

Chapter Three

Let us start by defining the functions that will be used in our discussions. These functions are called binary operations.

A binary operation on a non - empty set A is any function $f : A \times A \rightarrow A$.

It is customary to denote binary operations by a symbol like $+$, $*$, $-$, $\bullet$, Δ , $^\circ$, $\cap$, $\cup$, $\vee$, $\wedge$, etc. and write $x f y$ instead of $f(x, y)$. Thus, if $*$: $A \times A \rightarrow A$, we write $x * y$ instead of $*(x, y)$.

Example 1 The most common binary operations, on $\mathbf{Z}$, are $+$, $\times$, $-$. That is, for instance, $+: \mathbf{Z} \times \mathbf{Z} \rightarrow \mathbf{Z}$ is given by $+(x, y) = x + y$.

Example 2 Let $A = \mathbf{Z} - \{1\}$. Then $*$: $A \times A \rightarrow A$ given by $x * y = x + y - xy$ is a binary operation.

Note that the definition $f: A \times A \rightarrow A$ involves the facts

- a. That f is a function. When this does not hold we say f is not well defined.
For instance on $A=\{1,2,3,4\}$, $x * y = z$ where $z \leq x$ is a relation which is not a function. It gives, among others,
 $*(2,3)=2*3=1$ or 2 . Hence, $*$ is not a binary operation on $A=\{1,2,3,4\}$.
- b. That domain of $f = A \times A$. For example, $*$ where $x * y = x^y$ can not be a binary operation on $(-\infty, 0]$ because x^y is not defined in the set $(-\infty, 0]$.
- c. That range of $f \subseteq A$. When this is not satisfied we say A is not closed under $*$. For example $\mathbf{N}$ is not closed under $-$ because $2 - 3 = -1$ is not in $\mathbf{N}$

In the second example above, to show that $*$ is a binary operation on $\mathbf{Z} - \{1\}$, we need only show that $x * y = x + y - xy$ is different from one. This is because, as you know, the sum, difference and product of two integers are again integers. For example 2, this means $x * y$ is an integer. But since the set does not contain 1, we have to show that $x * y$ is different from 1. To do so we will use proof by contra positive. Thus,

$$x * y = 1 \Rightarrow x + y - xy = 1 \Rightarrow x + y - xy - 1 = 0. \Rightarrow (x - 1) - y(x - 1) = 0 \\ \Rightarrow (x - 1)(1 - y) = 0 \Rightarrow x = 1 \vee y = 1.$$

So, if $x \neq 1$ and $y \neq 1$, then $x * y \neq 1$. $\Rightarrow, x * y \in A = \mathbf{Z} - \{1\}$.

Here are some familiar examples:

Example3: Let $A \neq \emptyset$. On the power set of A union, intersection and relative complement are binary operations. Thus if $A = \{a, b\}$, then $2^A = \{\emptyset, \{a\}, \{b\}, A\}$. The following tables give the results of applying the above binary operations on the elements of $2^A \times 2^A$.

$\cap$	$\emptyset$	$\{a\}$	$\{b\}$	A
$\emptyset$	$\emptyset$	$\{a\}$	$\{b\}$	A
$\{a\}$	$\{a\}$	$\{a\}$	A	A
$\{b\}$	$\{b\}$	A	$\{b\}$	A
A	A	A	A	A

$\cup$	$\emptyset$	$\{a\}$	$\{b\}$	A
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{a\}$	$\emptyset$	$\{a\}$	$\emptyset$	$\{a\}$
$\{b\}$	$\emptyset$	$\emptyset$	$\{b\}$	$\{b\}$
A	$\emptyset$	$\{a\}$	$\{b\}$	A

$\setminus$	$\emptyset$	$\{a\}$	$\{b\}$	A
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{a\}$	$\{a\}$	$\emptyset$	$\{a\}$	$\emptyset$
$\{b\}$	$\{b\}$	$\{b\}$	$\emptyset$	$\emptyset$
A	A	$\{b\}$	$\{a\}$	$\emptyset$

Definition: A non – empty set A on which a binary operation is defined is called an algebraic structure. It is denoted by $(A, *)$, if $*$ is the only algebraic structure defined on it, and by $(A, *, \Delta)$, if $*$ and Δ are the binary operations defined on it.

Example 4: In example 1, $(\mathbf{N}, +)$, $(\mathbf{R}, +, \cdot)$, are some of the algebraic structures. In example 2, the algebraic structure is $(\mathbf{Z} - \{1\}, *)$, where $x * y = x + y - xy$.

Example 5: a) If A has n elements and B has m elements, how many functions are there from A into B?

b) If A has n elements, how many binary operations are there on it?

Solution:

a) You can find a complete proof in the section on the principle of mathematical induction. For now, consider the following special cases.

Let $A = \{a, b\}$, and $B = \{1, 2, 3\}$. Then, the functions are:

$$\begin{array}{ccccc} \left\{ \begin{array}{l} a \rightarrow 1 \\ b \rightarrow 2 \end{array} \right. & \left\{ \begin{array}{l} a \rightarrow 1 \\ b \rightarrow 3 \end{array} \right. & \left\{ \begin{array}{l} a \rightarrow 2 \\ b \rightarrow 3 \end{array} \right. & \left\{ \begin{array}{l} a \rightarrow 1 \\ b \rightarrow 1 \end{array} \right. & \left\{ \begin{array}{l} a \rightarrow 2 \\ b \rightarrow 2 \end{array} \right. \\ \left\{ \begin{array}{l} a \rightarrow 3 \\ b \rightarrow 3 \end{array} \right. & \left\{ \begin{array}{l} a \rightarrow 2 \\ b \rightarrow 1 \end{array} \right. & \left\{ \begin{array}{l} a \rightarrow 3 \\ b \rightarrow 1 \end{array} \right. & \left\{ \begin{array}{l} a \rightarrow 3 \\ b \rightarrow 2 \end{array} \right. & \end{array}$$

So there are $3^2 = 9$ functions. What happens if $A = \{a, b, c\}$ and $B = \{1, 2\}$?

The functions are:

$$\begin{array}{cccc} \left\{ \begin{array}{l} a \rightarrow 1 \\ b \rightarrow 1 \\ c \rightarrow 1 \end{array} \right. & \left\{ \begin{array}{l} a \rightarrow 2 \\ b \rightarrow 2 \\ c \rightarrow 2 \end{array} \right. & \left\{ \begin{array}{l} a \rightarrow 1 \\ b \rightarrow 1 \\ c \rightarrow 2 \end{array} \right. & \left\{ \begin{array}{l} a \rightarrow 1 \\ b \rightarrow 2 \\ c \rightarrow 2 \end{array} \right. \\ \left\{ \begin{array}{l} a \rightarrow 2 \\ b \rightarrow 1 \\ c \rightarrow 2 \end{array} \right. & \left\{ \begin{array}{l} a \rightarrow 2 \\ b \rightarrow 2 \\ c \rightarrow 1 \end{array} \right. & \left\{ \begin{array}{l} a \rightarrow 2 \\ b \rightarrow 1 \\ c \rightarrow 1 \end{array} \right. & \left\{ \begin{array}{l} a \rightarrow 1 \\ b \rightarrow 2 \\ c \rightarrow 1 \end{array} \right. \end{array}$$

$2^3 = 8$ functions.

This is generally true: If A has n elements and B has m elements, then the number of functions from A into B is m^n .

b) Recall that a binary operation on A is any function from $A \times A$ into A . Thus there

$$\text{are } n(A)^{n(A \times A)} = n^{n^2} \text{ binary operation on } A.$$

Consider the binary operations in examples 1 and 3 above. What are the properties they have in common? From your earlier experience I expect you to know the facts like $2 + 3 = 3 + 2$, $2 + (3 + 4) = (2 + 3) + 4$, $A \cup B = B \cup A$, and $(A \cup B) \cup C = A \cup (B \cup C)$.

The first two are from Arithmetic, while the last two are from set theory. Though they are dealing with different topics, they illustrate the common properties - commutativity and associativity. The following discussion is about these properties.

Let $(A, *)$ be an algebraic structure.

1. $*$ is called commutative if and only if $x * y = y * x$ for each x and y in A .
2. $*$ is called associative if and only if $(x * y) * z = x * (y * z)$ for each x, y and z in A .

Examples 6: Let A = a collection of functions. Let $\circ$ be composition of functions.

Recall that you defined composition of functions in unit two of module one. $\circ$ is always associative but may not be commutative.

