) decoding function $d : B^n \to B^m$ associated with e. We now discuss a method, called the **maximum likelihood technique**, for determining a decoding function d for a given e.

Since B^m has 2^m elements, there are 2^m code words in B^n. We first list the code words in a fixed order:

$$x^{(1)}, x^{(2)}, \ldots, x^{(2^m)}.$$

If the received word is x_t, we compute $\delta(x^{(i)}, x_t)$ for $1 \le i \le 2^m$ and choose the first code word, say it is $x^{(s)}$, such that

$$\min_{1 \le i \le 2^m} \{\delta(x^{(i)}, x_t)\} = \delta(x^{(s)}, x_t).$$

That is, $x^{(s)}$ is a code word that is closest to x_t and the first in the list. If $x^{(s)} = e(b)$, we define the **maximum likelihood decoding function** d associated with e by

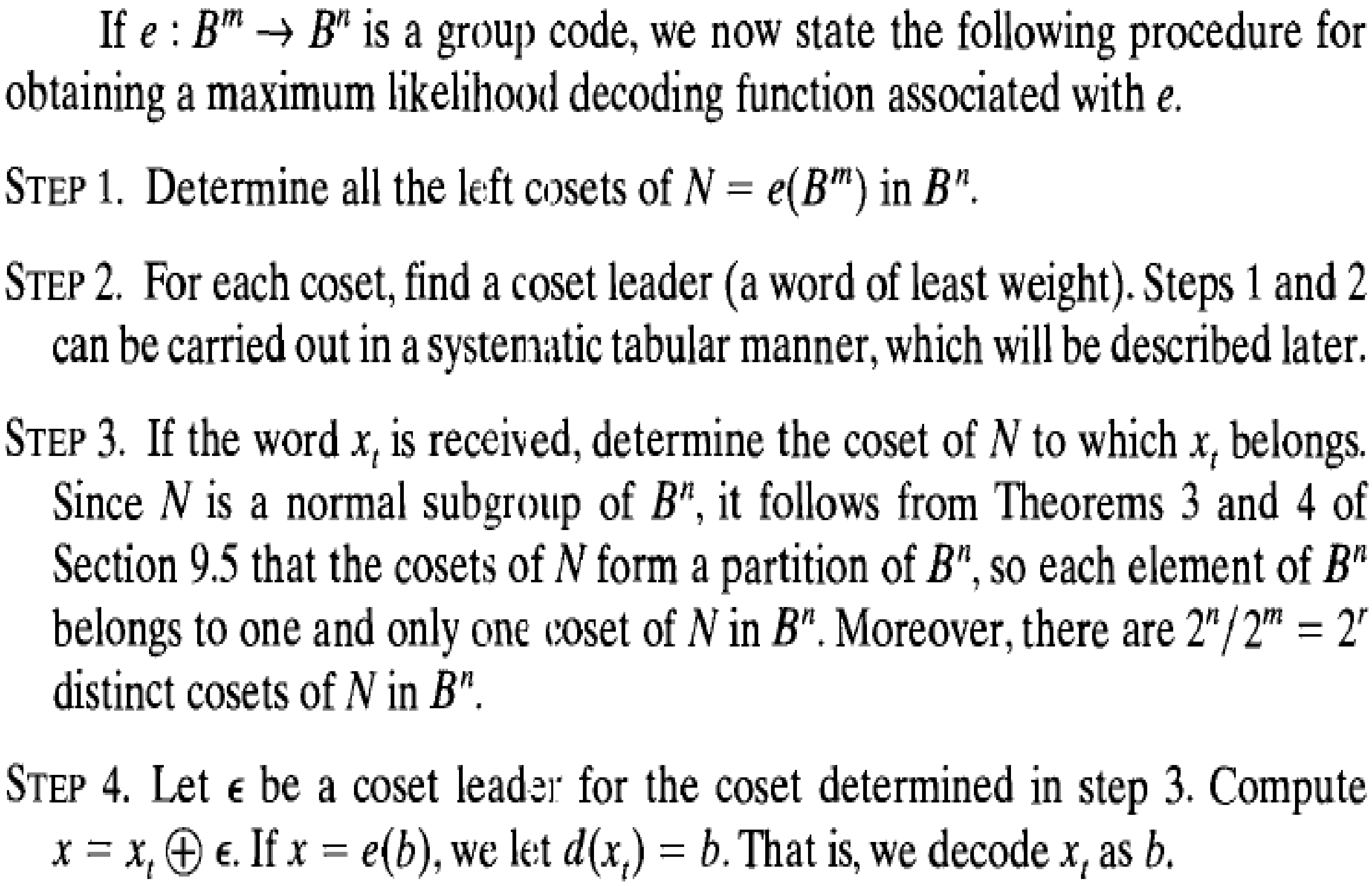
$$d(x_t) = b.$$

Observe that d depends on the particular order in which the code words in $e(B^m)$ are listed. If the code words are listed in a different order, we may obtain a different maximum likelihood decoding function d associated with e.

Theorem 1. *Suppose that e is an (m, n) encoding function and d is a maximum likelihood decoding function associated with e. Then (e, d) can correct k or fewer errors if and only if the minimum distance of e is at least $2k + 1$.*

Example 3. Let e be the $(3, 8)$ encoding function defined in Example 6 of Section 11.1, and let d be an $(8, 3)$ maximum likelihood decoding function associated with e. How many errors can (e, d) correct?

Solution: Since the minimum distance of e is 3, we have $3 \geq 2k + 1$, so $k \leq 1$. Thus (e, d) can correct one error. ◆



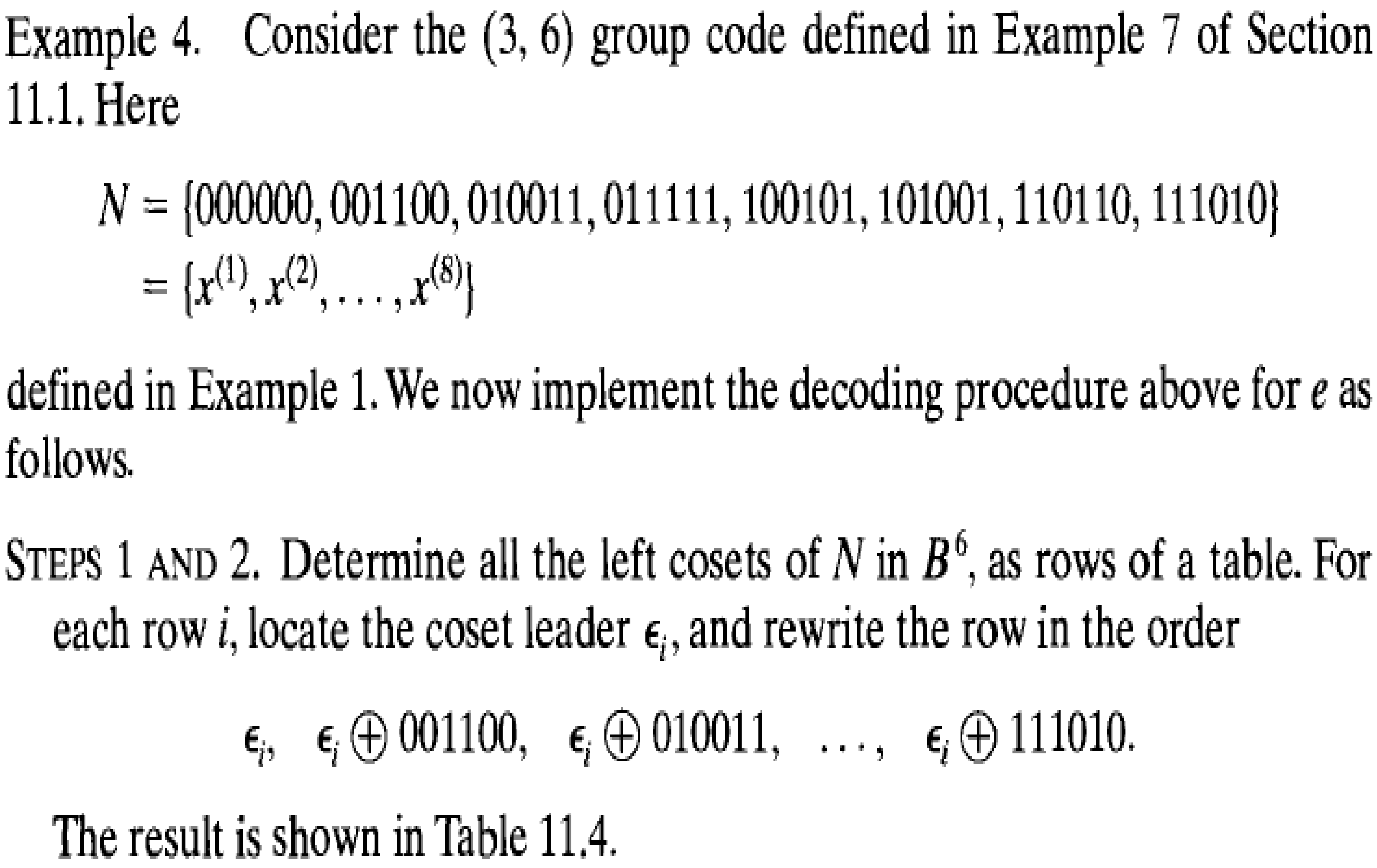
If $e : B^m \to B^n$ is a group code, we now state the following procedure for obtaining a maximum likelihood decoding function associated with e.

STEP 1. Determine all the left cosets of $N = e(B^m)$ in B^n.

STEP 2. For each coset, find a coset leader (a word of least weight). Steps 1 and 2 can be carried out in a systematic tabular manner, which will be described later.

STEP 3. If the word x_t is received, determine the coset of N to which x_t belongs. Since N is a normal subgroup of B^n, it follows from Theorems 3 and 4 of Section 9.5 that the cosets of N form a partition of B^n, so each element of B^n belongs to one and only one coset of N in B^n. Moreover, there are $2^n/2^m = 2^r$ distinct cosets of N in B^n.

STEP 4. Let ϵ be a coset leader for the coset determined in step 3. Compute $x = x_t \oplus \epsilon$. If $x = e(b)$, we let $d(x_t) = b$. That is, we decode x_t as b.



Example 4. Consider the (3, 6) group code defined in Example 7 of Section 11.1. Here

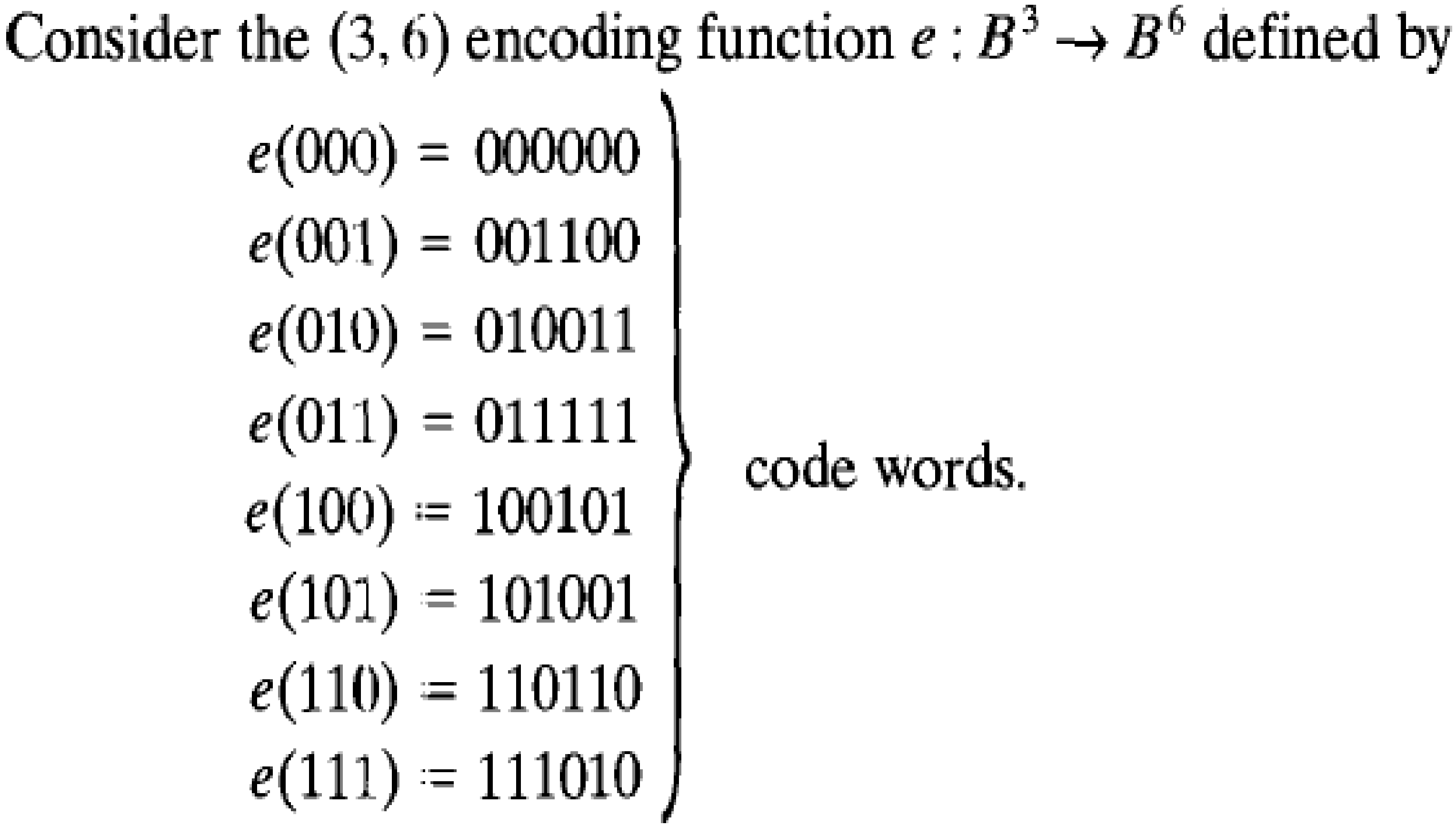
$$\begin{aligned} N &= \{000000, 001100, 010011, 011111, 100101, 101001, 110110, 111010\} \\ &= \{x^{(1)}, x^{(2)}, \ldots, x^{(8)}\} \end{aligned}$$

defined in Example 1. We now implement the decoding procedure above for e as follows.

STEPS 1 AND 2. Determine all the left cosets of N in B^6, as rows of a table. For each row i, locate the coset leader ϵ_i, and rewrite the row in the order

$$\epsilon_i, \quad \epsilon_i \oplus 001100, \quad \epsilon_i \oplus 010011, \quad \ldots, \quad \epsilon_i \oplus 111010.$$

The result is shown in Table 11.4.



