LECTURE NOTE ON ABSTRACT ALGEBRA I

Chapter · March 2020

CITATIONS
0

READS
5,683

1 author:

Abednego Orobosa Isere
Ambrose Alli University
30 PUBLICATIONS **67** CITATIONS

SEE PROFILE

LECTURE NOTE ON ABSTRACT ALGEBRA I

BY

A.O. Isere

ξ_1

GROUP THEORY

Let S be a non-empty set, and $*$ a binary operation. If $*$ is defined on S, then $(S, *)$ is a groupoid. If the groupoid is associative with respect to the binary operation $*$ then it is called a semi group. What makes a semi group a group?

Definition 5.1

A group is a non-empty set G together with a binary operation $'*'$ such that the following laws hold:

i. Closure law: For every $a, b \in G$ then $a * b \in G$. We assert that G is closed with respect to the operation.

ii. The associative law: There exists an element e of G such that $e * a = a = a * e$ for every element of G. (This implies the existence of an identity).

iii. Inverse law: if $a \in G$ implies that there exists an element $x \in G$ such that $a * x = e = x * a$. We say that there exists an inverse element in G.

Remarks 5.1.1

(a) If the above laws is true for a non-empty set G, then we call G a group and denote it as $(G, *)$ where $*$ is the binary operation.

(b) If it customary to call the operation $'*'$ either addition or 'multiplication'. We shall also call $'e'$ in (iii) the identity element of the group G and x in (iv) we call the inverse of $'a'$ in the group G.

(c) A group $(G, *)$ is always a semi group, but a semi group may not be a group.

(d) A semi group with an identity element $'e'$ is called monoid. An invertible monoid is a group.

(e) It is to be noted that $'e'$ is 1 when the binary operation $'*'$ is multiplication, then we write $a * b$ as ab, and the inverse law takes the form: given $a \in G \; \exists \; a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = 1$.

If $*$ is addition, then e is taken as 0 and we write $a * b$ as $a + b$ and the inverse law takes the form: given $a \in G, \; \exists - a \in G$ such that $a + (-a) = 0 = (-a) + a$.

Without loss of generality whatsoever we will refer to $(G, *)$ as G and $'e'$ as multiplicative or additive identity and the inverse a multiplicative or additive inverse depending on whether the operation is multiplication or addition.

(f) Let $(G, *)$ be groupoid or a magma. If for any $a, b \in G$, the system of equations: $a.x = b$ and $y.a = b$ have unique solutions in G for x and y for all $x, y \in G$ respectively, then $(G, *)$ is called a gussigroup.

(g) If there exists a unique element e in a gussigroup $(G, *)$, $'e'$ being called an identity element such that $x.e = x = e.x$ for all $x \in G$, then $(G, *)$ is called a loop.

ξ_2

UNIQUENESS OF IDENTITY AND INVERSE ELEMENTS IN A GROUP

Preposition 5.2

Let $(G, *)$ be a group with respect to a binary operation $*$, then:

i. For each $a \in G, \exists$ a unique element $e \in G$ such that $a * e = a = a * e$.

ii. If $a \in G$ implies that $x \in G$ (x unique) such that $a * x = e = x * a$

Proof:

To show that identity element e is unique in G. Suppose $'e'$ is not unique in G (proving by contradiction) Then let e^1 also be an identity element in G.

$e^1 * e = e * e^1$ (1)

$e * e^1 = e^1 * e = e$ (2)

From (1) and (2)

$e^1 = e * e^1 = e$

$\Rightarrow e^1 = e \ and \ e$ is unique

To show the uniqueness of inverse in a group.

Suppose that x is not unique (proving by contradiction) then let $x^1,\ x^{11}$ be inverse elements of x in G. We have by the laws that $\exists\ x^1 \in G$

Such that $x^1 * x = e = x * x^1 - - - - - - - -$ (1)

Since $*$ is a binary operation

$$x^{11} * x = e = x * x^{11} - - - - - - - - - - -(2)$$

Combining (1) and (2) we have

$$x * x^1 = x * x^{11}$$

Hence $x^1 = x^{11}$ and so x is unique.

Example 5.2.1

(i) The set Z of all integers, with the operation "$*$" taken as the usual operation '+' of addition is a group, denoted as $(Z, +)$

(ii) $(Q, +)$, Q being a set of rational numbers is a group with respect to $' + '$ (addition)

(iii) $(R, +)$, R being a set of real numbers is a group with respect to $' + '$

Other examples of group are $(Q = \{0\},\ .)$, $(R = \{0\},\ .)$ and $(C = \{0\},\ .)$etc. There are trivial examples.