To see that it is associative, For any x in the common domain of f, g and h

$$f \circ (g \circ h)(x) = f((g \circ h)(x)) = f(g(h(x))), \text{ and}$$

$$(f \circ g) \circ h(x) = f \circ g(h(x)) = f(g(h(x))). \text{ Thus, } f \circ (g \circ h) = (f \circ g) \circ h.$$

To see the issue of commutativity, let, for instance, A be the collections of all functions from $\mathbf{R}$ into $\mathbf{R}$. Consider the functions $f: \mathbf{R} \rightarrow \mathbf{R}$ and $g: \mathbf{R} \rightarrow \mathbf{R}$ be given by $f(x) = x + 1$ and $g(x) = 2x$, respectively.

$$\text{Then } f \circ g(x) = f(g(x)) = f(2x) = 2x + 1$$

and

$$g \circ f(x) = g(f(x)) = g(x + 1) = 2x + 2.$$

Thus, $f \circ g \neq g \circ f$. That is $\circ$ is not commutative.

Example 7: Let $(\mathbf{R}, *)$ be defined such that

$x * y =$ the largest integer $\leq x + y$. We will denote it by $x * y = \lfloor x + y \rfloor$. The function $f(x) = \lfloor x \rfloor$ is called the floor function and it maps $\mathbf{R}$ into $\mathbf{Z}$. Now, $x * y = \lfloor x + y \rfloor = \lfloor y + x \rfloor = y * x$, because $+$ is commutative. But the operation is not associative, as can be seen from the following counter example:

Let $x = 3.2$, $y = 0.6$ and $z = 2.9$. Then $x * (y * z) = 3.2 * 3 = 6$, and $(x * y) * z = 3 * 2.9 = 5$. Hence $x * (y * z) \neq (x * y) * z$.

Example 8: On $\mathbf{Z} - \{1\}$ define $*$ as $x * y = x + y - xy$. Then $*$ is both commutative and associative. For any x, y, z

$x * y = x + y - xy = y + x - yx = y * x$. So, $*$ is commutative.

and

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

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

Thus, $*$ is associative.

Example 9: On $\mathbf{R}$ both $+$ and $\times$ are commutative and associative, while subtraction is neither associative nor commutative.

?

Consider the algebraic structures in example 3. Which of the operations commutative? Which of them are associative?

Example 10: Let $S = \{1, 2, 3\}$. Define $*, \Delta, \nabla$ on S by the following tables.

$*$	1	2	3
1	1	2	3
2	2	3	1
3	3	1	1

Δ	1	2	3
1	1	1	2
2	2	3	3
3	3	2	1

∇	1	2	3
1	1	1	2
2	3	3	3
3	3	1	2

Compute

1. $(1 \Delta 1) \Delta 3$ and $1 \Delta (1 \Delta 3)$. Is Δ associative?
2. $(3 \Delta 2) \nabla 3$
3. $[(3 * 1) \Delta 2] * [(2 \Delta 1) \Delta (1 * 1)]$
4. It is easy to see the commutative property of a binary operation from a table. If the table is symmetric with respect to the principal diagonal, then the binary operation is commutative. There is no such easy way of telling if the binary operation is associative. Now, using the above information find which of the above binary operations are commutative, if any?

Solution:

1. $(1 \Delta 1) \Delta 3 = 1 \Delta 3 = 2$, while $1 \Delta (1 \Delta 3) = 1 \Delta 2 = 1$. Thus, Δ is not associative.
2. $(3 \Delta 2) \nabla 3 = 2 \nabla 3 = 3$
3. $[(3 * 1) \Delta 2] * [(2 \Delta 1) \Delta (1 * 1)] = (3 \Delta 2) * (\Delta 1) = 2 * 2 = 3$
4. $*$ is commutative; the others are not.

$(A, *)$ be an algebraic structure. An element e_r is called a right identity iff $x * e_r = x$ for each x in A . An element e_l is called a left identity iff $e_l * x = x$, for each x in A . When an

element is both a left and right identity then we will simply call it an identity without using the words left or right.

Example 11: In $(\mathbf{R}, +)$ 0 is the identity. In $(\mathbf{R}, \times)$ 1 is the identity.

Theorem: In an algebraic structure $(A, *)$, let e_r and e_l be right and left identities with respect to $*$, respectively. Then

$e_r = e_l = e$ (say), such that $e * x = x * e = x$ for each x in A . In such a case e is unique. It is called the identity of A with respect to $*$.

Proof: Since e_l and e_r are left and right identities, For each x , $e_l * x = x$. When, in particular, $x = e_r$, $e_l * e_r = e_r$. Again for each x , $x * e_r = x$. The case $x = e_l$ gives

$$e_l * e_r = e_l. \text{ Thus } e_l = e_l * e_r = e_l = e_r.$$

Next, let us assume e_1 and e_2 are two identities. Then For any x , $x * e_2 = x$ and $e_1 * x = x$. Taking $x = e_1$ in the first case and taking $x = e_2$ in the second case gives $e_1 = e_2$. Hence an identity element, if it exists is unique.

Example 12: On $\mathbf{Z} - \{1\}$ consider the binary operation we defined earlier,

$x * y = x + y - xy$. Then For each x in $\mathbf{Z} - \{1\}$, $x * 0 = 0 * x = x$. Thus 0 is the identity element.

Example 13: On $\mathbf{Z}$ define $x * y = |x|y$.

Then since $x * e = |x|e = x$, has no unique solution e , $(\mathbf{Z}, *)$ has no right identity.

But $e * x = |e|x = x$ has solutions $e = \pm 1$. That is there are two left identities.

Example 14 On $\mathbf{Z}$ define $x * y = x - y$

Then $x - 0 = x$, but $0 - x = -x$ which may be different from x , if x is different from 0. Hence, 0 is a right identity only.

Definition: Let $(A, *)$ be an algebraic structure with identity element e . An element a in A is called invertible if and only if there is b in A such that $a * b = b * a = e$.

Remark: The existence of an identity element is necessary for the existence of an invertible element. In other words where there is not an identity element there cannot be an invertible element.

Example 15: In $(\mathbb{Z}, +)$ every element has inverse, while in $(\mathbb{Z}, \times)$ only -1 and 1 are invertible.

Example 16: For $(\mathbb{Z} - \{1\}, *)$ where $x * y = x + y - xy$, if x is invertible its inverse is

found by using $\frac{-x}{1-x}$. This is, derived as follows. Let y be the inverse of x .

Then, since the identity element for this algebraic structure is 0 , we have $x * y = x$

$$+ y - xy = 0. \Rightarrow y(1 - x) = -x \Rightarrow y = \frac{-x}{1-x}.$$

Now, $\frac{-x}{1-x}$ is an integer, if $(x - 1)$ is a factor of x . So, 0 and 2 are their own inverses.

?

For $(\mathbb{R} - \{1\}, *)$ where $x * y = x + y - xy$, what are the invertible elements?

Theorem Let $*$ be associative in an algebraic structure $(A, *)$. Suppose the identity element e also exists in $(A, *)$. Then each invertible element has a unique inverse.

Proof: If x is invertible and y and z are its inverses, then
 $y = y * e = y * (x * z) = (y * x) * z = e * z = z$, because $*$ is associative.

The unique inverse of a , in the above theorem, is denoted by a^{-1}

Theorem In a algebraic structure $(A, *)$. Let $*$ be associative and e be the identify element of $(A, *)$. Then

- If x is invertible then $(x^{-1})^{-1} = x$
- If x, y invertible then $x * y$ is invertible and

$$(x * y)^{-1} = y^{-1} * x^{-1}$$
- If both x & y commute with z , then $x * y$ also commutes with z .

- d. If x commutes with y and if y is invertible, then x commutes with y^{-1}
- e. If x commutes with y and if both x and y are invertible, then x^{-1} commutes with y^{-1}

Proof

- a. If x^{-1} is the inverse of x , and x^{-1} is also invertible then

$$x^{-1} * x = e = x * x^{-1}. \quad \text{But the inverse of } x^{-1} \text{ is } (x^{-1})^{-1}$$

$$\Rightarrow (x^{-1})^{-1} * x^{-1} = x^{-1} * (x^{-1})^{-1} = e.$$

Since the inverse of x^{-1} is unique, $x = (x^{-1})^{-1}$.

$$\begin{aligned} \text{b. } (y^{-1} * x^{-1}) * (x * y) &= y^{-1} * (x^{-1} * x) * y \\ &= y^{-1} * y = e = (x * y) * (y^{-1} * x^{-1}) \end{aligned}$$

Since, $*$ is associative, $x * y$ has the unique inverse $(x * y)^{-1}$.