Consider the $(3, 6)$ encoding function $e : B^3 \to B^6$ defined by

$$\left.\begin{aligned}
e(000) &= 000000 \\
e(001) &= 001100 \\
e(010) &= 010011 \\
e(011) &= 011111 \\
e(100) &= 100101 \\
e(101) &= 101001 \\
e(110) &= 110110 \\
e(111) &= 111010
\end{aligned}\right\} \text{code words.}$$

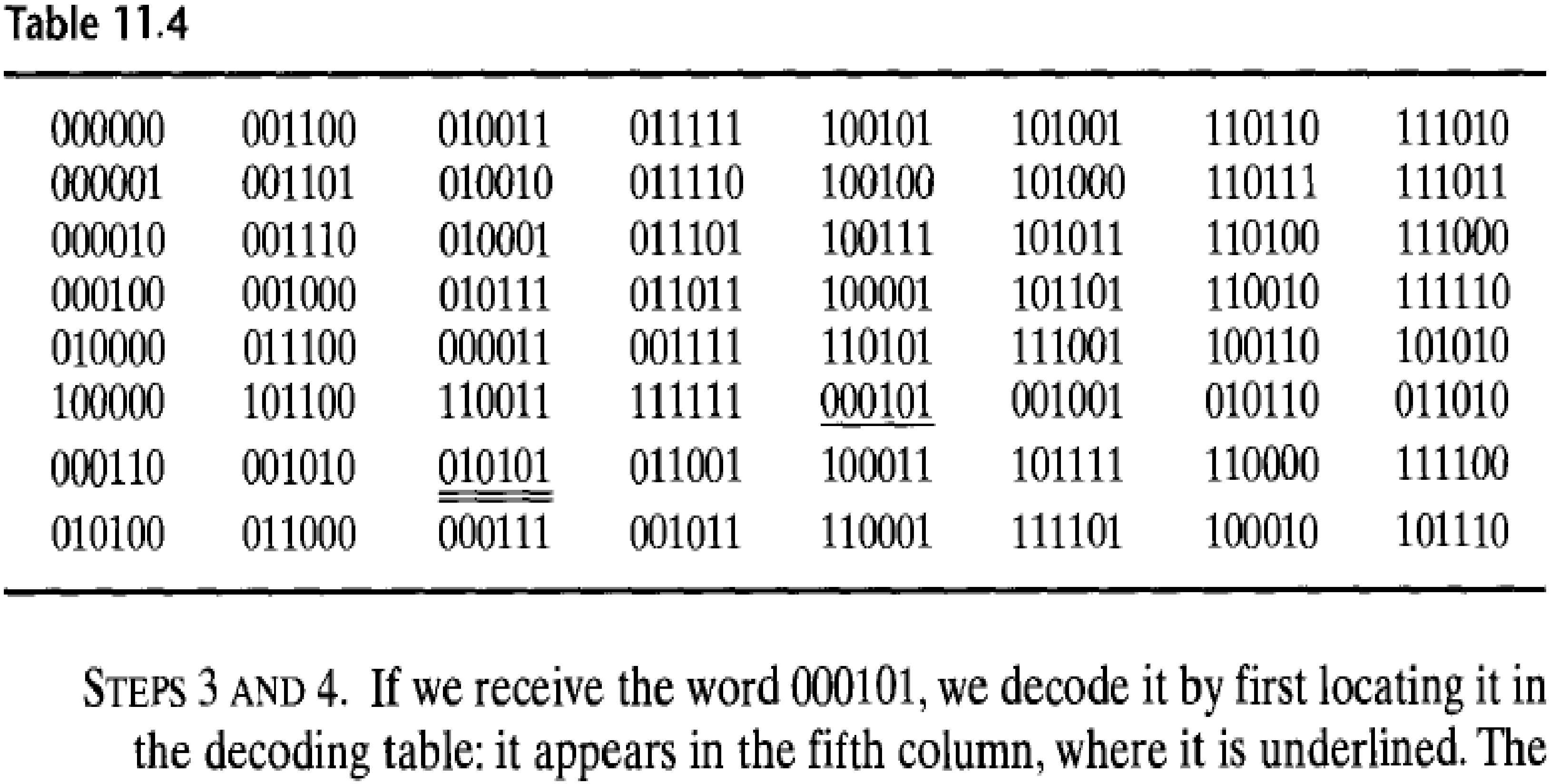
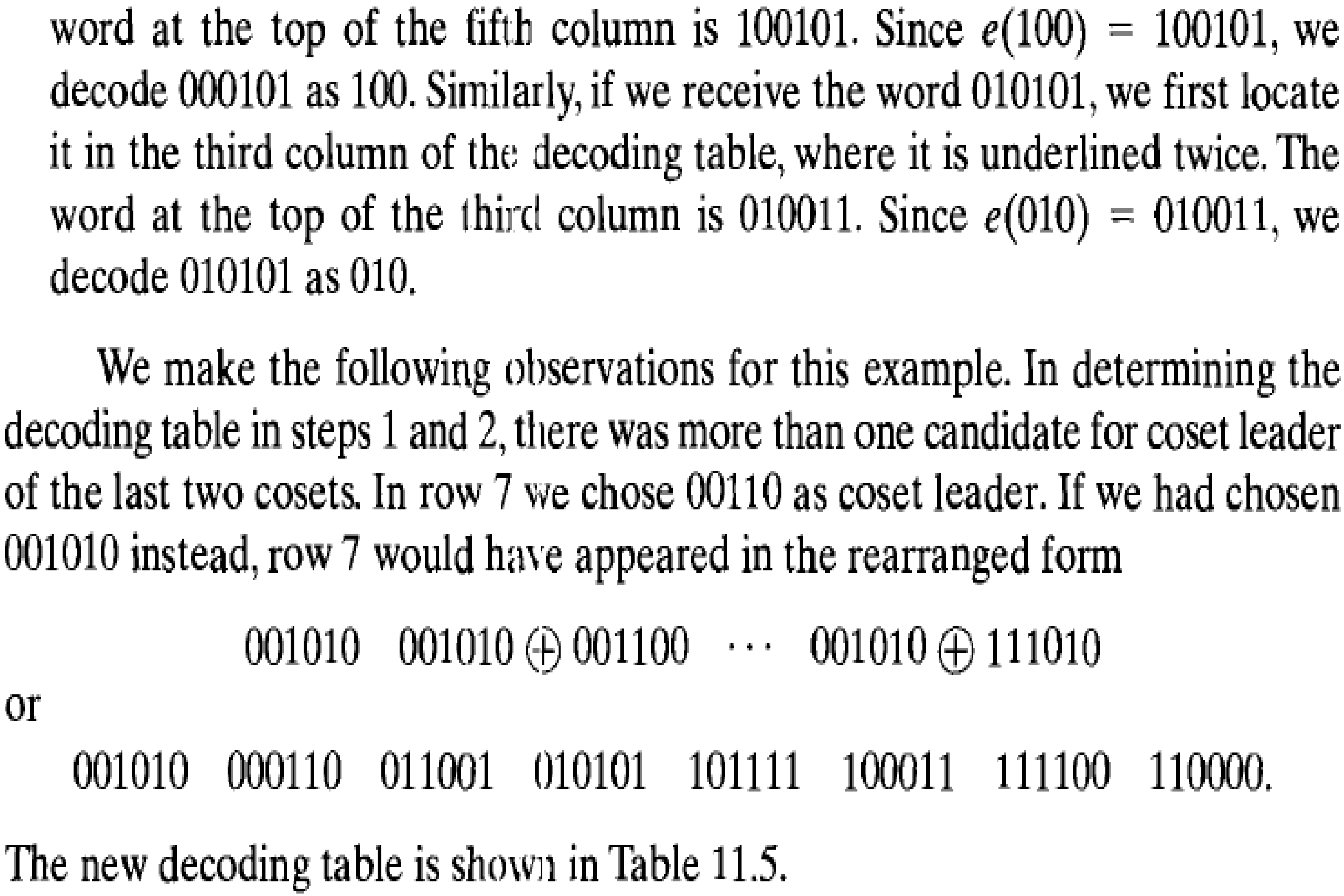


Table 11.4

000000	001100	010011	011111	100101	101001	110110	111010
000001	001101	010010	011110	100100	101000	110111	111011
000010	001110	010001	011101	100111	101011	110100	111000
000100	001000	010111	011011	100001	101101	110010	111110
010000	011100	000011	001111	110101	111001	100110	101010
100000	101100	110011	111111	000101	001001	010110	011010
000110	001010	010101	011001	100011	101111	110000	111100
010100	011000	000111	001011	110001	111101	100010	101110

STEPS 3 AND 4. If we receive the word 000101, we decode it by first locating it in the decoding table: it appears in the fifth column, where it is underlined. The



word at the top of the fifth column is 100101. Since $e(100) = 100101$, we decode 000101 as 100. Similarly, if we receive the word 010101, we first locate it in the third column of the decoding table, where it is underlined twice. The word at the top of the third column is 010011. Since $e(010) = 010011$, we decode 010101 as 010.

We make the following observations for this example. In determining the decoding table in steps 1 and 2, there was more than one candidate for coset leader of the last two cosets. In row 7 we chose 00110 as coset leader. If we had chosen 001010 instead, row 7 would have appeared in the rearranged form

$$001010 \quad 001010 \oplus 001100 \quad \cdots \quad 001010 \oplus 111010$$

or

$$001010 \quad 000110 \quad 011001 \quad 010101 \quad 101111 \quad 100011 \quad 111100 \quad 110000.$$

The new decoding table is shown in Table 11.5.

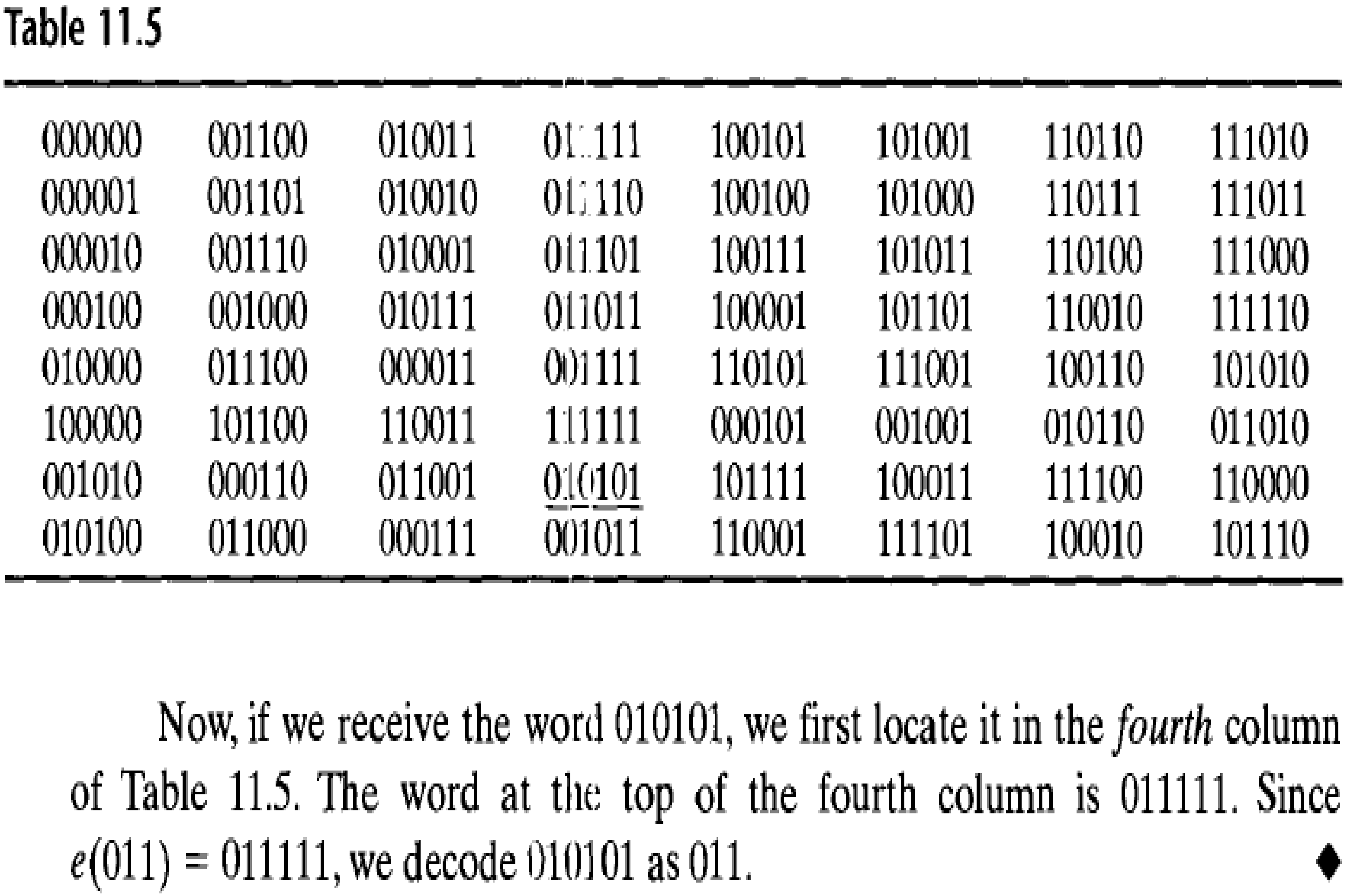


Table 11.5

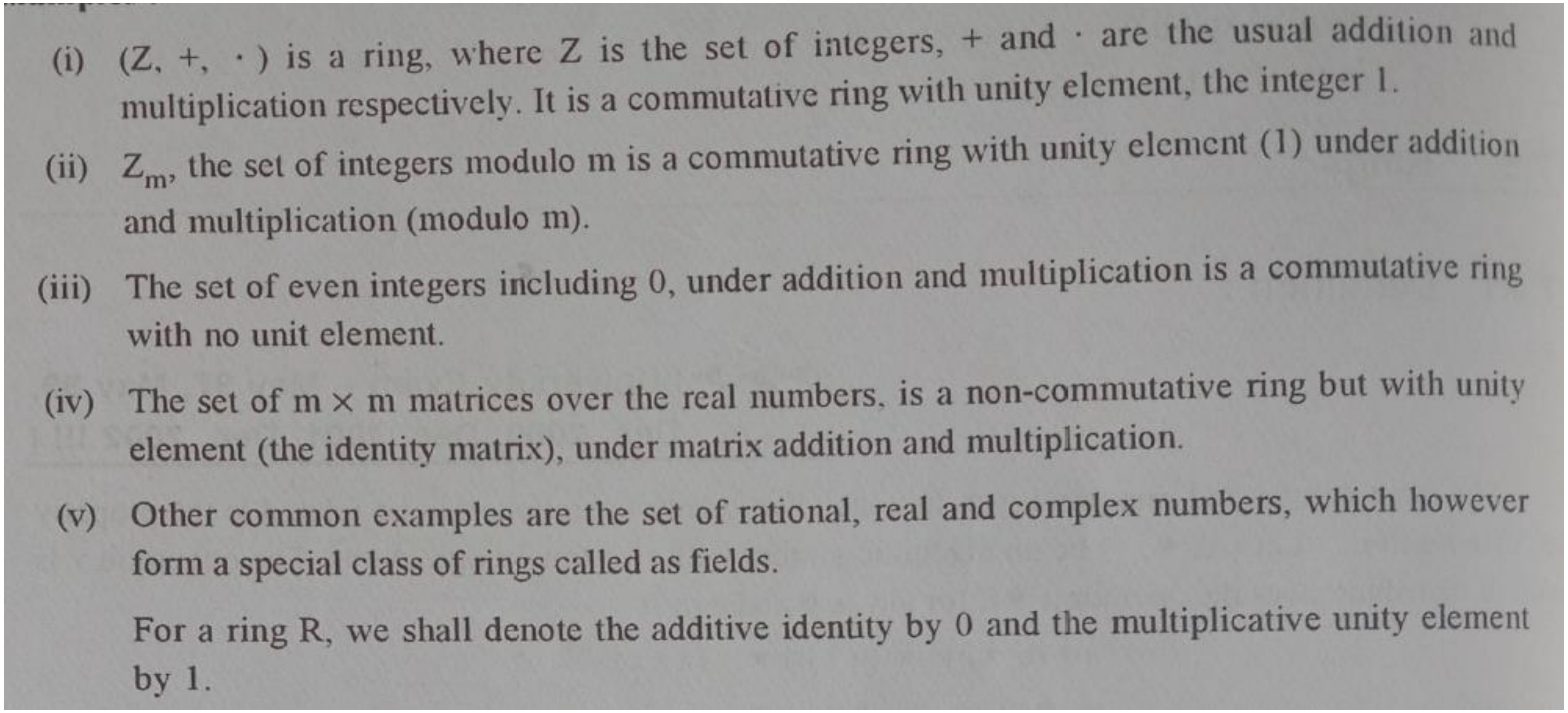
000000	001100	010011	011111	100101	101001	110110	111010
000001	001101	010010	011110	100100	101000	110111	111011
000010	001110	010001	011101	100111	101011	110100	111000
000100	001000	010111	011011	100001	101101	110010	111110
010000	011100	000011	001111	110101	111001	100110	101010
100000	101100	110011	111111	000101	001001	010110	011010
001010	000110	011001	010101	101111	100011	111100	110000
010100	011000	000111	001011	110001	111101	100010	101110

Now, if we receive the word 010101, we first locate it in the *fourth* column of Table 11.5. The word at the top of the fourth column is 011111. Since $e(011) = 011111$, we decode 010101 as 011. ♦

Types of Rings

1. **Commutative Ring**: A ring (R, +, .) is said to be commutative when a.b = b.a for all a,b ∈ R.
2. **Rings with unity element:** A ring (R, +, .) is said to be a ring with unity element if there exists an element, denoted by the symbol 1 such that a.1 = 1.a = a for all a ∈ R.