Example 5.2.2

Show that the set C of complex numbers consisting of $\{1, -1, i, -1\}$ with the operation of multiplication is a group.

Solution

Considering one element multiplying the others at a time will yield the required result. However we are going to tabulate the results of the multiplication of each of the elements:

.	(1)	-1	i	$-i$
1	(1)	-1	$-i$	$-i$
-1	-1	(1)	$-i$	i
i	i	$-i$	-1	(1)
$-i$	$-i$	$-i$	(1)	-1

Table 5.1

At a glance you can see all the results

Let examine C for a group

i. Closure law: C is closed with respect to the operation $'.'$ because all the result in the table make up the elements in the set C.

ii. $(1\ .\ 1)(-1) = -1 = 1(1\ .\ (-1))$

This is true for similar arrangements of the element presented in table 5.1

Thus we say, C is associative

iii. Since the operation is multiplication $(.)$. The multiplicative identity is 1 and is present in the set.

iv. For each element in the set, the inverse law holds. Let's circle the product that yields 1, each of the element is an inverse to the other.

(a) 1 is an inverse to itself.

(b) -1 is an inverse to itself

(c) $-i$ is an inverse to i

(d) i is an inverse to $-i$

Thus, $C = \{1, -1, i, -i\}$ is a group with respect to multiplication. Then, you are at liberty to write it as $(C, .)$

Example 5.2.3

The set of positive integers is not a group under ordinary addition of integers due to the following reasons.

There exists no identity element and each of the element 1, 2, 3, ... has no inverse element under ordinary addition.

Example 5.2.4

The set of natural numbers N under ordinary addition is not a group. Though $\exists$ an identity element but each of the element has no inverse element.

The set Z^+ under multiplication is left to the reader to state whether it is a group or not and outline his reason(s).

Example 5.2.5

Let $(G, *)$ be a group with respect to a binary operation $'*'$, then if b, c are elements of G the equation $c * x = b$ has a unique solution in $(G, *)$.

Proof:

Let b, c be elements of a group $(G, *)$. We want to show that the equation $c * x = b$ has a unique solution in $(G, *)$. Now $c * x = b$ implies $c^{-1} * c * x = c^{-1} * b$, by the inverse and associative laws in $(G, *)$ since $'*'$ is closed for being a binary operation where $c^{-1} \in G$ such that $c^{-1} * c = c * c^{-1} = e$. Thus by the identity law $x = e * x = c^{-1} * b$. So, the equation has a solution $x = c^{-1} * b$. Let us show that it is unique in $(G, *)$. If x^1, x^{11} are elements of G such that $c^{-1} * c = c * c^{-1} = e$ and so, since $*$ is a binary operation$c^{-1} * (c * x^1)$ equals $c^{-1} * (c * x^{11})$.

Thus by associative law in $(G, *)$, we have that

$$x^1 = e * x^1 = (c^{-1} * c) * x^1 = c^{-1} * (c * x^1)$$
$$= c^{-1} * (c * x^{11}) = (c^{-1} * c) * x^{11}$$
$$= e * x^{11} = x^{11}$$

Thus, there is only one such element $x = c^{-1} * b$ satisfying $c * x = b$ in $(G, *)$. So, the solution of the equation is unique in $(G, *)$.

Corollary 5.3

Let a be an element of a group $(G, *)$. If b is a right inverse of a and c a left inverse of a, then $b = c$.

Proof:

Let e be the identity element of G. Since b is a right inverse of a, $a * b = e$.

Also $c * a = e$ by hypothesis. So $c = c * (a * b) = (c * a) * b = e * b = b$. Thus $c = b$.

Remark 5.3.1

5.3 is known as the cancellation law.

Definition 5.4

A group $(G,*)$ is said to be commutative or Abelian if $a * b = b * a \quad \forall \ a, b \in G$.

Examples of abelian groups are (i) $(Z, +)$, $(Q, +)$, $(R, +)$ and $(C, +)$ etc.

Remark 5.4.1

(i) Abelian is from the name Abel. This property was named after a French mathematician name Niel Hennik Abel (1820 – 1829).

(ii) All abelian goups are groups all groups are not abelian groups.

Definition 5.5 (Order of an element)

Let a be an element of a group G and e, the identity element of G. The smallest positive integer n such that $a^n = e$ is called the order of a.