Thus, $(x * y)^{-1} = y^{-1} * x^{-1}$.

$$\begin{aligned} \text{c. } (x * y) * z &= x * (y * z) = x * (z * y) \\ &= (x * z) * y = (z * x) * y = z * (x * y) \\ &\Rightarrow x * y \text{ commute with } z. \end{aligned}$$

$$\begin{aligned} \text{d. } x * y^{-1} &= (e * x) * y^{-1} = ((y^{-1} * y) * x) * y^{-1} \\ &= y^{-1} * (x * y) * y^{-1} = (y^{-1} * x) * (y * y^{-1}) = y^{-1} * x \end{aligned}$$

$$\text{e. } x^{-1} * y^{-1} = (y * x)^{-1} = (x * y)^{-1} = y^{-1} * x^{-1}.$$

Definition: Let $(A, *, \Delta)$ be an algebraic structure with two binary operations. We say:

- Δ is left-distributive over $*$ if $x \Delta (y * z) = (x \Delta y) * (x \Delta z)$, $\forall x, y, z \in A$
- Δ is right – distributive over $*$ if $(y * z) \Delta x = (y \Delta x) * (z \Delta x)$, $\forall x, y, z \in A$
- Δ is distributive over $*$ if Δ is both left and right – distributive over $*$.

Example 17: Consider $(\mathbf{R}, \times, *)$ where $x * y = y$. Then $x * (y \times z) = y \times z = yz$ and $(x * y) \times (x * z) = y \times z = yz$. Hence $*$ is left distributive over $\times$.

But, $(y \times z) * x = x$ while, $(y \times x) * (z \times x) = x \times x = x^2$. Thus $*$ is not right distributive over $\times$.

Example 18: Let $A \neq \emptyset$. We have already seen that $(2^A, \cup, \setminus)$ is an algebraic structure.

Then, for any B, C and D in 2^A ,

$$(B \cup C) \setminus D = (B \cup C) \cup D' = B \cup C \cup D' \text{ and}$$

$$(B \setminus D) \cup (C \setminus D) = (B \cup D') \cup (C \cup D') = B \cup C \cup D'.$$

Hence $\setminus$ is right – distributive over $\cup$. But,

$$\begin{aligned} D \setminus (B \cup C) &= D \cup (B \cup C)' = D \cup (B' \cap C') = (D \cup B') \cap (D \cup C') \\ &= (D \setminus B) \cap (D \setminus C) \end{aligned}$$

Hence $\setminus$ is not left – distributive over $\cup$

Example 19: In $(\mathbf{R}, +, \times)$, $\times$ is distributive over $+$.

Now that we have considered the basic properties of an algebraic structure, let us define functions that map one algebraic structure into another, while preserving the structure that is found by defining a binary operation on them. The functions relate not only the sets (as 1 – 1 and onto functions do), but the corresponding binary operations as well.

Here is the definition:

Definition: Let $(A, *)$ and (B, Δ) be algebraic structures. Then $f : A \rightarrow B$ is called a

homomorphism if and only if $f(x * y) = f(x) \Delta f(y) \forall x, y \in A$. Also,

Let $(A, *, *)', (B, \Delta, \Delta')$ be algebraic structures. Then $f : A \rightarrow B$ is called a homomorphism iff 1) $f(x * y) = f(x) \Delta f(y)$, & 2) $f(x *' y) = f(x) \Delta' f(y) \forall x, y \in A$

Example 20: $f : (\mathbf{R}, +) \rightarrow f(\mathbf{R}^+, \times)$ given by $f(x) = 2^x$. Here $\mathbf{R}^+ = (0, \infty)$

Now for any x, y in $\mathbf{R}$, $f(x + y) = 2^{x+y} = 2^x 2^y = f(x) f(y)$. Thus f is a

homomorphism. Note also that f is both one – to – one and onto. To see this:

$$\text{For any } x, y \text{ in } \mathbf{R}, f(x) = f(y) \Rightarrow 2^x = 2^y \Rightarrow \frac{2^x}{2^y} = 1$$

$$\Rightarrow 2^{x-y} = 1 \Rightarrow x-y=0 \Rightarrow x = y. \text{ So, } f \text{ is 1 – 1.}$$

Since for any $y \in (0, \infty)$, taking $x = \log_2 y$ gives

$f(x) = f(\log_2 y) = 2^{\log_2 y} = y$. Thus f is onto. Such a homomorphism is called an isomorphism.

Definition: A homomorphism $f : A \rightarrow B$ is

- a) a monomorphism if and only if f is 1-1
 - b) an epimorphism if and only if f is onto
 - c) an isomorphism if and only if f is a bijection
- (1-1 correspondence)

Example 21: $f: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$ given by $f(x) = 2x$

f is 1-1, but is not onto. Besides for any $x, y \in \mathbb{Z}$,

$$f(x + y) = 2(x + y) = 2x + 2y = f(x) + f(y).$$

Thus, f is a monomorphism.

Example 22: $g: (\mathbb{R}^*, \times) \rightarrow (\{-1, 1\}, \times)$ given by $g(x) = \begin{cases} 1 & x > 0 \\ -1 & x < 0 \end{cases}$

g is clearly, onto. But it can not be 1-1, because, for instance,

$g(2) = g(1) = 1$. To see that g is a homomorphism, we need to consider three cases.

Case 1: $x > 0$ and $y > 0$. Then $xy > 0$.

$$\Rightarrow f(xy) = 1. \text{ But then, } f(x).f(y) = 1 \times 1 = 1$$

$$\Rightarrow f(xy) = f(x).f(y).$$

Case 2: $x < 0$ and $y < 0$. Then $xy > 0$.

$$\Rightarrow f(xy) = 1. \text{ On the other hand, } f(x).f(y) = -1 \times -1 = 1$$

$$\Rightarrow f(xy) = f(x).f(y)$$

Case 3: $x < 0$ and $y > 0$. Then $xy < 0$.

$$f(xy) = -1 \text{ and } f(x).f(y) = -1 \times 1 = -1$$

Thus f is an epimorphism.

Example 23: Define $f: ((0, \infty), \cdot) \rightarrow (\mathbb{R}, +)$ by $f(x) = \log_{10} x$.

To show that it is a homomorphism, Take arbitrary elements from $(0, \infty)$.

Let x and y be any two such elements. Then,

$f(xy) = \log_{10} xy = \log_{10} x + \log_{10} y = f(x) + f(y)$. This means f is a homomorphism. Since f is also a 1 – 1 correspondence, f is an isomorphism.

The important and interesting property of these functions is that they preserve the properties of algebraic structures. Here is the theorem that states this fact.

Theorem Let $(A, *)$ and (B, Δ) be two algebraic structures. Suppose

$f: A \rightarrow B$ be an epimorphism. Then

- a) $*$ is associative $\Rightarrow \Delta$ is associative
- b) $*$ is commutative $\Rightarrow \Delta$ is commutative
- c) e is the identity in $(A, *) \Rightarrow f(e)$ is the identity in (B, Δ) .
- d) $x \in A$ is invertible in $A \Rightarrow f(x)$ is invertible in B and $f(x)^{-1} = f(x^{-1})$.

Proof:-

$$\begin{aligned} \text{a) } (f(x) \Delta f(y)) \Delta f(z) &= f(x * y) \Delta f(z) = f((x * y) * z) \\ &= f(x * (y * z)) = f(x) \Delta f(y * z) \\ &= f(x) \Delta (f(y) \Delta f(z)) \end{aligned}$$

$$\text{b) } f(x) \Delta f(y) = f(x * y) = f(y * x) = f(y) \Delta f(x).$$

$$\begin{aligned} \text{c) } \forall y \in B, \exists x \in A \text{ such that } f(x) = y. \text{ Now, } f(e) \Delta f(x) &= f(e * x) = f(x * e) \\ &= f(x) \Delta f(e) = y \Delta f(e). \end{aligned}$$

d) Suppose x is invertible

$$\Rightarrow x^{-1} \in A \text{ such that } x * x^{-1} = x^{-1} * x = e.$$

$$\Rightarrow f(e) = f(x * x^{-1}) = f(x) \Delta f(x^{-1})$$

$$\Rightarrow f(x^{-1}) \text{ is the inverse of } f(x). \text{ But } f((x)^{-1}) \text{ is also the inverse of } f(x)$$

$$\Rightarrow f(x)^{-1} = f(x^{-1})$$

Example 24: There is no isomorphism from $(\mathbf{R}^*, \cdot)$ into $(\mathbf{R}, +)$ where $\mathbf{R}^*$ is the set of non-zero real numbers.