Examples:



(i) (Z, +, ·) is a ring, where Z is the set of integers, + and · are the usual addition and multiplication respectively. It is a commutative ring with unity element, the integer 1.

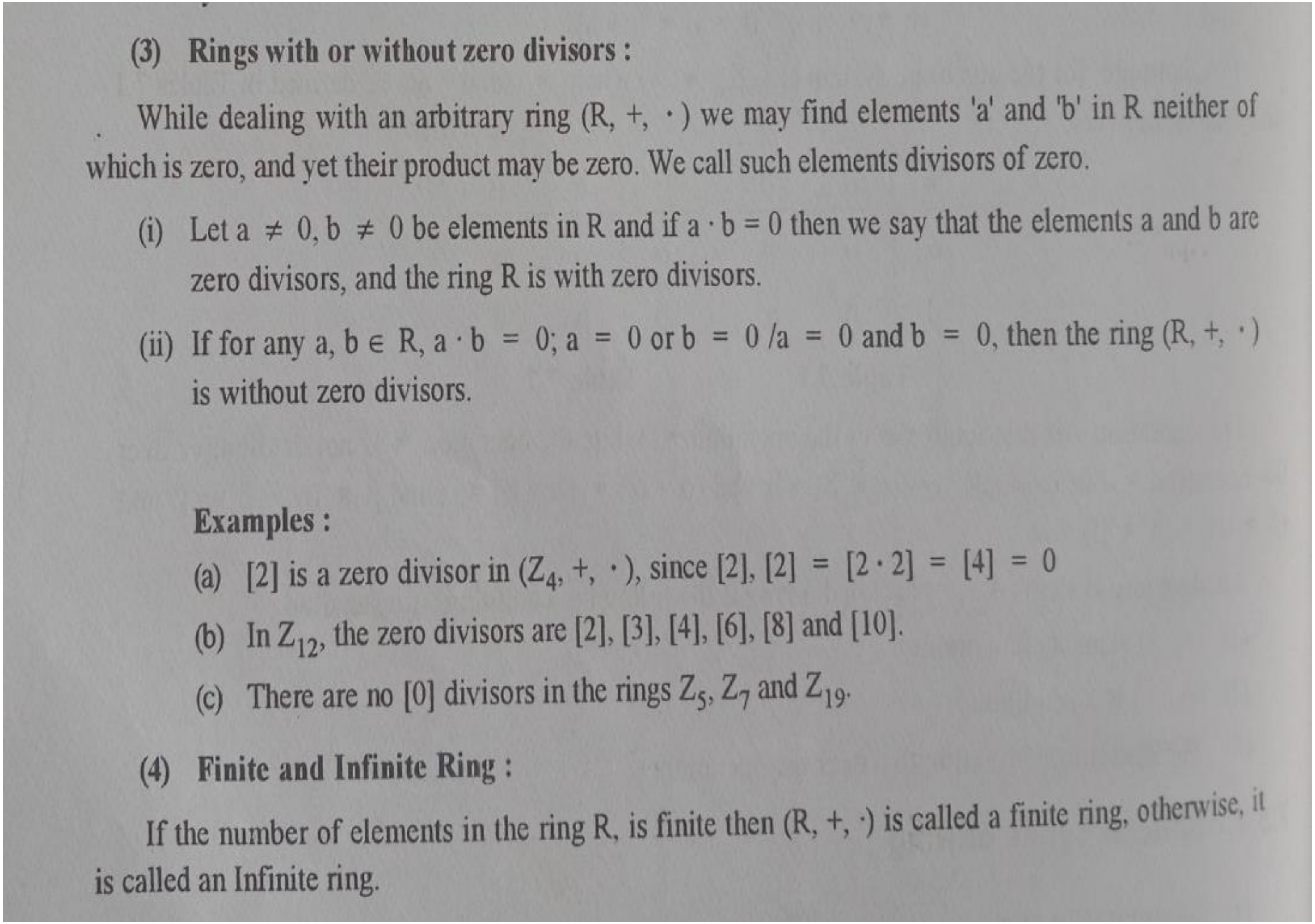
(ii) Z_m, the set of integers modulo m is a commutative ring with unity element (1) under addition and multiplication (modulo m).

(iii) The set of even integers including 0, under addition and multiplication is a commutative ring with no unit element.

(iv) The set of m × m matrices over the real numbers, is a non-commutative ring but with unity element (the identity matrix), under matrix addition and multiplication.

(v) Other common examples are the set of rational, real and complex numbers, which however form a special class of rings called as fields.

For a ring R, we shall denote the additive identity by 0 and the multiplicative unity element by 1.



(3) Rings with or without zero divisors :

While dealing with an arbitrary ring (R, +, ·) we may find elements 'a' and 'b' in R neither of which is zero, and yet their product may be zero. We call such elements divisors of zero.

(i) Let $a \neq 0, b \neq 0$ be elements in R and if $a \cdot b = 0$ then we say that the elements a and b are zero divisors, and the ring R is with zero divisors.

(ii) If for any $a, b \in R$, $a \cdot b = 0$; $a = 0$ or $b = 0$ /$a = 0$ and $b = 0$, then the ring (R, +, ·) is without zero divisors.

Examples :

(a) [2] is a zero divisor in (Z_4, +, ·), since [2], [2] = [2 · 2] = [4] = 0

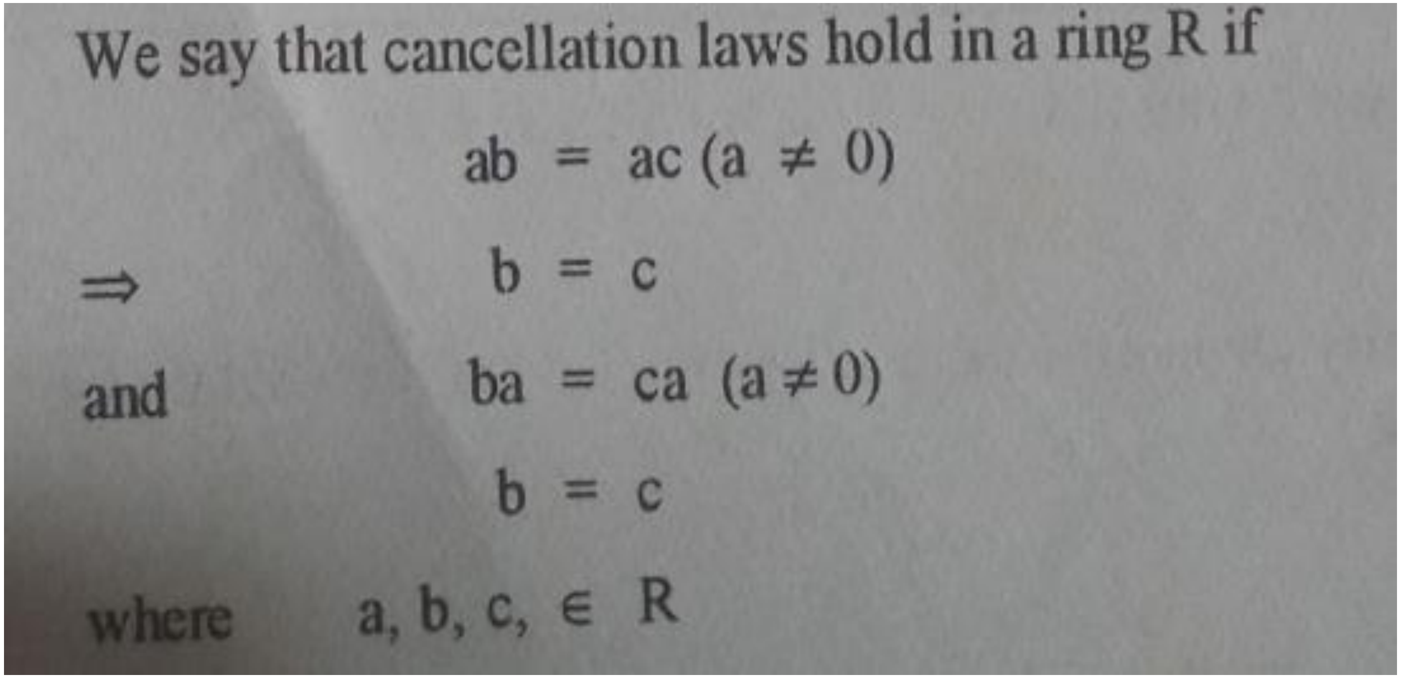
(b) In Z_{12}, the zero divisors are [2], [3], [4], [6], [8] and [10].

(c) There are no [0] divisors in the rings Z_5, Z_7 and Z_{19}.

(4) Finite and Infinite Ring :

If the number of elements in the ring R, is finite then (R, +, ·) is called a finite ring, otherwise, it is called an Infinite ring.

Cancellation Laws in a Ring



We say that cancellation laws hold in a ring R if

$$ab = ac \quad (a \neq 0)$$

$$\Rightarrow \qquad b = c$$

and $$ba = ca \quad (a \neq 0)$$

$$b = c$$

where $a, b, c, \in R$

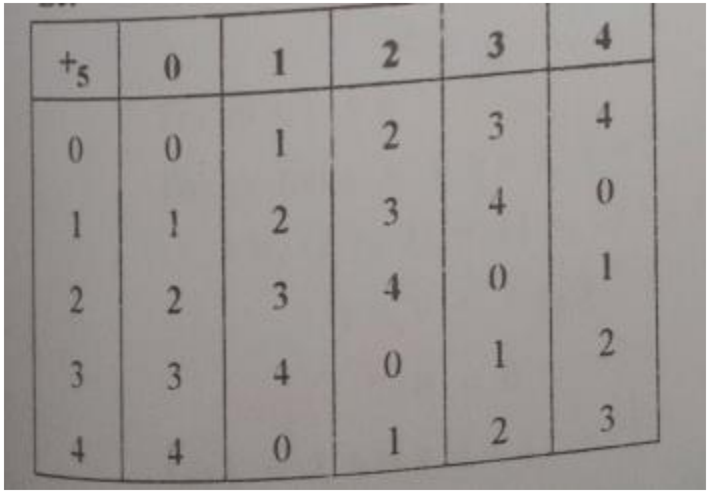
SUBRINGS

- Analogous to the concept of subgroup of a group, this is that of a subring of a ring.
- Let (R, +, ·) be a ring and S be a non-empty subset of R. If (S, +, ·) is called a subring of R.
- Let (S, +, ·) be a subring of (R, +, ·), where R is a ring with identity element 1. If 1 ∊ S, then **S is called a Unitary Subring of R** and **the ring is said to be Unitary over ring (S, +, ·)**
- **For Example:**
  - The ring of even integers is a subring of the ring of integers. More generally, for any positive integer n, the set, nZ = {n m|m ∈ Z} is a subring of Z
  - The set of rationals is a subring of the ring of real numbers.

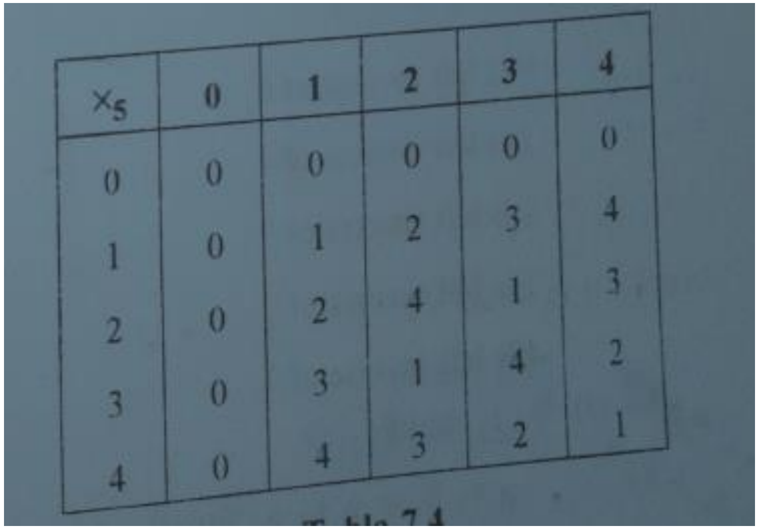
EXAMPLES

Q1. Show that the set {0, 1, 2, 3, 4} is a ring w.r.t addition and multiplication mod 5.