If no such n exists a is said to have infinite order.

The order of a group G written $|G|$ is the cardinal number of elements of G. G is said to be finite or infinite according as its order is finite or infinite.

Example 5.5.1

(i) $1 \in (Z, +)$ has infinite order

(ii) $[1] \in Z_n$ has finite order

Theorem 5.6

Let a, b be two elements of a group G

Then

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

(ii) $(a^{-1})^{-1} = a$

Proof:

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

$= b^{-1}(e\ b)$

$= b^{-1}\ b = e$

Where e is the identity element of G. So $b^{-1}a^{-1}$ is then inverse of $a\ b$. Generally if $a_1, a_2, \ldots\ldots, a_n$ are elements of G, $(a_1\ a_2 \ldots, a_n)^{-1} = {a_n}^{-1}\ {a_{n-1}}^{-1}, \ldots\ldots, {a_1}^{-1}$

(ii) Is left as an exercise

Theorem 5.7

Let a, b, c be elements of a group G.

Then

(i) $ab = ac$ implies that $b = c$, i.e. left cancellation law holds

(ii) $ba = ca$ implies that $b = c$, i.e. right cancellation law holds.

Proof:

(i) $b = e\ b = (a^{-1})b$

$= a^{-1}(ab)$

$= a^{-1}(ac)$

$= (a^{-1}a)c = ec = c$

$\Rightarrow \quad b = c$

(ii) Let e be the identity element of G

$b = b\ e = b(aa^{-1}) = (ba)a^{-1}$

$= (c\ a)a^{-1}$

$= c(a\ a^{-1}) = c\ e = c$

Exercise

(i) Let G be a group and b a fixed element of G. Prove tha the map G into G given by x into bx is bijective.

(ii) Let G be a group and g be an element of G. Prove that (a) $(g^{-1})^{-1} = g$. (b) $g^m\ g^n = g^{m+n}$.

(iii) Show that $(Z_4, +)$ is a group. Hence find the order of the group and of the element $2 \in Z_4$, if it exists.

ξ_3

SUBGROUPS

Definition 5.8

The subset H of a group G is called a subgroup of G if H is also a group under the "same" binary operation as that of G, i.e. if $(G,*)$ is a group, a subset H of G is a subgroup if $(H,*)$ is also a group.

Remark 5.8.1

When H is a subgroup of G, we write $H \leq G$. One can easily deduce from this definition that every subgroup of an abelian group is abelian.

Example 5.8.2

(i) If G is any group and e its identity then both G and $\{e\}$ are subgroups of G called trivial subgroups.

(ii) Let n be a fixed positive integer and $nZ = \{nz / z \in Z\}$. Then nZ is a subgroup of $(Z, +)$.

(iii) The set of all integers is a group under addition and the set S of all even integers
i.e. $S = \{0, \pm 2, \pm 4, \ldots\}$ is a subgroup.

(iv) Let $S = Z$ or R or C. Suppose that H is the subset of $M_{2,3}(S)$ consisting of elements of the form

$\begin{pmatrix} a_{11} & a_{12} & 0 \\ 0 & a_{22} & a_{23} \end{pmatrix}$ then $(H, +)$ is a subgroup of $(M_{2,3}(S), +)$

(v) $(R = \{0\}, \circ)$ is not a subgroup of $(R, +)$ nor of $(R, .)$. Subgroups other then $\{e\}$ and G are called proper subgroups. And if $a \in G$, then the set of all powers of $'a'$ i.e. $\{a^n : n = 0, \pm 1, \pm 2, \dots\}$

Writing it multiplicatively is a subgroup of G with : $a^0 = e, a^{-m} = (a^{-1})^m = (a^m)^{-1}\ a^0 = e,\ a^{-m} = (a^{-1})^m,\ (a^m)^{-1} = a^{-m},\ a^m a^n = a^{m+n}$

Preposition 5.9

A non-empty subset S of a group G with respect to a binary operation $' * '$ is a subgroup of $(G,*)$ if, and only if, the following two conditions hold:

(i) If $a,\ b \in S$ and $a * b \in S$, and

(ii) If $a \in S$ then $a^{-1} \in S$, where or a^{-1} denotes the inverse of a in $(G,*)$.