Proof Suppose $\exists f : (\mathbf{R}^*, \cdot) \rightarrow (\mathbf{R}, +)$ an isomorphism.

$$\Rightarrow f(1) = 0 \text{ by the above theorem.}$$

$$\text{Now } 0 = f(-1 \times -1) = f(-1) + f(-1) = 2f(-1).$$

$$\Rightarrow f(-1) = f(1) \text{ contradiction.}$$

Definition: Two algebraic structures are said to be isomorphic if there is an isomorphism of one onto the other

Remark: Two isomorphic algebraic structures are the same except that their elements are labeled differently. Thus, if you study one algebraic structure then you know all the algebraic properties of any algebraic structure that is isometric to the one under consideration. This simplifies your study of algebraic structures a lot. Besides, if there is an epimorphism from an algebraic structure $(A, *)$, which you have investigated its properties, into (B, Δ) , then you can use the fact that similar properties hold for (B, Δ) as mentioned in the last theorem above.



Self - Check Exercises

1) State which of the following are binary operations:

a) On $\mathbf{Q}$ define $a * b = \frac{a}{b}$

b) On $\mathbf{R}$ define $a \Delta b = a$

c) On $\mathbf{R}$ define $a \Delta b = \pm ab$

d) On $\mathbf{R}^2$ define $(x, y) \Delta (u, v) = \left(\frac{x+u}{2}, \frac{y+v}{2} \right)$

2) If A has n elements, how many commutative binary operations are there on A ?

3) Check if the following binary operations are associative or commutative:

- a) On $\mathbf{R}$, $x \Delta y = x + y x^2 y$
 - b) On $\mathbf{R}$, $x \Delta y = \min \{x, 2\}$
 - c) On $\mathbf{R}$, $x \Delta y = x + \log(10y-1 + 1)$
 - d) On $\mathbf{R}$, $x \Delta y = \sqrt{x^2 + y^2 + 1}$
 - e) On $\mathbf{R}^+$, $x \Delta y = x \log y$
 - f) On $\mathbf{R}$, $x \Delta y = x + \log(1 + 10^{y-x} + 10^y)$
 - g) On $\mathbf{R}$, $x \Delta y = 17$
 - h) On $\mathbf{R}$, $x \Delta y = yx^{1-\log y}$
- 4) a) Let A be a set with n elements. If $a \in A$, for how many binary operations in A is a the identity element?
b) How many of the binary operations on A have no identity?
- 5) Which of the following algebraic structures admit an identity element? For those that have identity elements, find the invertible elements.
- a) On $\mathbf{Q}$, $x \Delta y = \frac{xy}{2}$
 - b) On $\mathbf{Z}$, $x \Delta y = (1 - x) y$
 - c) On $\mathbf{N}$, $x \Delta y = \max \{x, y\}$
 - d) On $\mathbf{Z}$, $x \Delta y = |x| y$
- 6) Let Δ be a binary operation on $\mathbf{R}$, given by $x \Delta y = x + y + x^2 y$. Prove that Δ admits an identity element and that every real number has a unique right inverse for Δ , but that there exist numbers that have not left inverse for Δ . Show also that the identity element is the only invertible element.
- 7) Let Δ be a binary operation with identity element in S . Prove that the operations both associative and commutative iff it satisfies:
- $$(a \Delta b) \Delta (c \Delta d) = (a \Delta c) \Delta (b \Delta d)$$
- for any element a, b, c, d in S .
- 8) Determine which of the following maps are homomorphisms:

- a) $f: (\mathbf{R}, +) \rightarrow (\mathbf{Z}, +)$ given by $f(x) = \lfloor x \rfloor$
- b) $g: (\mathbf{R}^*, \cdot) \rightarrow (\mathbf{R}^*, \cdot)$ given by $f(x) = |x|$
- 9) Show that $f: (\mathbf{R}, +) \rightarrow (\mathbf{R}^+, \cdot)$ given by $f(x) = 10^x$ is an isomorphism.
- 10) a) Prove that there is no isomorphism from $(\mathbf{R}^*, \cdot)$ into $(\mathbf{R}, +)$
- b) Show that $\mathbf{Z}$ and $\mathbf{Q}$, both under addition, are not isomorphic.
- 11) Let ∇ and Δ be binary operations defined on $\mathbf{R}$ by
- $$x \nabla y = \max \{x, y\} \text{ and } x \Delta y = \min \{x, y\}.$$
- Exhibit an isomorphism from $(\mathbf{R}, \nabla)$ into $(\mathbf{R}, \Delta)$.

Section Two: Elementary ideas of Groups and Rings

Overview



This section discusses the ideas of Groups and Rings. The algebraic structure group is one of the fundamental building blocks of algebra. It is an algebraic structure with one binary operation. The second algebraic structure we consider – ring is an algebraic structure with two binary operations, that is related with groups. These structures are significant to your study of mathematics. You will also find them to be very fascinating to study.

We will try to make you understand the concepts by considering some well-chosen examples. At this stage you will do well to revise the topic in the last section and the Section on Mathematical Proofs from Module One.

Objectives

When you will have completed this section you will be able to:

- Define a group
- Give examples of abelian and non- abelian groups
- Define subgroups
- Give subgroups of some common groups
- Define rings
- Give some examples of rings
- State some properties of rings

Let us start our discussion by defining what a group is.



An algebraic structure $(G, *)$ is called a group if and only if the following axioms are satisfied:

1. G is closed under $*$
2. $*$ is associative
3. G has an identity with respect to $*$
4. Every element of G is invertible with respect to $*$

Note that in the definition commutativity of the binary operation $*$ is not a requirement.

In case the binary operation of the group is commutative then the group is called an abelian or commutative group. Another useful property in a group is the number of elements the group. The number of elements of a finite group G is called its order and is denoted by $0(G)$ or $|G|$. The order of $(G, *)$ when G is infinite is not defined.

Below are given some examples of groups:

Examples 1 $(\mathbf{Z}, +)$ is a group

Example 2 $(\mathbf{Z}, \times)$ is not a group. This is because no elements except 1 and -1 have inverses in $\mathbf{Z}$. Note that The first three axioms of the definition are satisfied. Here 1 is the identity.

Example 3 $(\mathbf{Q}, +)$ and $(\mathbf{R}^+, \times)$ are abelian groups. To see one of them,

Let $x, y \in \mathbf{R}^+ = (0, \infty)$. Then $x > 0$ and $y > 0$. But then $xy > 0 \Rightarrow xy \in \mathbf{R}^+$.

Multiplication of real numbers is also associative.

$\forall x \in \mathbf{R}^+, (x \times 1 = 1 \times x = x)$. i. e. 1 is the identity element for multiplication and it

is in $\mathbf{R}^+$. Moreover, Given $x \in \mathbf{R}^+, x^{-1} = \frac{1}{x} \in \mathbf{R}^+$,

and $(x \times \frac{1}{x} = \frac{1}{x} \times x = 1)$. Thus, $(\mathbf{R}^+, \times)$ is a group. Since multiplication is

commutative, $(\mathbf{R}^+, \times)$ is abelian.

Example 3: $(\mathbf{R} - \{1\}, *)$ $x * y = x + y - xy$ is an abelian group.

To check the first axiom, since the sum, difference, and product of any two real numbers are also real numbers, you only need to check that

$x * y = x + y - xy \neq 1$. Adapt Example 2 of the first section of this module to $\mathbf{R} - \{1\}$ and show this holds. Adapt Example 7,10 and 14 of Section One of this module, to show that $(\mathbf{R} - \{1\}, *)$ is an abelian group.

Example 4: $(\mathbf{Z}, *)$, $x * y = x + y - xy$ is not be a group, because 1 has no inverse with respect to*.

Note that in the above groups the operations are all commutative. In other words all of them are abelian. The following two are examples of non – abelian groups.

Example 5:

Let $A = \{1, 2, 3\}$

Define	I:	$1 \rightarrow 1$	$f_1:$	$1 \rightarrow 2$
		$2 \rightarrow 2$		$2 \rightarrow 3$
		$3 \rightarrow 3$		$3 \rightarrow 1$
	$f_2:$	$1 \rightarrow 3$	$f_3:$	$1 \rightarrow 1$
		$2 \rightarrow 1$		$2 \rightarrow 3$
		$3 \rightarrow 2$		$3 \rightarrow 2$
	$f_4:$	$1 \rightarrow 3$	$f_5:$	$1 \rightarrow 2$
		$2 \rightarrow 2$		$2 \rightarrow 1$
		$3 \rightarrow 1$		$3 \rightarrow 3$

Consider (G, o) where $G = \{I, f_1, f_2, f_3, f_4, f_5\}$.