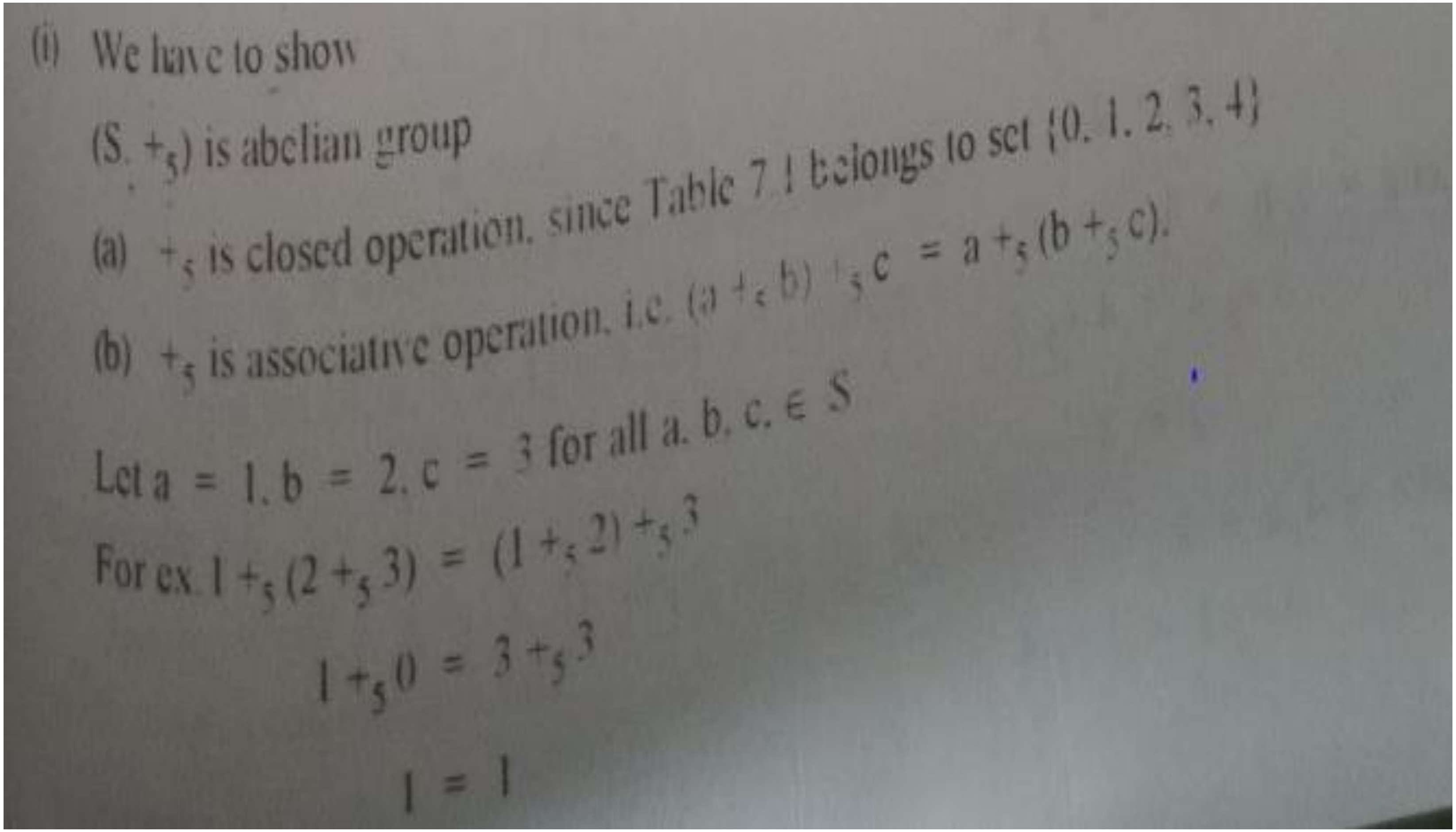
Soln: Let S = {0, 1, 2, 3, 4}



$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3



$\times_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1



(i) We have to show

$(S, +_5)$ is abelian group

(a) $+_5$ is closed operation, since Table 7.1 belongs to set $\{0, 1, 2, 3, 4\}$

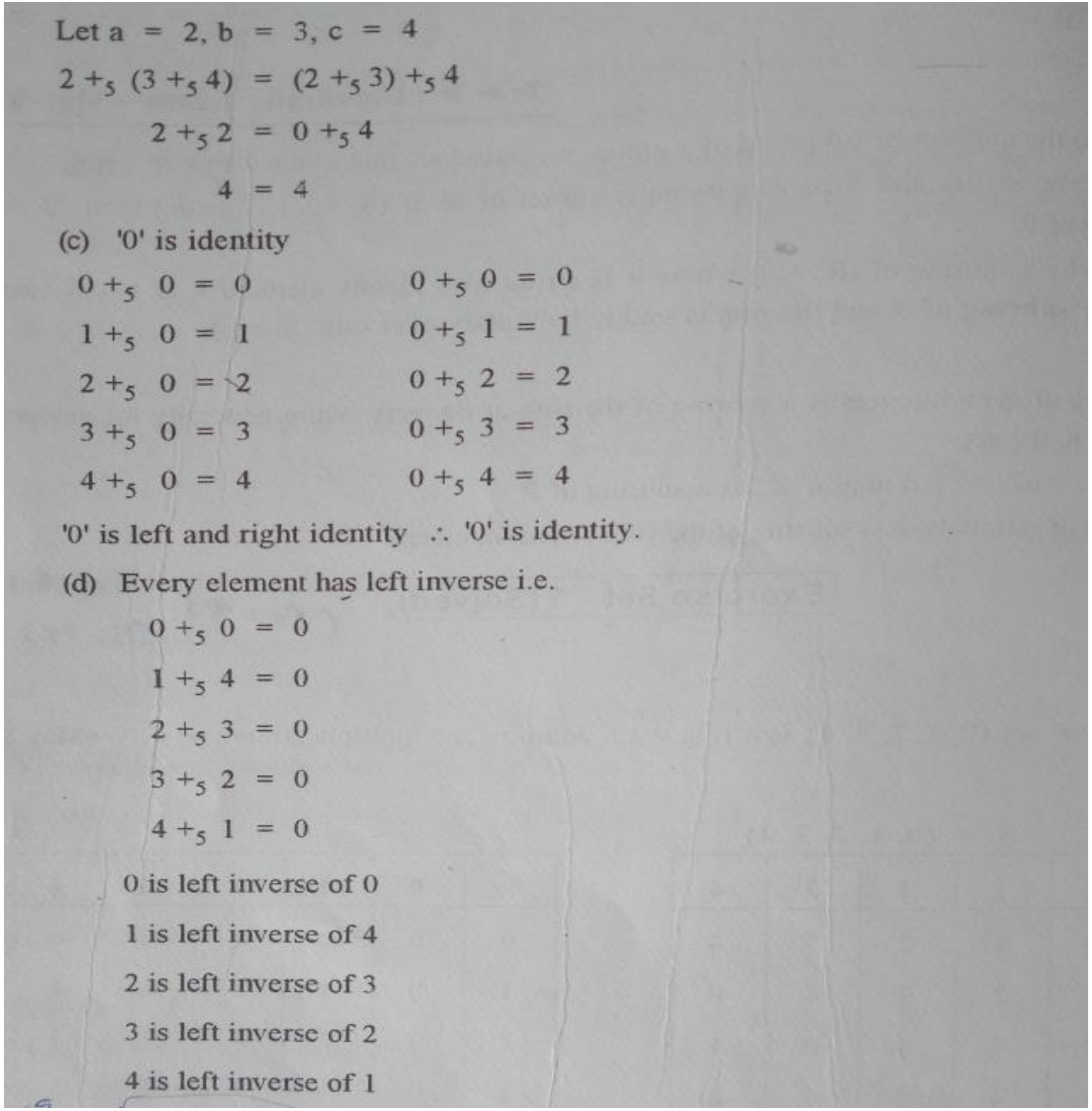
(b) $+_5$ is associative operation, i.e. $(a +_5 b) +_5 c = a +_5 (b +_5 c)$.

Let $a = 1, b = 2, c = 3$ for all $a, b, c, \in S$

For ex. $1 +_5 (2 +_5 3) = (1 +_5 2) +_5 3$

$$1 +_5 0 = 3 +_5 3$$

$$1 = 1$$



Let a = 2, b = 3, c = 4

$$2 +_5 (3 +_5 4) = (2 +_5 3) +_5 4$$

$$2 +_5 2 = 0 +_5 4$$

$$4 = 4$$

(c) '0' is identity

$0 +_5 0 = 0$ $\qquad$ $0 +_5 0 = 0$

$1 +_5 0 = 1$ $\qquad$ $0 +_5 1 = 1$

$2 +_5 0 = 2$ $\qquad$ $0 +_5 2 = 2$

$3 +_5 0 = 3$ $\qquad$ $0 +_5 3 = 3$

$4 +_5 0 = 4$ $\qquad$ $0 +_5 4 = 4$

'0' is left and right identity $\therefore$ '0' is identity.

(d) Every element has left inverse i.e.

$$0 +_5 0 = 0$$

$$1 +_5 4 = 0$$

$$2 +_5 3 = 0$$

$$3 +_5 2 = 0$$

$$4 +_5 1 = 0$$

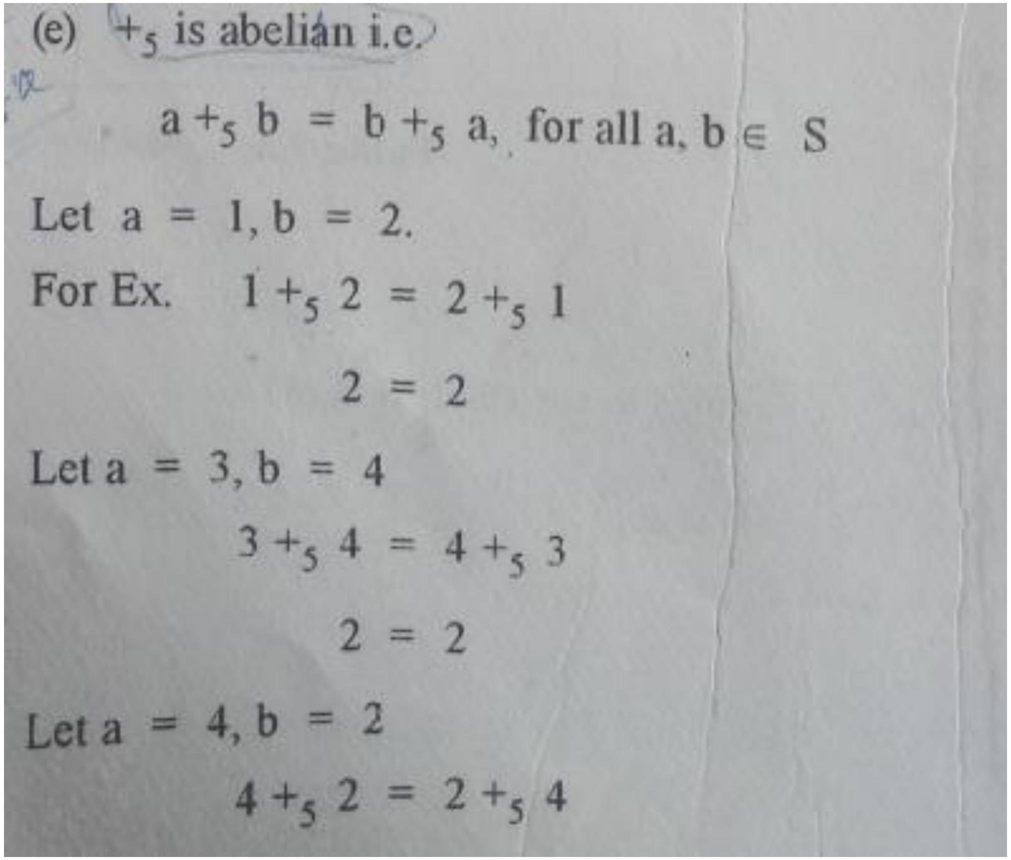
0 is left inverse of 0

1 is left inverse of 4

2 is left inverse of 3

3 is left inverse of 2

4 is left inverse of 1



(e) $+_5$ is abelian i.e.

$$a +_5 b = b +_5 a, \text{ for all } a, b \in S$$

Let $a = 1, b = 2.$

For Ex. $1 +_5 2 = 2 +_5 1$

$$2 = 2$$

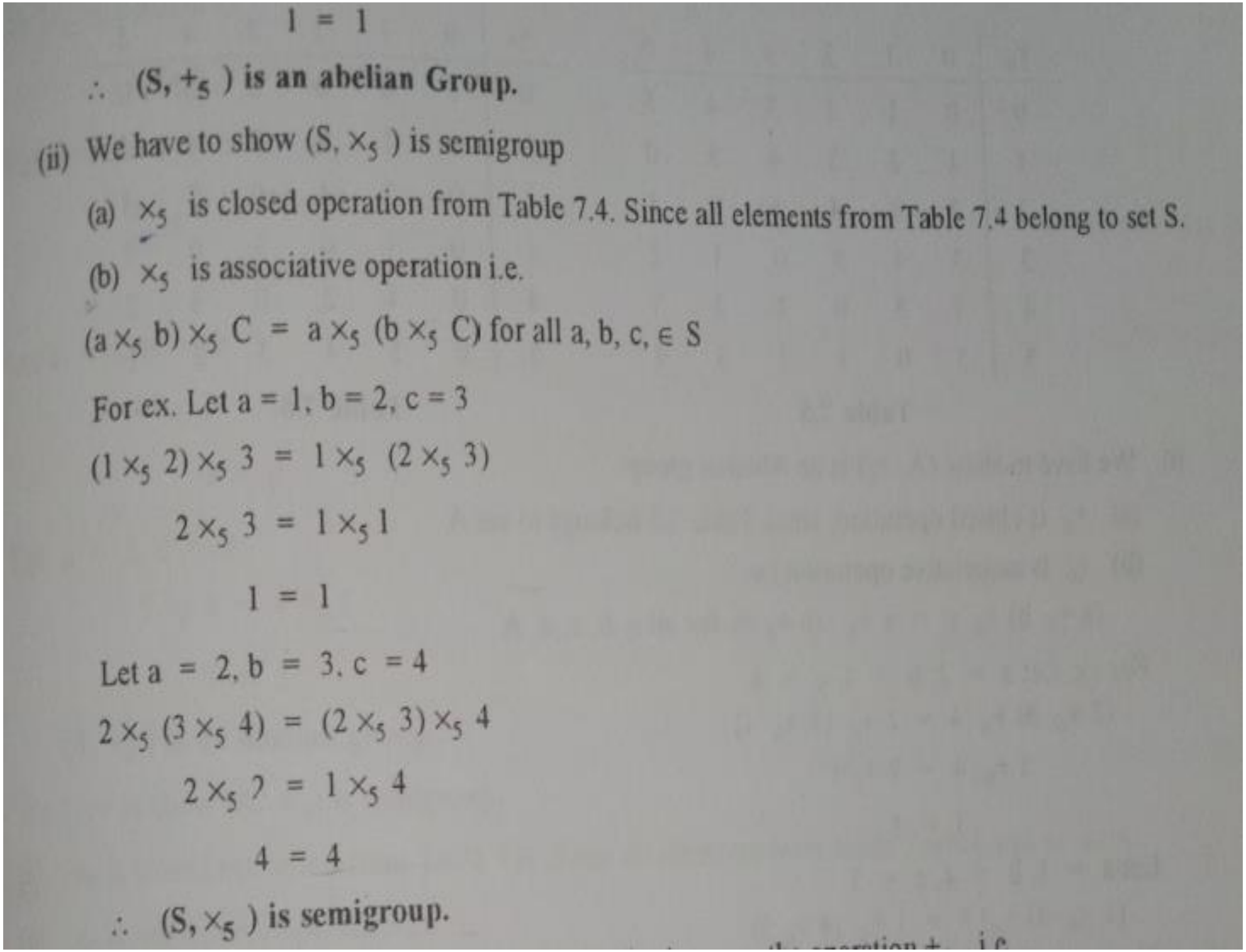
Let $a = 3, b = 4$

$$3 +_5 4 = 4 +_5 3$$

$$2 = 2$$

Let $a = 4, b = 2$

$$4 +_5 2 = 2 +_5 4$$



$1 = 1$

∴ **$(S, +_5)$ is an abelian Group.**

(ii) We have to show $(S, \times_5)$ is semigroup

(a) $\times_5$ is closed operation from Table 7.4. Since all elements from Table 7.4 belong to set S.

(b) $\times_5$ is associative operation i.e.

