

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

Definition: 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 $*$

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 $(G, \circ)$ 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 $g(x) = w$.

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

Therefore $f \circ g$ is a 1-1 correspondence from $\mathbf{R}$ into $\mathbf{R}$.

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

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:

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

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 $(\mathbf{R}, +)$

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

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

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

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

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

Example 9: Let $(G, *)$ be a group and $a \in G$. Let $\langle a \rangle = \{a^i \mid i \in \mathbb{Z}\}$. 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 $(S_3, \circ)$ in Example 6,

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

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

$\circ$	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.

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 $\mathbf{E}$ is the set of even integers.

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

$+$	0	1	2	3	$\times$	0	1	2	3
0	0	1	2	3	0	0	0	0	0
1	1	2	3	0	1	0	1	2	3
2	2	3	0	1	2	0	2	0	2
3	3	0	1	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:

$$\text{For } x = (a, b) \text{ and } y = (c, d), x \bullet y = (ac - bd, ad + bc).$$

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

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

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

$$\text{Similarly, } 0 \times a = 0.$$

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

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

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

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

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

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

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

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

$$f(x + y) = f(x) + f(y) \text{ and } f(xy) = f(x)f(y)$$

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

Definition: 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: $(\mathbb{Z}, +, \cdot)$ and $(\mathbb{Q}, +, \cdot)$ are subrings of $(\mathbb{R}, +, \cdot)$.



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

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 .