$G = S_3$ is a non - abelian group of order 6. The table for the algebraic structure is given below:

$\circ$	I	f_1	f_2	f_3	f_4	f_5
I	I	f_1	f_2	f_3	f_4	f_5
f_1	f_1	f_2	I	f_5	f_3	f_4
f_2	f_2	I	f_1	f_4	f_5	f_3
f_3	f_3	f_4	f_5	I	f_1	f_2
f_4	f_4	f_5	f_3	f_2	I	f_1
f_5	f_5	f_3	f_4	f_1	f_2	I

As can be seen from the table,

S_3 is closed under composition and I is the identity element. It has been shown that composition of functions is always associative. We can also see that f_1 and f_2 are inverses of each other, while I, f_3 , f_4 , and f_5 are their own inverses.

Thus $(S_3, \circ)$ is a group. Since, $f_1 \circ f_3 = f_5$, and $f_3 \circ f_1 = f_4$ the group is not abelian.

?

In S_3 , give an example of two elements x, y such that

$$(x \circ y)^2 \neq x^2 \circ y^2.$$

Show also that there are four elements satisfying $x^2 = I$ and there are three elements satisfying $y^3 = I$.

Example 6 Let $G = \{f \mid f : \mathbf{R} \rightarrow \mathbf{R}, f \text{ a } 1-1 \text{ correspondence}\}$. We can show that $(G, \circ)$ is an infinite non-abelian group.

Let $f, g, \in G$. Then $f : \mathbf{R} \rightarrow \mathbf{R}$ and $g : \mathbf{R} \rightarrow \mathbf{R}$ are 1-1 correspondences. We need to show that $f \circ g : \mathbf{R} \rightarrow \mathbf{R}$ is also a 1-1 correspondence.

Suppose $f \circ g(x) = f \circ g(y)$ for any $x, y \in \mathbf{R}$.

$$\Rightarrow f(g(x)) = f(g(y))$$

$$\Rightarrow g(x) = g(y), \text{ since } f \text{ is } 1-1$$

$$\Rightarrow x = y, \text{ since } g \text{ is } 1-1.$$

Hence, $f \circ g$ is 1 – 1.

To show on to ness, let $z \in \mathbf{R}$. Then since f is onto there is $w \in \mathbf{R}$ such that $f(w) = z$. But, since g is also onto there is $x \in \mathbf{R}$ such that $g(x) = w$.

$\Rightarrow y = f(w) = f(g(x)) = f \circ g(x)$. So, $f \circ g$ is onto.

There fore $f \circ g$ is a 1 – 1 correspondence from $\mathbf{R}$ into $\mathbf{R}$.

$\Rightarrow f \circ g \in G$. This means G is closed under $\circ$.

In Example 5 of unit one, It has been shown that Composition of function is associative.

Take $I: \mathbf{R} \rightarrow \mathbf{R}$ given by $I(x) = x$. Let f be an arbitrary element of G .

Now, for any $x \in \mathbf{R}$, $f \circ I(x) = f(I(x)) = f(x) \Rightarrow f \circ I = f$.

Similarly, $I \circ f(x) = I(f(x)) = f(x) \Rightarrow I \circ f = f$. Then, I is the identity.

Let $f: \mathbf{R} \rightarrow \mathbf{R}$ be an element of G . Since $\circ$ is associative, there is a unique inverse f^{-1} . We want to show that f^{-1} is also a 1 – 1 correspondence.

Domain $f = \mathbf{R} \Rightarrow \text{Range } f^{-1} = \mathbf{R} \Rightarrow f^{-1}$ is onto.

Since f is 1 – 1, for any $x, y \in \mathbf{R}$ $f(x) = f(y) \Rightarrow x = y$. This means

$f^{-1} \circ f(x) = f^{-1} \circ f(y) \Rightarrow f^{-1}(f(x)) = f^{-1}(f(y))$. That is $x = y \Rightarrow f^{-1}(f(x)) = f^{-1}(f(y))$.

So, f^{-1} is a function.

Range $f = \mathbf{R} \Rightarrow \text{domain } f^{-1} = \mathbf{R} \Rightarrow f^{-1}: \mathbf{R} \rightarrow \mathbf{R}$ is onto.

The fact that f is a function implies that $x = y \Rightarrow f(x) = f(y)$.

Then $f^{-1}(f(x)) = f^{-1}(f(y)) \Rightarrow f^{-1} \circ f(x) = f^{-1} \circ f(y) \Rightarrow x = y \Rightarrow f^{-1}$ is 1 – 1.

There fore, f^{-1} is a 1 – 1 correspondence. $f^{-1} \in \mathbf{R}$.

What we have done up to now shows that $(G, \circ)$ is a group. To show that it is non – abelian, Take $f(x) = x + 1$ and $g(x) = 2x + 5$. Both are 1 – 1 correspondences.

But,

$$f \circ g(x) = f(2x+5) = 2x + 6, \text{ and } g \circ f(x) = g(x+1) = 2x + 7$$

$\Rightarrow f \circ g \neq g \circ f$. This completes the proof.

One of the basic results in group theory is the following simple theorem. It gives us the cancellation laws that are necessary to solve equations.

Theorem

Suppose $a, b, x \in (G, *)$ be arbitrary . Then the following are true:

- i) $a * x = b * x \Rightarrow a = b$ (right – cancellation)
- ii) $x * a = x * b \Rightarrow a = b$ (left – cancellation)

Proof:

- i) $a * x = b * x \Rightarrow (a * x) * x^{-1} = (b * x) * x^{-1}$, x is invertible
 $\Rightarrow a * (x * x^{-1}) = b * (x * x^{-1})$, $*$ is associative
 $\Rightarrow a * e = b * e$, the identity e exists in the group G
 $\Rightarrow a = b$

ii) Similar

You might wonder why we needed to consider left – cancellation and right – cancellation separately. That was necessary because, $*$ may not be commutative.

Subgroups

Given a group it happens that some of its subsets are themselves groups under the binary operation of the main group. Such subsets are called subgroups of the given group.



Let $(G, *)$ be a group . A non - empty subset H of G is a subgroup of G if $(H, *)$ is also a group.

We write $H < G$

In any group, the group itself and the set containing the identity element are always subgroups. These are called trivial subgroups. Any subgroup different from the trivial subgroups is called a non – trivial subgroup.

Example 7: For $(\mathbf{R}, +)$

$(\mathbf{Z}, +)$, $(\mathbf{Q}, +)$, $(\mathbf{H}, +)$, where $\mathbf{H} = \{5n \mid n \in \mathbf{Z}\}$ are non – trivial subgroups, while $(\mathbf{R}, +)$ and $(\{0\}, +)$ are trivial subgroups.

The following are not subgroups of $(\mathbf{R}, +)$:

$(\mathbf{N}, +)$, $(\mathbf{I}, +)$ where $\mathbf{I} = \{x \mid x \text{ is irrational}\}$.

Example 8: For $(\mathbf{R}^*, \times)$ the following are subgroups:

$(\mathbf{Q}^*, \times)$, $(\mathbf{R}^*, \times)$, $(\{1\}, \times)$, $(\{-1, 1\}, \times)$, $(\mathbf{Q}^+, \times)$

while the following are not subgroups of $(\mathbf{R}^*, \times)$:

$(\mathbf{Q}, \times)$, $(\mathbf{Z}^*, \times)$.



Let a be an element of an algebraic structure A with ∇ associative, and m be an integer. Then

$$a^m = \begin{cases} \underbrace{a \nabla a \nabla \dots \nabla a}_{m \text{ times}}, & \text{if } m > 0 \\ e, & \text{if } m = 0 \\ \underbrace{a^{-1} \nabla a^{-1} \nabla \dots \nabla a^{-1}}_{-m \text{ times}}, & \text{if } m < 0 \end{cases}$$

Example 9: Let $(G, *)$ be a group and $a \in G$. Let $\langle a \rangle = \{a^i \mid i \in \mathbf{Z}\}$. Then $\langle a \rangle$ is called the cyclic subgroup generated by a .

Observe that for any two elements a^i, a^j of $\langle a \rangle$, $a^i * a^j = a^{i+j}$ and $(a^i)^{-1} = (a^{-1})^i$.

If for some choice of a $G = \langle a \rangle$, then G is called a cyclic group.