$(a \times_5 b) \times_5 C = a \times_5 (b \times_5 C)$ for all a, b, c, $\in$ S

For ex. Let a = 1, b = 2, c = 3

$(1 \times_5 2) \times_5 3 = 1 \times_5 (2 \times_5 3)$

$2 \times_5 3 = 1 \times_5 1$

$1 = 1$

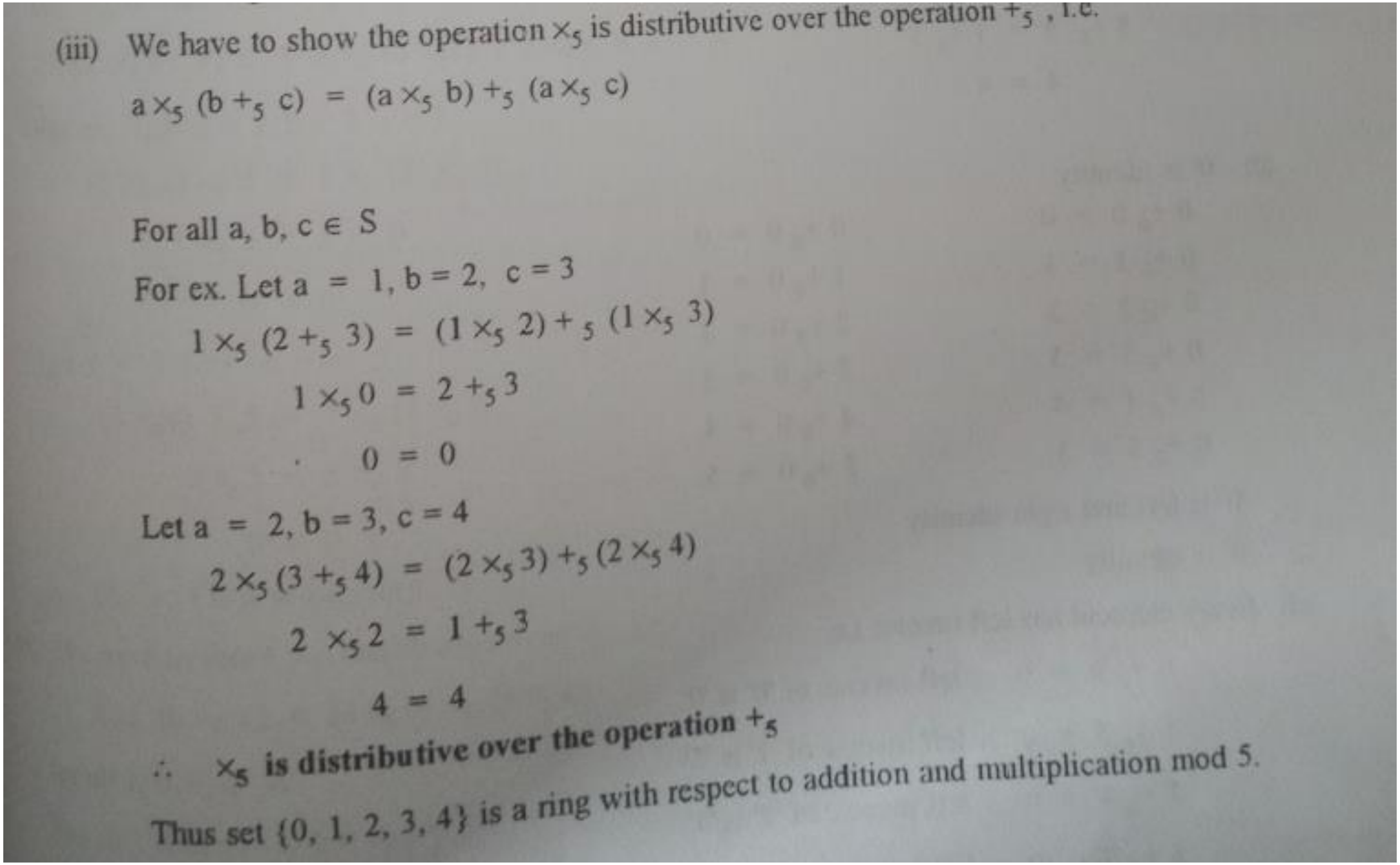
Let a = 2, b = 3, c = 4

$2 \times_5 (3 \times_5 4) = (2 \times_5 3) \times_5 4$

$2 \times_5 2 = 1 \times_5 4$

$4 = 4$

∴ **$(S, \times_5)$ is semigroup.**



(iii) We have to show the operation $\times_5$ is distributive over the operation $+_5$, i.e.

$a \times_5 (b +_5 c) = (a \times_5 b) +_5 (a \times_5 c)$

For all a, b, c ∈ S

For ex. Let a = 1, b = 2, c = 3

$1 \times_5 (2 +_5 3) = (1 \times_5 2) +_5 (1 \times_5 3)$

$1 \times_5 0 = 2 +_5 3$

$0 = 0$

Let a = 2, b = 3, c = 4

$2 \times_5 (3 +_5 4) = (2 \times_5 3) +_5 (2 \times_5 4)$

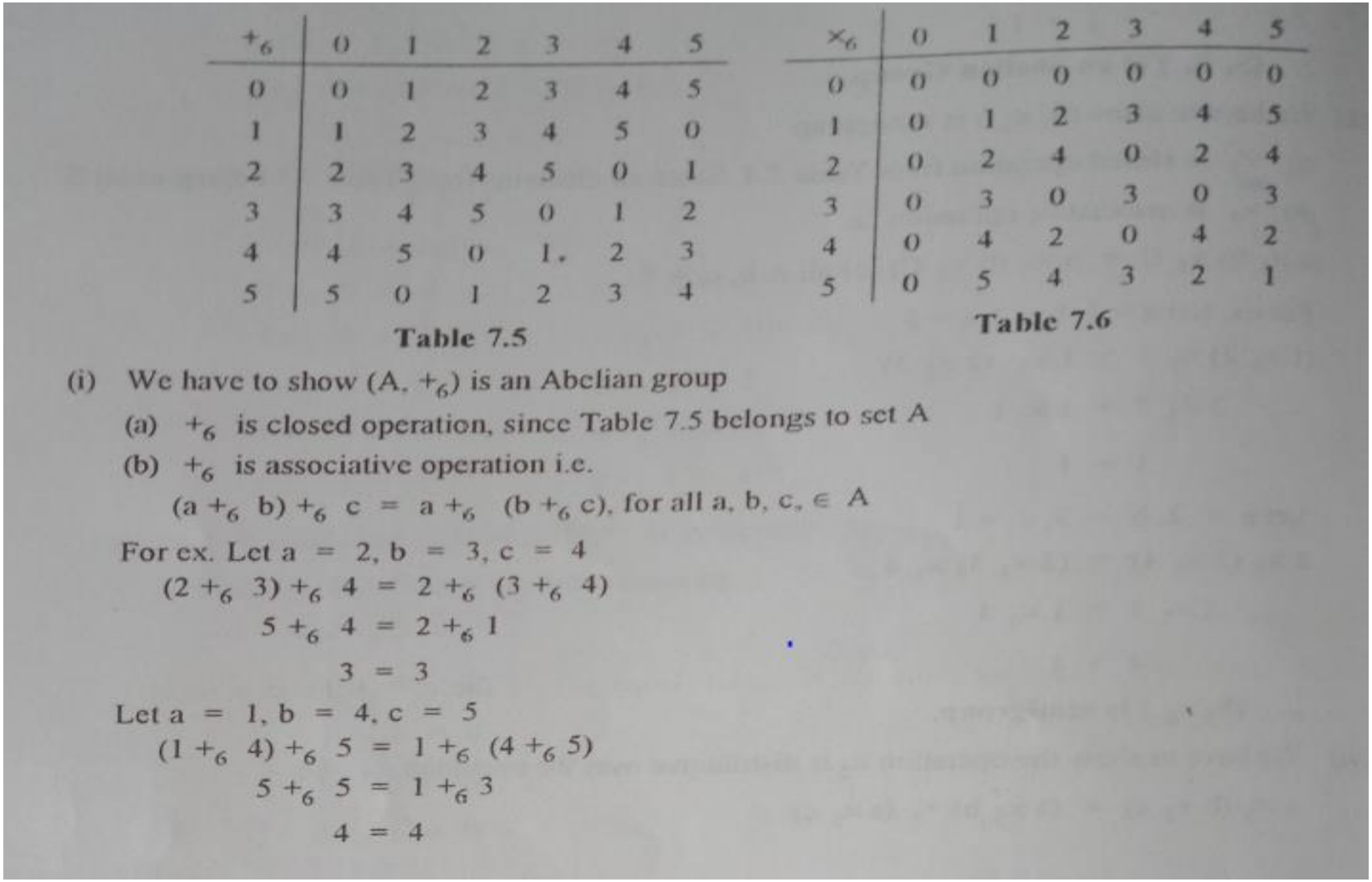
$2 \times_5 2 = 1 +_5 3$

$4 = 4$

∴ $\times_5$ **is distributive over the operation** $+_5$

Thus set {0, 1, 2, 3, 4} is a ring with respect to addition and multiplication mod 5.

Q2. Show that A = {0, 1, 2, 3, 4, 5} together addition modulo 6 and multiplication modulo 6 is a commutative ring.



$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Table 7.5

$\times_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Table 7.6

(i) We have to show $(A, +_6)$ is an Abelian group

(a) $+_6$ is closed operation, since Table 7.5 belongs to set A

(b) $+_6$ is associative operation i.e.

$(a +_6 b) +_6 c = a +_6 (b +_6 c)$, for all a, b, c, $\in$ A

For ex. Let a = 2, b = 3, c = 4

$(2 +_6 3) +_6 4 = 2 +_6 (3 +_6 4)$

$5 +_6 4 = 2 +_6 1$

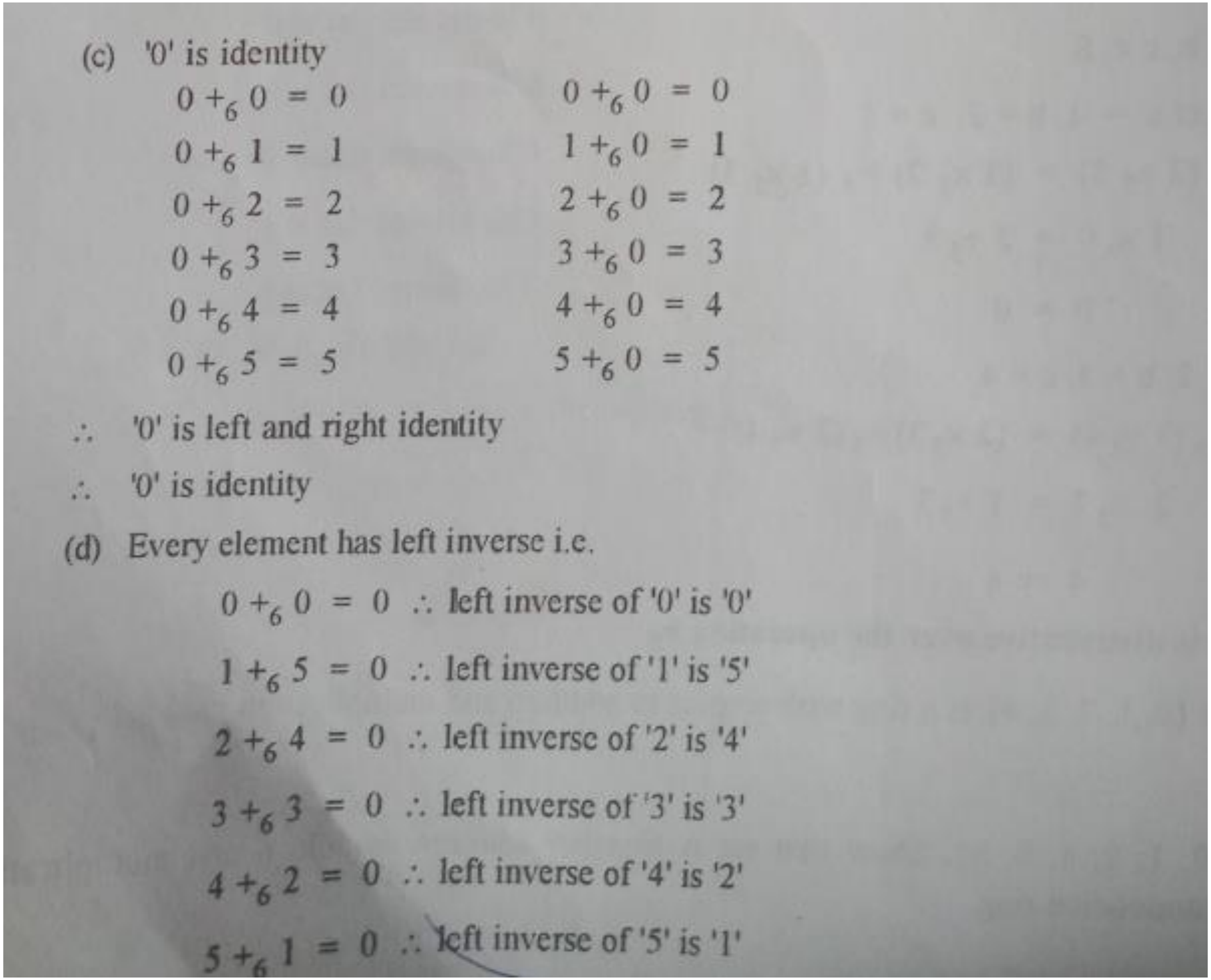
$3 = 3$

Let a = 1, b = 4, c = 5

$(1 +_6 4) +_6 5 = 1 +_6 (4 +_6 5)$

$5 +_6 5 = 1 +_6 3$

$4 = 4$



(c) '0' is identity

$$\begin{array}{lcl} 0 +_6 0 = 0 & \qquad & 0 +_6 0 = 0 \\ 0 +_6 1 = 1 & & 1 +_6 0 = 1 \\ 0 +_6 2 = 2 & & 2 +_6 0 = 2 \\ 0 +_6 3 = 3 & & 3 +_6 0 = 3 \\ 0 +_6 4 = 4 & & 4 +_6 0 = 4 \\ 0 +_6 5 = 5 & & 5 +_6 0 = 5 \end{array}$$

$\therefore$ '0' is left and right identity

$\therefore$ '0' is identity

(d) Every element has left inverse i.e.