In the exercises you will show that every cyclic group is abelian.

Theorem Let $(G, *)$ be a group & H is a non-empty subset of G . $H < G$ iff i)

$$x, y \in H \Rightarrow x * y \in H$$

$$\text{ii) } x \in H \Rightarrow x^{-1} \in H.$$

Proof If $H < G$, then it is obvious that i) and ii) hold.

Conversely, suppose i) and ii) hold.

Then for any x, y, z in H , x, y, z are in G , because $H \subseteq G$. Thus $x * (y * z) = (x * y) * z$. Thus $*$ is associative in H . Besides, for any $x \in H$, $x^{-1} \in H$, by ii).

But then by i), $x * x^{-1} = e \in H$. So, $H < G$.

Corollary Let $(G, *)$ be a group & H is a non-empty subset of G .

$$H < G \text{ iff } x, y \in H \Rightarrow x * y^{-1} \in H$$

The following theorem, due to Lagrange, reveals a very interesting relation ship between a finite group and its subgroups. We will not prove the theorem, because it requires some concepts that we will not cover in this course.

Theorem If G is a finite group & $H < G$ then $o(H)$ divides $o(G)$.

To see what the theorem claims we will consider the following example.

Example 10: For the group (S_3, o) in Example 6,

the subgroups are (S_3, o) , (I, o) , $(\{I, f_1, f_2\}, o)$, $(\{I, f_3\}, o)$, $(\{I, f_4\}, o)$, and $(\{I, f_5\}, o)$.

To see one of them consider the table for $(\{I, f_1, f_2\}, o)$.

o	I	f_1	f_2
I	I	f_1	f_2
f_1	f_1	f_1	I

f_2	f_2	I	f_1
-------	-------	-----	-------

The table shows that $\{I, f_1, f_2\}$ is closed under $\circ$. Each element also has inverse.

The inverse of I is I itself, while f_1 and f_2 are inverses of each other. Thus, by the theorem on subgroups $(\{I, f_1, f_2\}, \circ) < (S_3, \circ)$.

You can check the other subsets similarly. Note that the listed subgroups have 6, 1, 3, 2, 2, and 2 elements respectively. And these numbers are divisors of 6.

One thing you should note about Lagrange's theorem though, is that the converse does not hold. For instance, the number of elements of

$\{I, f_1, f_3\}$ divides $o(S_3)$, but $\{I, f_1, f_3\}$ is not a subgroup of $(S_3, \circ)$. $f_1 \circ f_3 = f_5$ which is not a member of $\{I, f_1, f_3\}$.



If G is a group and $a \in G$, the order (or period) of a , denoted by $o(a)$, is the least positive integer m such that $a^m = e$. If no such an integer exists we say that a is of infinite order.

Theorem: If G is a finite group and $a \in G$, then $o(a)$ divides $o(G)$.

Proof: Consider the cyclic subgroup generated by a , $\langle a \rangle$. Since, by the above definition, $a^{o(a)} = e$, $\langle a \rangle$ can at most have $o(a)$ elements. It can not have fewer number of elements, because if it has $a^i = a^j$ for some integers, $0 \leq i < j < o(a)$. Then $a^{j-i} = e$. But then $0 < j - i < o(a)$. Which contradicts the above definition. Thus the cyclic group generated by a has $o(a)$ elements. Now, this means by Lagrange's theorem, $o(a)$ divides $o(G)$.

Corollary: If G is a finite group and $a \in G$, then $a^{o(G)} = e$.

You are now ready for the second concept that we planned to discuss in this chapter - the concept of a ring. Here is the definition.



An algebraic structure with two binary operations $(R, *, \Delta)$ is called a ring if:

1. $(R, *)$ is an abelian group
2. R is closed under Δ
3. Δ is associative
4. Δ is distributive over $*$

Notation It is customary to replace $*$ by $+$ and Δ by $\times$ or $\bullet$ and write $(R, +, \times)$ or $(R, +, \bullet)$ instead of $(R, *, \Delta)$. In this representation the identity for $*$ is denoted by 0, the identity for Δ , if it exists, is denoted by 1, the inverse of x under $*$, is denoted by $-x$, and, if it exists, the inverse of x under Δ is denoted by x^{-1} .

Notes In a ring $(R, +, \times)$:

- 1) If $\times$ is commutative, we say $(R, +, \times)$ is a commutative ring.
- 2) If $(R, +, \times)$ has an identity for $\times$ it is called a ring with unity.
- 3) If $(R - \{0\}, \times)$ is closed with respect to the operation $\times$, then

$\forall a, b \in R - \{0\}$, we have $a \times b \neq 0$, and we call $(R, +, \times)$ a ring without divisors of zero. In a ring without divisors of zero it holds that

$$a \times b = 0 \Rightarrow (a = 0 \text{ or } b = 0).$$

A commutative ring $(R, +, \times)$ with identity and without divisors of zero is called an integral domain. In the definition of an integral domain, it is

assumed, that the ring $(R, +, \times)$ has more than one element, which means it has at least one nonzero element.

- 4) A ring $(R, +, \times)$ with unity in which every non – zero element is invertible under $\times$ is called a division ring .
- 5) A commutative division ring is called a field

Example 11: $(\mathbf{Z}, +, \times)$ is an integral domain that is not a field. It is not a field because the only invertible elements in $\mathbf{Z}$ under $\times$ are 1 and -1 .

Example 12. $(\mathbf{Q}, +, \times)$ is a field? Note that every non-zero element of $\mathbf{Q}$ is invertible under $\times$.

Example 13. $(\mathbf{E}, +, \times)$ is a commutative ring with out unity, where E is the set of even integers.

Example 14. Consider $(\{0, 1, 2, 3\}, +, \times)$ whose operations are given below.

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

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

This is a commutative ring with unity that is not an integral domain ($2 \neq 0$ but $2 \times 2 = 0$) (See the next section for a detailed treatment of this example).

Example 15: Let R be the set of all symbols (a, b) where a and b are real numbers. We define $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$. Now define $+$ as follows: if $x = (a, b)$ and $y = (c, d)$ then $x + y = (a + c, b + d)$.

You can easily show that $(R, +)$ is an abelian group. If you now define multiplication on R as follows $(R, +, \bullet)$ will be a field:

For $x = (a, b)$ and $y = (c, d)$, $xy = (ac - bd, ad + bc)$.

You can check that the unity is $(1, 0)$ and for any $x = (a, b) \neq (0, 0)$, since

$$a \neq 0 \text{ or } b \neq 0, a^2 + b^2 \neq 0. \text{ Thus } x^{-1} = \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right)$$

Remark: The above field is called the field of complex numbers. (a, b) is usually written as $a + ib$, where $i^2 = -1$.

Example 16: The set $R = \{a, b, c, d\}$ is a non – commutative ring under the following operations:

+	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

•	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	a	a	a
d	a	b	c	d

Theorem Let $(R, +, \times)$ be a ring

a) $a \times 0 = 0 \times a = 0 \quad \forall a \in R$

b) $(-a) \times b = a \times (-b) = -(a \times b) \quad \forall a, b \in R$

c) $(-a) \times (-b) = a \times b \quad \forall a, b \in R.$

Proof a) $0 + 0 = 0. \Rightarrow a \times (0 + 0) = a \times 0, \quad 0 \text{ is its own inverse.}$

$$\Rightarrow a \times 0 + a \times 0 = a \times 0 + 0, \quad \text{Distributivity}$$

$$\Rightarrow a \times 0 = 0, \quad \text{Left Cancellation}$$

Similarly, $0 \times a = 0.$

b) $(-a) \times b + a \times b = (-a + a) \times b = 0. \Rightarrow (-a) \times b = a \times b.$

Similarly, $a \times (-b) = a \times b.$

$$c) (-a) \times (-b) + (-a) \times b = (-a) \times (-b + b) = (-a) \times 0 = 0.$$

$$\text{Thus, } (-a) \times (-b) = a \times b.$$

Example 17: Let $(R, +, \cdot)$ be a ring.

a) If $a, b, c, d \in R$, evaluate $(a + b)(c + d)$

b) Prove that if $a, b \in R$ then $(a + b)^2 = a^2 + ab + ba + b^2$

Solution: a) Applying distributive property, $(a + b)(c + d) = (a + b)c + (a + b)d$

$$= ac + bc + ad + bd.$$

b) $(a + b)^2 = (a + b)(a + b) = aa + ba + ab + bb = a^2 + ab + ba + b^2$, by a) above.

Note that, unless R is a commutative ring you cannot write $ab + ba = 2ab$.

Ring homomorphism



A mapping f from the ring R_1 into the ring R_2 is called a ring homomorphism iff:

$$f(x + y) = f(x) + f(y)$$

$$f(xy) = f(x)f(y)$$

In this definition the two additions are the respective additions of the two rings. Similarly the multiplications are the respective multiplications of the two rings.

Example 18: For any ring R , define $f: R \rightarrow R$, by $f(x) = x$. Then f is a ring isomorphism.

Example 19: Let R be the set of all continuous functions, real – valued functions on the

closed unit interval. Then $(R, +, \cdot)$ is a ring where $+$ and $\cdot$ are addition and

multiplication of functions. Now define F from this ring into the field of real

numbers by $F(g(x)) = g\left(\frac{1}{2}\right)$. Then, F is a homomorphism.

Subrings



A subset S of a ring R is called a subring of R if and only if S is a subgroup of R under addition and S is closed under multiplication.

Example 20: $(\mathbf{Z}, +, \cdot)$ and $(\mathbf{Q}, +, \cdot)$ are subrings of $(\mathbf{R}, +, \cdot)$.

Summary:

In this section we have discussed binary operations, and algebraic structures. The properties of binary and homomorphisms are discussed. Two important algebraic structures group and ring are also treated. In a group the definition, subgroup and order of a group and an element are discussed. In rings you have seen various kinds of rings, ring homomorphism and subrings.



Self - Check Exercises

1) In the following determine whether the system described are groups. If they are not point out which of the group axioms fail to hold:

a) $G = \mathbf{Z}$, $a \Delta b = a - b$

b) $G = \{ a_0, a_1, a_2, \dots, a_6 \}$ where

$$a_i \Delta a_j = \begin{cases} a_{i+j} & , \text{if } i+j < 7 \\ a_{i+j-7} & , \text{if } i+j \geq 7 \end{cases}$$

c) $G = \{ \frac{a}{b} \mid a, b \in \mathbf{Z}, b \text{ is odd} \}$ $\frac{a}{b} \Delta \frac{c}{d} = \frac{a}{b} + \frac{c}{d}$

2) If (G, Δ) is a group such that $(a \Delta b)^2 = a^2 \Delta b^2$, $\forall a, b \in G$, show that G is abelian.

3) Show that if every element of a group G is its own inverse, then G is abelian

4) Show that any cyclic group is abelian. Give an example to show that the converse is false.

5) Let G be a group. Then show that the map $f: G \rightarrow G$ given by $f(a) = a^{-1}$ is an isomorphism if and only if G is abelian.

6) Show that the intersection of a non – empty family of subgroups of a group G is a subgroup of the group G . Can you say the same thing about the union?

7) If G is a group of even order, prove that it has an element $a \neq e$ satisfying $a^2 = e$.

8) If G is a finite group whose order is a prime number p , then G is a cyclic group.

9) Let R be a ring with unity. Show that the set of units of R forms a multiplicative group.

10) If f is a ring homomorphism from R_1 into R_2 , then show that

a) $f(0) = 0$

b) $f(-x) = -f(x)$, for every $x \in R_1$

11) Investigate an example of a ring having a subring S such that

- a) R has a unity and S does not have a unity
- b) R and S have the same unity
- c) R is non – commutative and S is commutative.

13) Let S and T be subrings of a ring R . Then Show that $S \cap T$ is a subring of R .

Section Three: Equivalence relations and Quotient structures

Overview



In this section you will study a way of getting a new algebraic structure given an equivalence relation and an algebraic structure. The problem you try to answer will be: - given an algebraic structure and an equivalence relation what binary operation can be defined on the quotient set so that the quotient set can be an algebraic structure by itself?

We will use two very important examples for our discussion. The algebraic structures that we form are the ring of integer modulo m , denoted by $\mathbf{Z}_m$ and the set of rational numbers $\mathbf{Q}$. Both are derived from $\mathbf{Z}$ and $\mathbf{N}$, in some sense.

Objectives

When you will have completed this section you will be able to:

- Define quotient rings
- Define rings of integer modulo m
- Define $\mathbf{Q}$
- Give examples of quotient structures
- Describe $\mathbf{Z}_m$ and $\mathbf{Q}$

Recall that If R is an equivalence relation on R set A , then the quotient set

$\bar{A} = A/R$ is the set of all distinct equivalent classes on A.

Example 1: The relation R on $\mathbf{Z}$ given by $x R y \Rightarrow x - y$ is a multiple of m,

$m \in \mathbf{N}$ is an equivalence relation (This was shown in Section Three of Module One)

The quotient set $\bar{\mathbf{Z}} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}\}$ is usually denoted by $\mathbf{Z}_m$.

Example 2: On $\mathbf{Z} \times \mathbf{Z}^*$ define $(a, b) R (c, d) \Leftrightarrow ad = bc$.

$\forall (a, b) \in \mathbf{Z} \times \mathbf{Z}^*$, $(a, b) R (a, b)$ because $ab = ba$ holds due to commutability of multiplication.

$\Rightarrow$ R is reflexive

$(a, b) R (c, d) \Leftrightarrow ad = bc$

$\Rightarrow bc = ad \Rightarrow cb = da \Rightarrow (c, d) R (a, b)$

$\Rightarrow$ R is symmetric

$(a, b) R (c, d) \wedge (c, d) R (e, f)$

$\Rightarrow ad = bc \wedge cf = de \Rightarrow adf = bcf \wedge bcf = bde$

$\Rightarrow adf = bde \Rightarrow af = be \Rightarrow (a, b) R (e, f) \Rightarrow R$ is transitive

$\therefore$ R is an equivalence relation

For the given equivalent relation if $(a, b) \in \mathbf{Z} \times \mathbf{Z}^*$,

$$\overline{(a, b)} = \{(x, y) \mid x \in \mathbf{Z}, y \in \mathbf{Z}^* \text{ \& } ay = bx\} = \{(x, y) \mid \frac{x}{y} = \frac{a}{b}\}$$

It is customary to denote $\overline{(a, b)} = \frac{a}{b}$.

Thus, the quotient set $\overline{\mathbf{Z} \times \mathbf{N}} = \{\overline{(a, b)} \mid a \in \mathbf{Z} \text{ and } b \in \mathbf{Z}^*\}$

$$= \left\{ \frac{a}{b} \mid a \in \mathbf{Z} \text{ and } b \in \mathbf{Z}^* \right\} = \mathbf{Q}$$

Our aim is to get algebraic structures from these quotient sets. This requires defining binary operations. The binary operations on quotient structures are defined as follows.



Let R be an equivalence relation on the set A . suppose $(S, *)$ is an algebraic structure we say R is compatible with $*$ if and only if

$$x R y \wedge u R v \Rightarrow x * u R y * v.$$

Now define a relation on $\bar{S} = S / R$, by $\bar{x} \bar{*} \bar{y} = \overline{x * y}$. If $*$ is compatible with the equivalence relation R , then $\bar{*}$ is a binary operation on the quotient set $\bar{S}$.

Proof Define $\bar{x} \bar{*} \bar{y} = \overline{x * y}$. Then $\forall \bar{x}, \bar{y} \in \bar{S}, x, y \in S$. Since S is closed

$$\text{under } *, x * y \in S \Rightarrow \overline{x * y} \in \bar{S} \Rightarrow \bar{x} \bar{*} \bar{y} \in \bar{S}$$

$$\Rightarrow \bar{S} \text{ is closed under } \bar{*}$$

To show well – defined ness:

Let $(\bar{x}, \bar{y}) \in \bar{S} \times \bar{S} \wedge (\bar{u}, \bar{v}) \in \bar{S} \times \bar{S}$. Suppose

$$(\bar{x}, \bar{y}) = (\bar{u}, \bar{v}) \Rightarrow \bar{x} = \bar{u} \wedge \bar{y} = \bar{v} \Rightarrow x R u \wedge y R v$$

But since R is compatible with $*$, it follows that $x * y R u * v$

$$\Rightarrow \overline{x * y} = \overline{u * v} \Rightarrow \bar{x} \bar{*} \bar{y} = \bar{u} \bar{*} \bar{v} \text{ by definition}$$

$$\Rightarrow \bar{*}(\bar{x}, \bar{y}) = \bar{*}(\bar{u}, \bar{v}) \Rightarrow \text{It is well - defined}$$

Example 3: For the Example 1, R is compatible with $+$ & $\times$ and $\mathbf{Z}$.