$0 +_6 0 = 0$ $\therefore$ left inverse of '0' is '0'

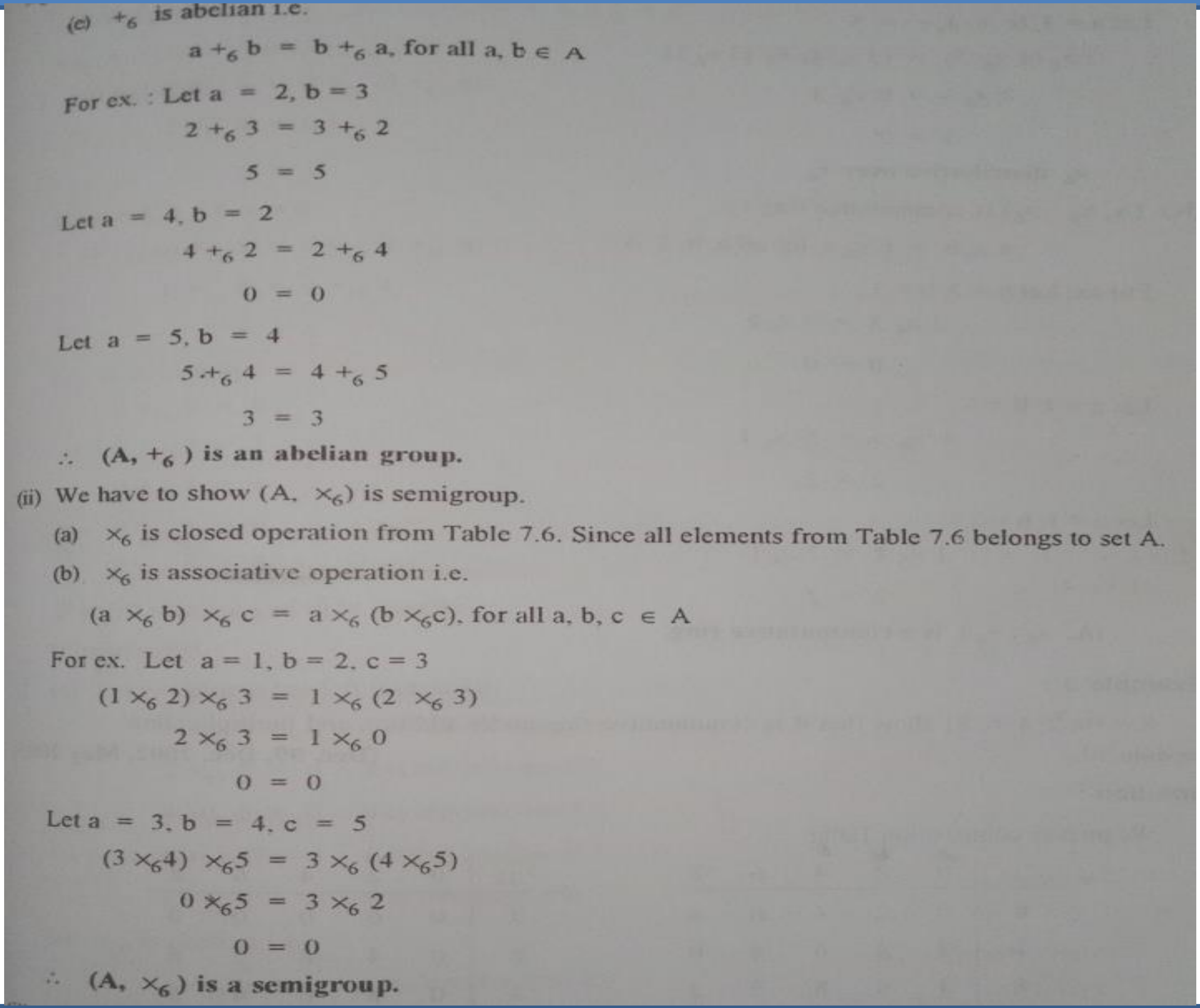
$1 +_6 5 = 0$ $\therefore$ left inverse of '1' is '5'

$2 +_6 4 = 0$ $\therefore$ left inverse of '2' is '4'

$3 +_6 3 = 0$ $\therefore$ left inverse of '3' is '3'

$4 +_6 2 = 0$ $\therefore$ left inverse of '4' is '2'

$5 +_6 1 = 0$ $\therefore$ left inverse of '5' is '1'



(e) $+_6$ is abelian i.e.

$$a +_6 b = b +_6 a, \text{ for all } a, b \in A$$

For ex. : Let a = 2, b = 3

$$2 +_6 3 = 3 +_6 2$$

$$5 = 5$$

Let a = 4, b = 2

$$4 +_6 2 = 2 +_6 4$$

$$0 = 0$$

Let a = 5, b = 4

$$5 +_6 4 = 4 +_6 5$$

$$3 = 3$$

$\therefore$ **(A, $+_6$) is an abelian group.**

(ii) We have to show (A, $\times_6$) is semigroup.

(a) $\times_6$ is closed operation from Table 7.6. Since all elements from Table 7.6 belongs to set A.

(b) $\times_6$ is associative operation i.e.

$$(a \times_6 b) \times_6 c = a \times_6 (b \times_6 c), \text{ for all } a, b, c \in A$$

For ex. Let a = 1, b = 2, c = 3

$$(1 \times_6 2) \times_6 3 = 1 \times_6 (2 \times_6 3)$$

$$2 \times_6 3 = 1 \times_6 0$$

$$0 = 0$$

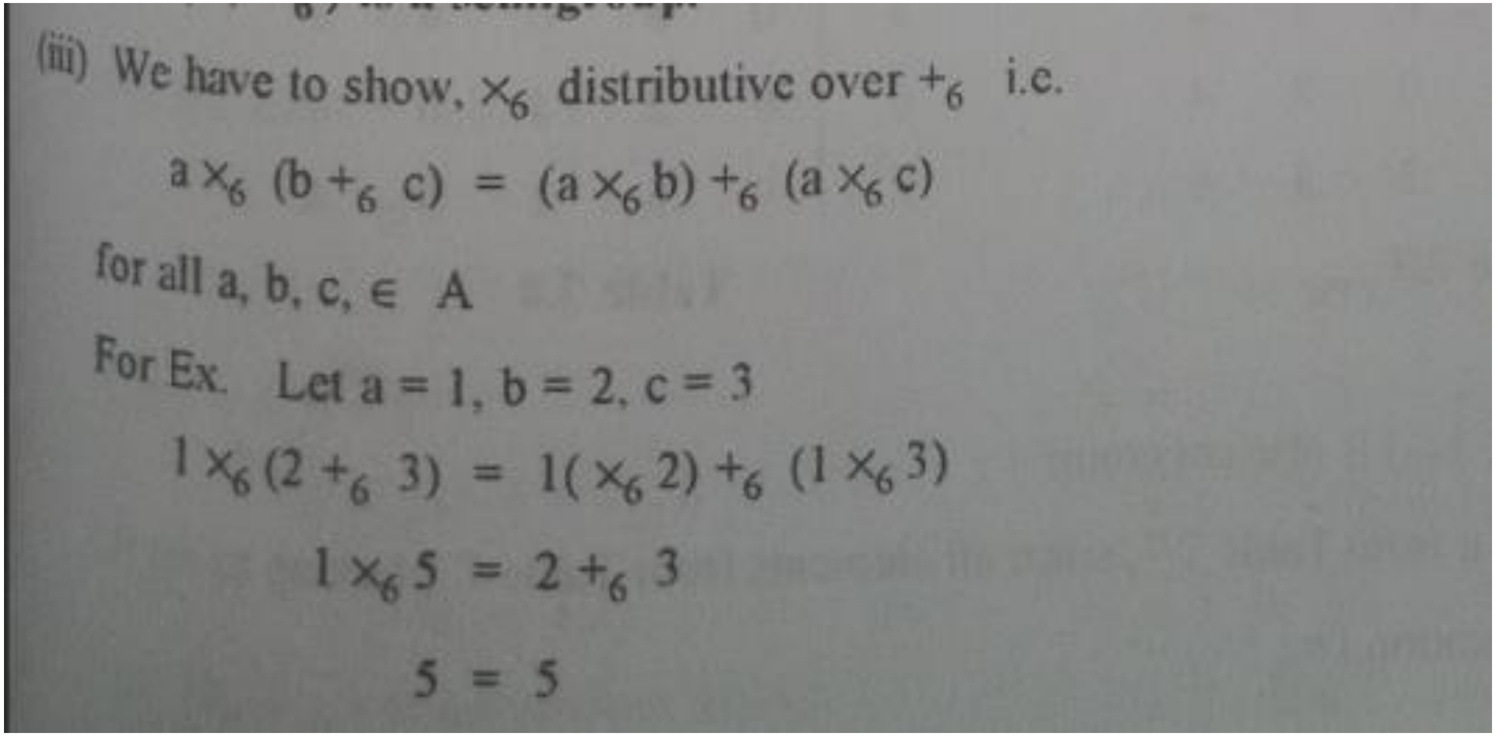
Let a = 3, b = 4, c = 5

$$(3 \times_6 4) \times_6 5 = 3 \times_6 (4 \times_6 5)$$

$$0 \times_6 5 = 3 \times_6 2$$

$$0 = 0$$

$\therefore$ **(A, $\times_6$) is a semigroup.**



$_6$) is a semigroup.

(iii) We have to show, $\times_6$ distributive over $+_6$ i.c.

$$a \times_6 (b +_6 c) = (a \times_6 b) +_6 (a \times_6 c)$$

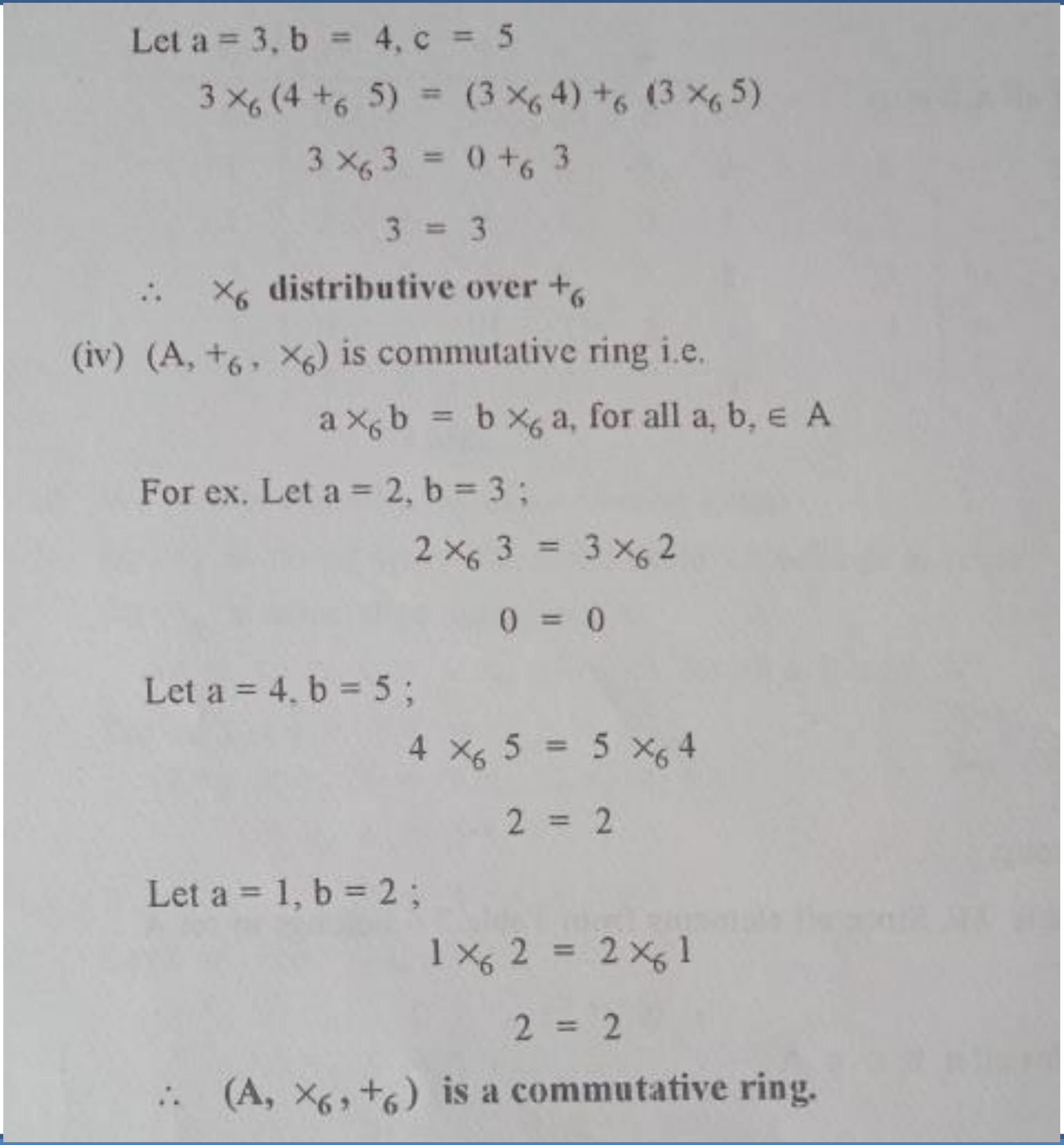
for all a, b, c, ∈ A

For Ex. Let a = 1, b = 2, c = 3

$$1 \times_6 (2 +_6 3) = 1(\times_6 2) +_6 (1 \times_6 3)$$

$$1 \times_6 5 = 2 +_6 3$$

$$5 = 5$$



Let a = 3, b = 4, c = 5

$$3 \times_6 (4 +_6 5) = (3 \times_6 4) +_6 (3 \times_6 5)$$

$$3 \times_6 3 = 0 +_6 3$$

$$3 = 3$$

$\therefore$ $\times_6$ **distributive over** $+_6$

(iv) $(A, +_6, \times_6)$ is commutative ring i.e.

$$a \times_6 b = b \times_6 a, \text{ for all } a, b, \in A$$

For ex. Let a = 2, b = 3 ;

$$2 \times_6 3 = 3 \times_6 2$$

$$0 = 0$$

Let a = 4, b = 5 ;

$$4 \times_6 5 = 5 \times_6 4$$

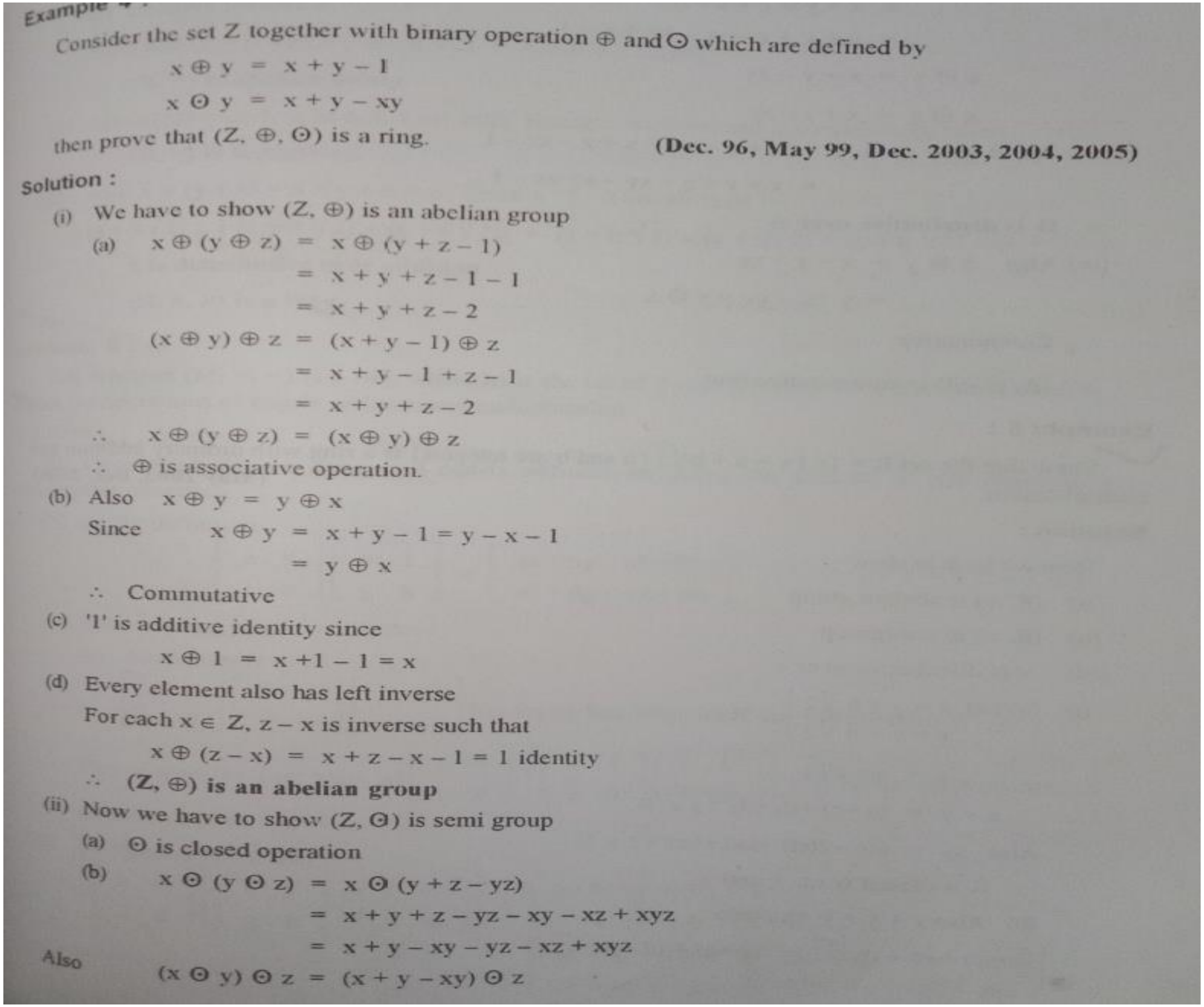
$$2 = 2$$

Let a = 1, b = 2 ;

$$1 \times_6 2 = 2 \times_6 1$$

$$2 = 2$$

$\therefore$ **$(A, \times_6, +_6)$ is a commutative ring.**



Example

Consider the set Z together with binary operation $\oplus$ and $\odot$ which are defined by

$$x \oplus y = x + y - 1$$

$$x \odot y = x + y - xy$$

then prove that $(Z, \oplus, \odot)$ is a ring. **(Dec. 96, May 99, Dec. 2003, 2004, 2005)**

Solution :

(i) We have to show $(Z, \oplus)$ is an abelian group

(a)
$$\begin{aligned} x \oplus (y \oplus z) &= x \oplus (y + z - 1) \\ &= x + y + z - 1 - 1 \\ &= x + y + z - 2 \\ (x \oplus y) \oplus z &= (x + y - 1) \oplus z \\ &= x + y - 1 + z - 1 \\ &= x + y + z - 2 \end{aligned}$$

$\therefore$ $x \oplus (y \oplus z) = (x \oplus y) \oplus z$

$\therefore$ $\oplus$ is associative operation.

(b) Also $x \oplus y = y \oplus x$

Since
$$\begin{aligned} x \oplus y &= x + y - 1 = y - x - 1 \\ &= y \oplus x \end{aligned}$$

$\therefore$ Commutative

(c) '1' is additive identity since

$$x \oplus 1 = x + 1 - 1 = x$$

(d) Every element also has left inverse

For each $x \in Z$, $z - x$ is inverse such that

$$x \oplus (z - x) = x + z - x - 1 = 1 \text{ identity}$$

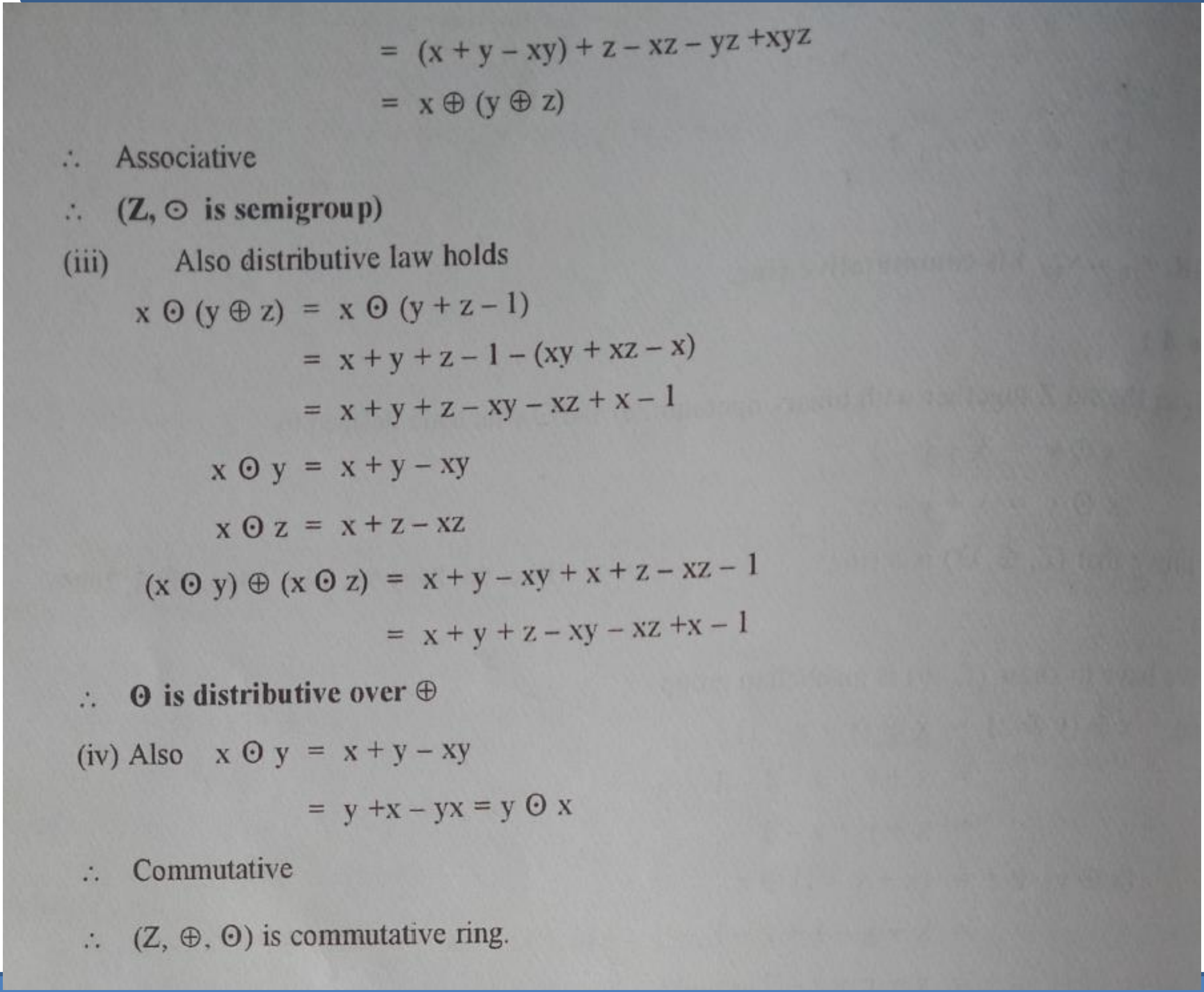
$\therefore$ **$(Z, \oplus)$ is an abelian group**

(ii) Now we have to show $(Z, \odot)$ is semi group

(a) $\odot$ is closed operation

(b)
$$\begin{aligned} x \odot (y \odot z) &= x \odot (y + z - yz) \\ &= x + y + z - yz - xy - xz + xyz \\ &= x + y - xy - yz - xz + xyz \end{aligned}$$

Also
$$(x \odot y) \odot z = (x + y - xy) \odot z$$



$$= (x + y - xy) + z - xz - yz + xyz$$

$$= x \oplus (y \oplus z)$$

∴ Associative

∴ **(Z, ⊙ is semigroup)**

(iii) Also distributive law holds

$$x \odot (y \oplus z) = x \odot (y + z - 1)$$

$$= x + y + z - 1 - (xy + xz - x)$$

$$= x + y + z - xy - xz + x - 1$$

$$x \odot y = x + y - xy$$

$$x \odot z = x + z - xz$$

$$(x \odot y) \oplus (x \odot z) = x + y - xy + x + z - xz - 1$$

$$= x + y + z - xy - xz + x - 1$$

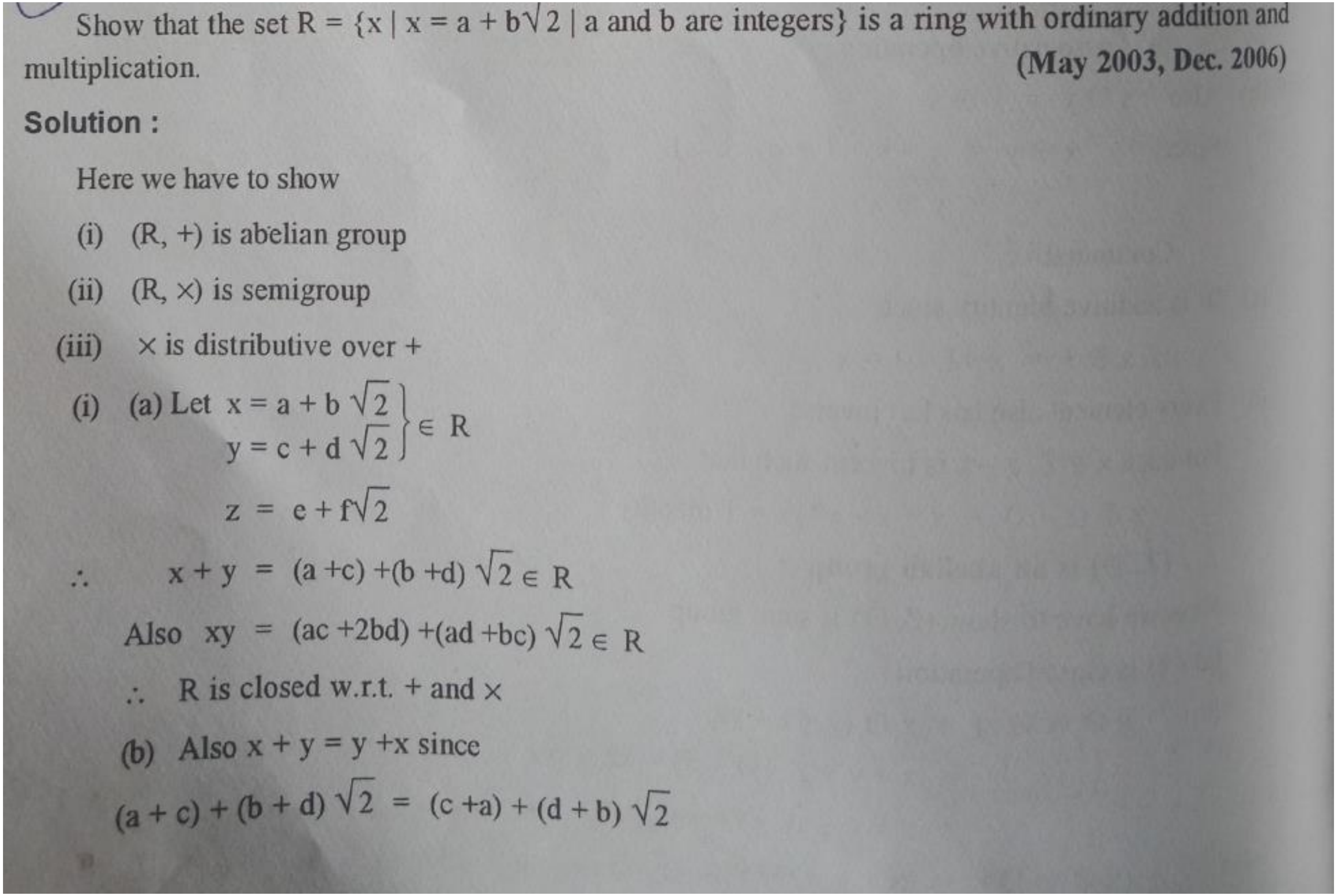
∴ **⊙ is distributive over ⊕**

(iv) Also $x \odot y = x + y - xy$

$$= y + x - yx = y \odot x$$

∴ Commutative

∴ (Z, ⊕, ⊙) is commutative ring.



Show that the set $R = \{x \mid x = a + b\sqrt{2} \mid a$ and b are integers$\}$ is a ring with ordinary addition and multiplication. **(May 2003, Dec. 2006)**

Solution :

Here we have to show

(i) (R, +) is abelian group

(ii) (R, ×) is semigroup

(iii) × is distributive over +

(i) (a) Let $\left.\begin{array}{l} x = a + b\sqrt{2} \\ y = c + d\sqrt{2} \end{array}\right\} \in R$

$$z = e + f\sqrt{2}$$

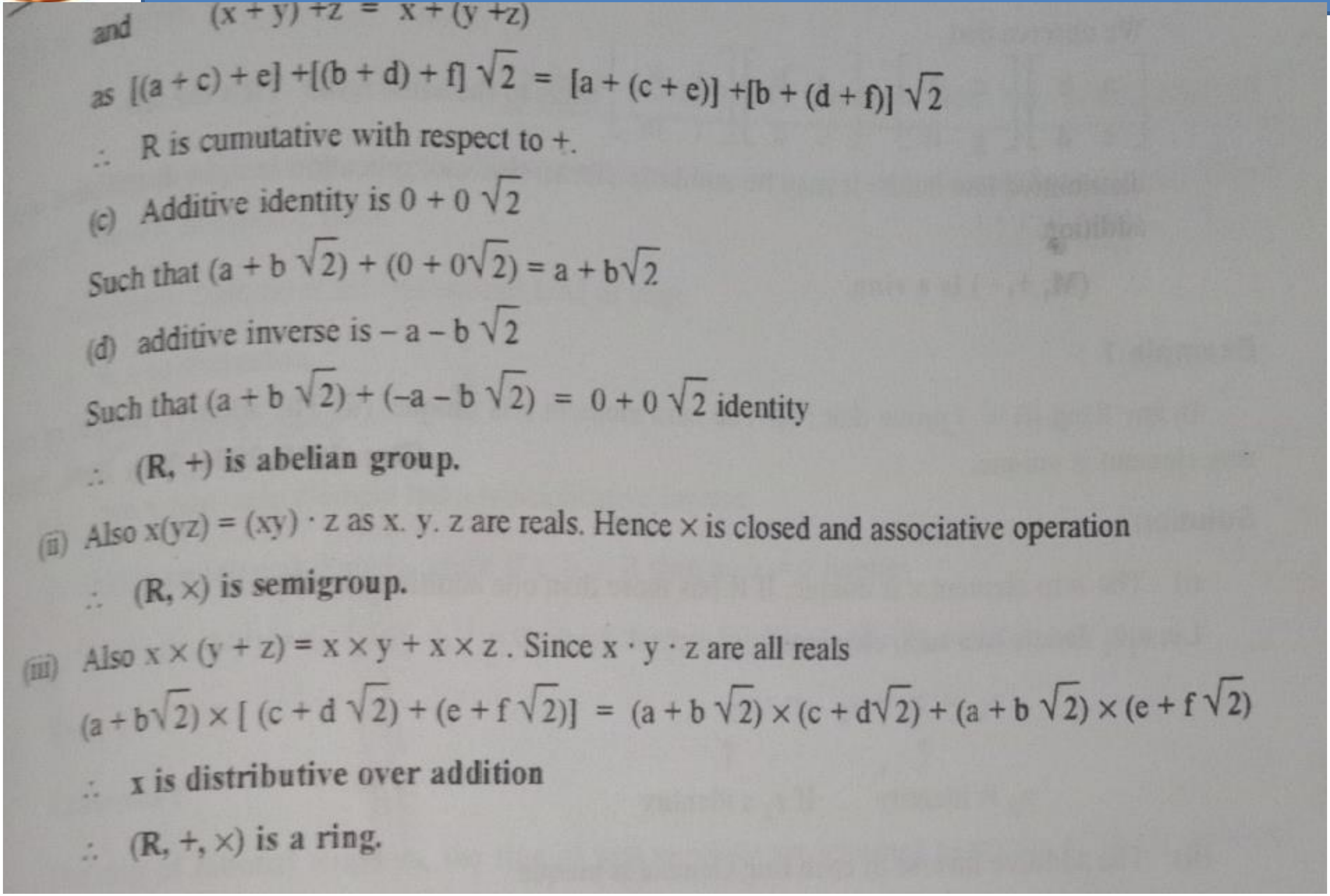
$$\therefore \quad x + y = (a + c) + (b + d)\sqrt{2} \in R$$

Also $xy = (ac + 2bd) + (ad + bc)\sqrt{2} \in R$

$\therefore$ R is closed w.r.t. + and ×

(b) Also $x + y = y + x$ since

$$(a + c) + (b + d)\sqrt{2} = (c + a) + (d + b)\sqrt{2}$$



and $(x + y) + z = x + (y + z)$

as $[(a + c) + e] + [(b + d) + f]\sqrt{2} = [a + (c + e)] + [b + (d + f)]\sqrt{2}$

∴ R is cumutative with respect to +.