To see this

Suppose $x R y \wedge u R v$

$$\Rightarrow x - y \text{ \& } u - v \text{ are multiples of } m$$

$$\Rightarrow x - y = mk \text{ \& } u - v = ml, \text{ for some } m, k, l \in \mathbf{Z} \quad (1)$$

$$\Rightarrow x - y + u - v = mk + ml$$

$$\Rightarrow (x + u) - (y + v) = m(k + l)$$

$$\Rightarrow x + u - (y + v) \text{ is a multiple of } m$$

$$\Rightarrow (x + u) R (y + v)$$

$\Rightarrow$ R is compatible with +.

Similarly $x R y \wedge u R v$

$\Rightarrow x = y + mk \wedge u = ml + u,$ from (1)

$\Rightarrow x \times u = (y + mk) \times (v + ml) = yu + yml + vmk + m^2lk$

$\Rightarrow xu - yu = m(yl + vk + mlk)$

$\Rightarrow (xu)R(yu) \Leftrightarrow (x \times u) R (y \times v).$

$\Rightarrow$ R is compatible with $\times$

Hence $(\mathbf{Z}_m, \bar{+}, \bar{\times})$ given by

$\bar{x} \bar{+} \bar{y} = \overline{x+y}$ & $\bar{x} \bar{\times} \bar{y} = \overline{xy}$ is an algebraic structure.

Note If $(A, *)$ is an algebraic structure such that there is an equivalence relation on A, compatible with *, then $(\bar{A}, \bar{*})$ is an equivalence relation by the above theorem.

Define $f:A \rightarrow \bar{A}$ by $f(x) = \bar{x}$. Then $f(x * y) = \overline{x * y} = \bar{x} \bar{*} \bar{y}$

$= f(x) \bar{*} f(y) \Rightarrow f$ is a homomorphism

And for any $\bar{y} \in \bar{A}$ take $x = y \Rightarrow f(x) = f(y) = \bar{y} \in \bar{A} \Rightarrow f$ is onto.

Therefore, f is an epimorphism. f is called the canonical map on A.

Now by a theorem on epimorphisms, it follows that if * is commutative the $\bar{*}$ is commutative and so on. Hence if $(A, *)$ is a group then $(\bar{A}, \bar{*})$ is also a group and if $(A, *, \Delta)$ is a ring so is $(\bar{A}, \bar{*}, \bar{\Delta})$.

For our example, It follows that $(\mathbf{Z}_m, \bar{+}, \bar{\times})$ is a commutative ring with unity since $(\mathbf{Z}, +, \times)$ is a commutative ring with unity.

Theorem If m is prime then $(\mathbf{Z}_m, \bar{+}, \bar{\times})$ is a field

Proof: We only need to show that $(\mathbf{Z}_m, \bar{+}, \bar{\times})$ has no divisor of zero. For

$\bar{r} \bar{\times} \bar{s} \in \mathbf{Z}_m, \bar{r} \bar{\times} \bar{s} = \overline{rs} = \bar{0}$ if and only if $rs = kp$, for some q in $\mathbf{Z}$.

Since, p is a prime p divides the product rs if and only if p divides either r or s , i. e.

$\bar{r} = \bar{0}$ or $\bar{s} = \bar{0}$. Hence Z_p has no divisors of zero. Therefore Z_p is an integral domain. But a finite integral domain is a field.

?

Construct the tables for $(Z_5, \bar{+}, \bar{\times})$ and $(Z_6, \bar{+}, \bar{\times})$ as examples for the above theorem.

Given any integral domain D , it is possible to construct a quotient ring from it. Let us state a theorem to this effect. In our construction we will imitate the way $\mathbf{Q}$ is constructed from $\mathbf{Z}$ in , say freshman mathematics.

Motivation:

Let D be the integral domain under consideration. Our aim is to construct a field of elements of the form $\frac{a}{b}$, where $a, b \in D$, and $b \neq 0$. In D , $\frac{a}{b}$ might not have any meaning. Continuing with our imitation we have to answer

- When is $\frac{a}{b} = \frac{c}{d}$?
- What is $\frac{a}{b} + \frac{c}{d}$?
- What is $\left(\frac{a}{b}\right)\left(\frac{c}{d}\right)$?

To answer these questions let them have the meaning they have in $(\mathbf{Q}, +, \cdot)$. So,

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$$

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{and}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

But how can this be achieved using D? First we will state a definition. We say a ring R_1 can be imbedded in to a ring R_2 iff there is a monomorphism from R_1 into R_2 .

Theorem: Every integral domain can be imbedded into a field.

Proof: Let M be the set of all ordered pairs of the form (a, b) where $a, b \in D$ and

$b \neq 0$ (Think of (a, b) as $\frac{a}{b}$). On M define a relation R as follows.

$(a, b) R (c, d)$ if and only if $ad = bc$.

You can follow example 2 to show that R is an equivalence relation.

Now let $F = \{ \overline{(a, b)} \mid \text{where } (a, b) \in M \}$. F is the candidate for the field that we want to construct. We need to define addition and multiplication on F . Based on our motivation we mentioned before, define

$$\overline{(a, b)} + \overline{(c, d)} = \overline{(ad + bc, bd)} \quad \text{and} \quad \overline{(a, b)} \overline{(c, d)} = \overline{(ac, bd)}$$

Since D is an integral domain and both $b \neq 0$ and $d \neq 0$ we have that $bd \neq 0$. Thus

$\overline{(ad + bc, bd)} \in F$. You will be asked to show that $+$ is well – defined. Similar

reasoning as above shows that $\overline{(a, b)} \overline{(c, d)} \in F$. Here $\overline{(0, b)}$ is the zero element,

$\overline{(-a, b)}$ is the inverse of $\overline{(a, b)}$ and F is an abelian group under $+$. You can easily

show that the non – zero elements of F form a group under multiplication with unity

$\overline{(d, d)}$, $d \neq 0$. The inverse of $\overline{(c, d)}$ in F , with $c \neq 0$, is $\overline{(d, c)}$. Routine computation is

required to show that distributivity holds in F . Thus, we conclude that F is a field.

Now we are ready to show that D can be imbedded in F . Note that if $x \neq 0$ and

$y \neq 0$ in D , since $(ax)y = x(ay)$, it follows that $\overline{(ax, x)} = \overline{(ay, y)}$. Let us denote $\overline{(ax, x)}$

by $\overline{(a, 1)}$. The monomorphism that imbeds D into F is given by

$f: D \rightarrow F$ by $f(a) = \overline{(a, 1)}$. This completes the proof.

F is usually called the field of quotients of D . When $D = \mathbf{Z}$, $F = \mathbf{Q}$ the set of rational numbers.

Summary

In this section you discussed how you can construct a quotient structure given an algebraic structure on which an equivalence relation is defined. Compatibility of the binary operation and the equivalence relation are considered. A theorem on how to embed an integral domain into a field is also discussed.



Self - Check Exercises

- 1) Show that the addition and multiplication in the above theorem are well defined.
- 2) Prove the distributive law holds in F of the above theorem.
- 3) Prove that the mapping $f: D \rightarrow F$ defined by $f(a) = \overline{(a,1)}$ is a monomorphism.
- 4) On $\mathbf{Z} \times \mathbf{Z}$ define addition and multiplication by

$$(a, b) + (c, d) = (a + c, b + d) \text{ and } (a, b) \bullet (c, d) = (ac, bd).$$

- a) Show that $(\mathbf{Z} \times \mathbf{Z}, +, \bullet)$ is a commutative ring with unity.
 - b) Define R on $\mathbf{Z} \times \mathbf{Z}$ by $(a, b) R (c, d)$ if and only if $a + d = b + c$. Is R an equivalence relation? If so is R compatible with the operations?
- 5) Let $G = \{f \mid f: \mathbf{R} \rightarrow \mathbf{R} \text{ and } f \text{ is continuous}\}$ under addition of functions is a group.
- a) Show that $H = \{f \in G \mid f(0) = 0\}$ is a subgroup of G
 - b) Define a relation R on G by $f R g \Leftrightarrow f - g \in H$. Show that R is an equivalence relation.
 - c) Consider the set $S = \{ \overline{f}_a \mid a \in \mathbf{R} \text{ and } f(0) = a \}$. Then $S \subseteq G/H$. Show that elements of S are distinct.
 - d) Show that $S = G/H$.
 - e) Show that R is compatible with $+$ of G .
 - f) Show that $(\mathbf{R}, +) \cong (G/H, +)$. (Hint: Show that $F: \mathbf{R} \rightarrow G/H$ given by $F(a) = \overline{f}_a$ is an isomorphism.)