(c) Additive identity is $0 + 0\sqrt{2}$

Such that $(a + b\sqrt{2}) + (0 + 0\sqrt{2}) = a + b\sqrt{2}$

(d) additive inverse is $-a - b\sqrt{2}$

Such that $(a + b\sqrt{2}) + (-a - b\sqrt{2}) = 0 + 0\sqrt{2}$ identity

∴ **(R, +) is abelian group.**

(ii) Also $x(yz) = (xy) \cdot z$ as x. y. z are reals. Hence × is closed and associative operation

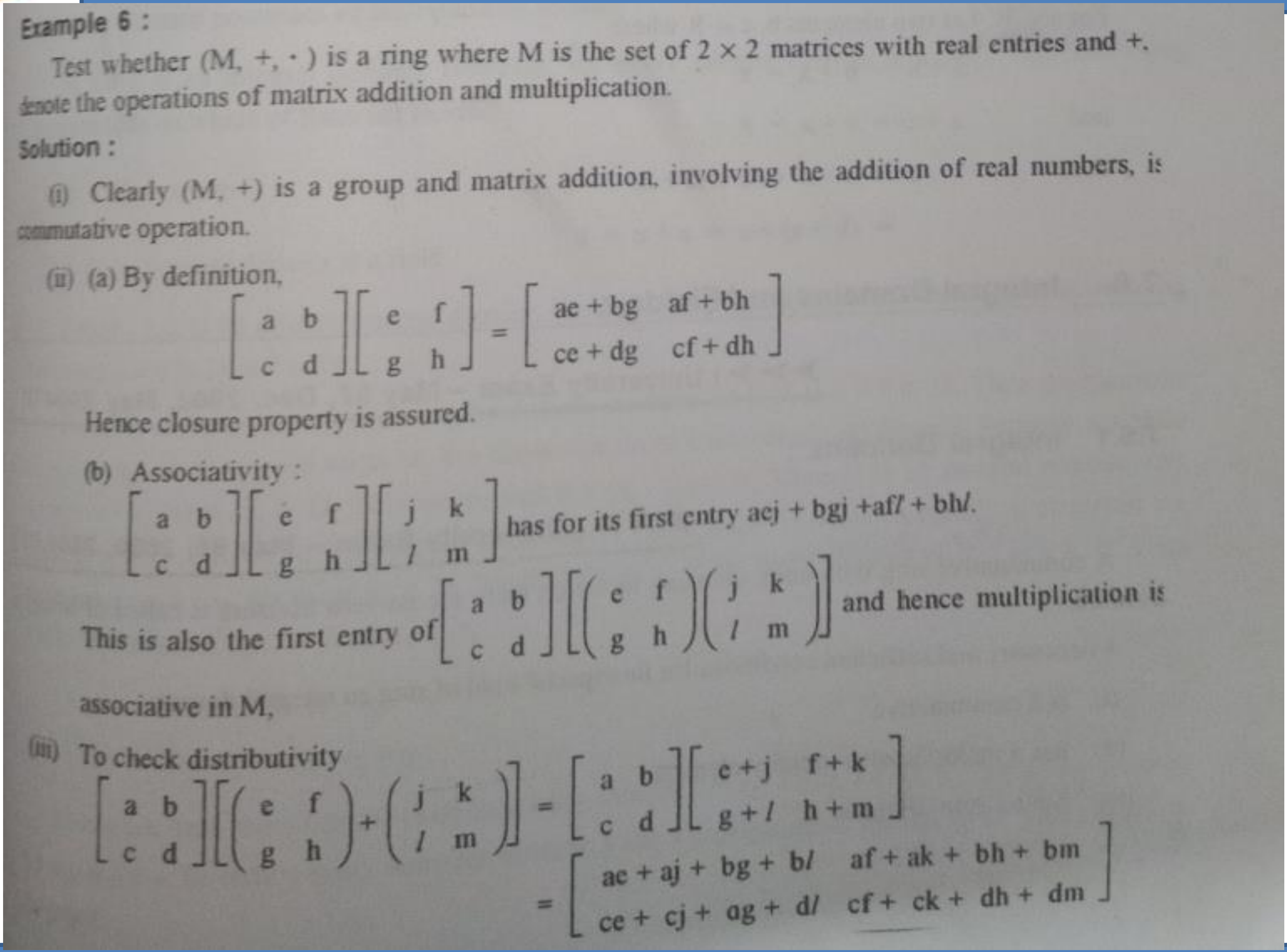
∴ **(R, ×) is semigroup.**

(iii) Also $x \times (y + z) = x \times y + x \times z$. Since $x \cdot y \cdot z$ are all reals

$(a + b\sqrt{2}) \times [(c + d\sqrt{2}) + (e + f\sqrt{2})] = (a + b\sqrt{2}) \times (c + d\sqrt{2}) + (a + b\sqrt{2}) \times (e + f\sqrt{2})$

∴ **x is distributive over addition**

∴ **(R, +, ×) is a ring.**



Example 6 :

Test whether (M, +, ·) is a ring where M is the set of 2 × 2 matrices with real entries and +, · denote the operations of matrix addition and multiplication.

Solution :

(i) Clearly (M, +) is a group and matrix addition, involving the addition of real numbers, is commutative operation.

(ii) (a) By definition,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}$$

Hence closure property is assured.

(b) Associativity :

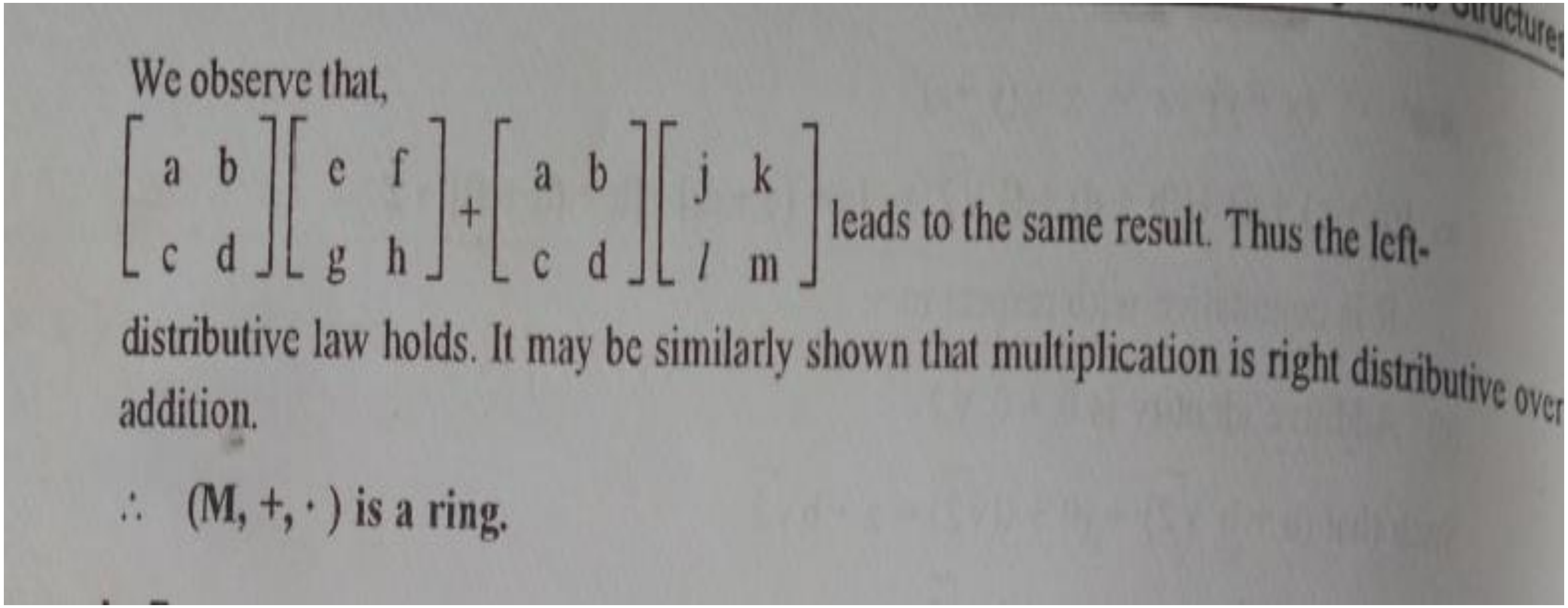
$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} e & f \\ g & h \end{bmatrix}\begin{bmatrix} j & k \\ l & m \end{bmatrix}$ has for its first entry $aej + bgj + afl + bhl$.

This is also the first entry of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}\left[\begin{pmatrix} e & f \\ g & h \end{pmatrix}\begin{pmatrix} j & k \\ l & m \end{pmatrix}\right]$ and hence multiplication is associative in M,

(iii) To check distributivity

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\left[\begin{pmatrix} e & f \\ g & h \end{pmatrix}+\begin{pmatrix} j & k \\ l & m \end{pmatrix}\right] = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} e+j & f+k \\ g+l & h+m \end{bmatrix}$$

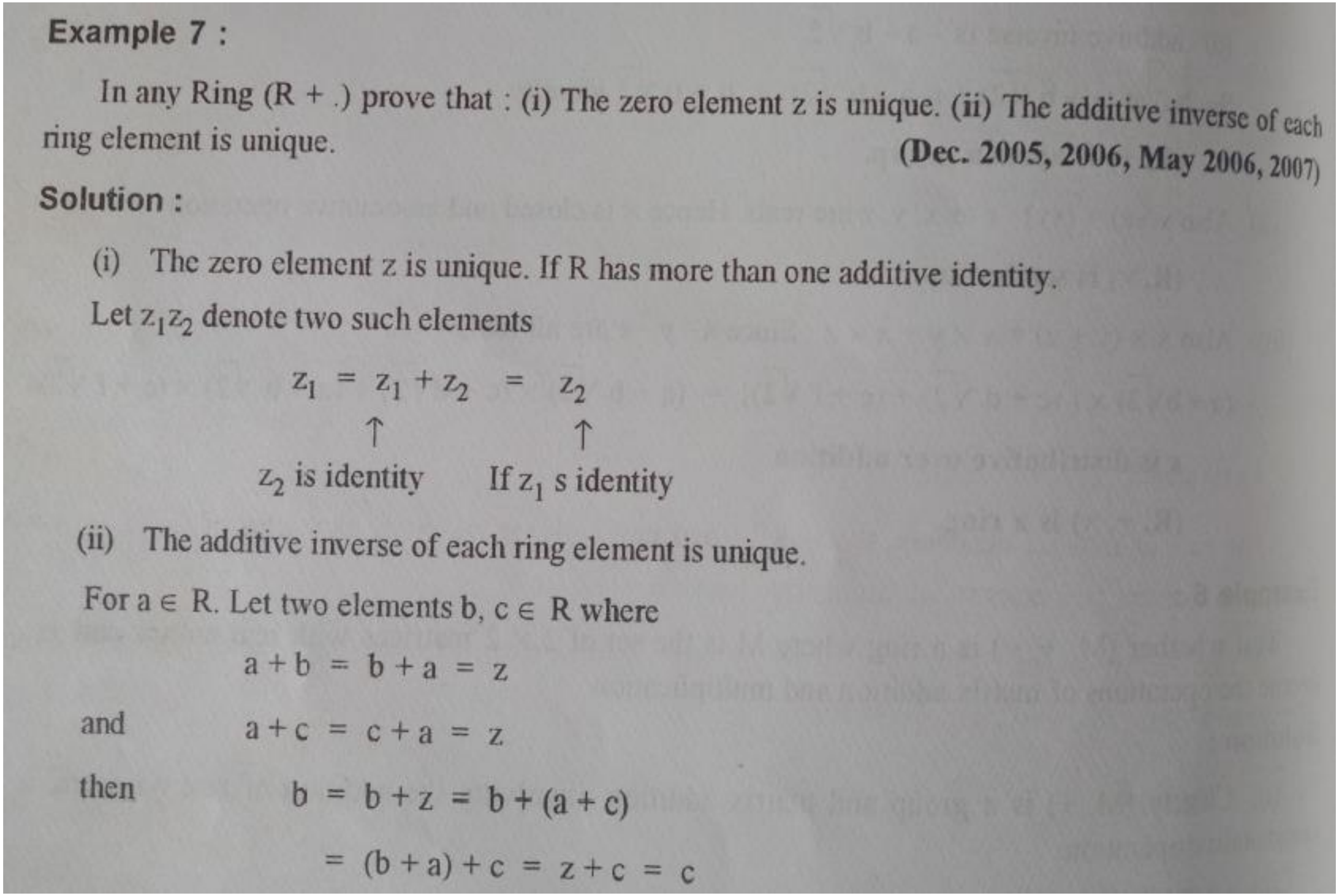
$$= \begin{bmatrix} ae+aj+bg+bl & af+ak+bh+bm \\ ce+cj+ag+dl & cf+ck+dh+dm \end{bmatrix}$$



We observe that,

$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} e & f \\ g & h \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} j & k \\ l & m \end{bmatrix}$ leads to the same result. Thus the left-distributive law holds. It may be similarly shown that multiplication is right distributive over addition.

$\therefore$ (M, +, $\cdot$) is a ring.



Example 7 :

In any Ring (R + .) prove that : (i) The zero element z is unique. (ii) The additive inverse of each ring element is unique.

(Dec. 2005, 2006, May 2006, 2007)

Solution :

(i) The zero element z is unique. If R has more than one additive identity.

Let $z_1 z_2$ denote two such elements

$$z_1 = \underset{\substack{\uparrow \\ z_2 \text{ is identity}}}{z_1 + z_2} = \underset{\substack{\uparrow \\ \text{If } z_1 \text{ s identity}}}{z_2}$$

(ii) The additive inverse of each ring element is unique.

For $a \in$ R. Let two elements $b, c \in$ R where

$$a + b = b + a = z$$

and $$a + c = c + a = z$$

then $$b = b + z = b + (a + c)$$

$$= (b + a) + c = z + c = c$$