"Only if" part

Proof:

Let S be a non-empty subset of G, where $(G,*)$ is a group. Let us prove the only if part. If S is a group under $' * '$ then since $' * '$ is a binary operation in S, when $a, b \in S$ we have that $a * b \in S$ and so (i) holds. Next, if $a \in S$ then by the inverse law in $(S,\ *)$, $\exists\ a^{-1} \in S$ such that $a^{-1} * a = a * a^{-1} = e$ where e is the identity element in $(S,\ *)$. Since S is a subset of G, $a^{-1} \in G$ and

$a = b \cdot c$. Since a^{-1} is unique, (ii) holds. This proves the only if part.

"If" part

Suppose (i) and (ii) hold. Since S is a non-empty subset of G, $'*'$ is a binary operation is S because of (i). Hence the associative law holds in S with respect to $'*'$. Since S is not – empty, $\exists\ a \in S$. Hence by (ii) $a^{-1} \in S$. Thus by (i) $e = a * a^{-1} \in S$. So $a^{-1} * a = e = a * a^{-1}$ and the identity law holds in S under $'*'$. Finally, by inverse law with b as e we have that a^{-1} is unique in $(G, *)$ for $a \in G$. Hence by (ii) $a^{-1} \in S$ if $a \in S$ and by its uniqueness, the inverse law holds in S with respect to $'*'$. Hence S is a group under $'*'$.

N.B Prop. 5.9. may be regarded as the necessary & sufficient condition for a subset to be a subgroup.

Example 5.9.1

Let us show that the set of all even integer is a subgroup of the group $(Z, +)$ of all integers under addition.

Solution

Let $S = \{even\ integer\}$, and let $(G, *)$ = the integers under addition i.e. $(G,*) = (Z, +)$ i.e. $G = Z$ and $'*'$ is $+$. Now 2 is an even integer so, S is non-empty. If $a = 2n,\ b = 2m$ where

$n, m \in Z$, then $a + b = 2n + 2m = 2(n + m)$ is even as $n + m \in Z$ by the closure law. So prop. 5.9. (i) is satisfied. Suppose $c \in S$. Then $c = 2n_0$ for some $n_0 \in Z$ so, by the inverse law in $(Z, +)$, $-n_0 \in Z \; and \; 0 = -n_0 + n_0 = n_0 - n_0$. Thus $-n_0 - n_0 = 2(-n_0)$ is an even integer and so belongs to S. Now $n_0 + n_0 - n_0 - n_0$ equals $n_0 + 0 - n_0 = n_0 - n_0 = 0$ by the inverse law in $(Z, +)$ where 0 is the identity in $(Z, +)$.

By the uniqueness of the solution of $(2n_0) + x = 0$ in $(Z, +)$, $2(-n_0) = -2n_0 = -c$. Hence $-c \in S$ as it is an even integer so (ii) of prop. 5.9 holds. Hence, S is a subgroup of $(Z, +)$.

OR

Let $(G, *)$ be an abelian group. Prove that if $\forall \; a \in G, \; a = a^{-1}$, then the group $G = \{a : a = a^{-1}, a \in G\}$ is a group

Proof:

If $a, b \in (G^1, *)$, then a = a^{-1} and $a * b = a^{-1} * b^{-1} = (b * a)^{-1} = (a * b)^{-1}$ then G^1 is closed. Next, $\forall \; a, b, c \in G^1$ then $(a^1 * b^{-1}) * c^{-1} = (b * a)^{-1} * c^{-1} = a^{-1} * (b^{-1} * c^{-1}) = a^{-1}((c * b)^{-1}) = (c * b)^{-1} * a^{-1} = ((a * b) * a)^{-1}$

$a^0 = e$

$a^{-1} * a^{-(-)} = a^0 = a^{-(-)} * a^{-1} \Rightarrow a^{-(-)}$ is the inverse of a^{-1}.

Example 5.9.2

Prove that if $(G, *)$ is a group such that $a = a^{-1}$ for every $a \in G$, then $(G,*)$ is Abelian.

Solution

Let $(G,*)$ be a group such that $\forall\ a \in G,\ a = a^{-1}$, then if $a,\ b \in G$ we have that $a^{-1} = a\ and\ b^{-1} = b$. Thus $a * b = a^{-1} * b^{-1} = (a * b)^{-1}$. Hence $*$ is closed as a binary operation. Now $(b * a) * (a^{-1} * b^{-1}) = \left((b * a) * a^{-1}\right) * b^{-1} \equiv (b * e) * b^{-1} = e$ where e is the identity of $(G, *)$ if we use the associative law in $(G,*)$.

Similarly $(a^{-1} * b^{-1}) * (b * a) = e$. Hence $(b * a)^{-1} = a^{-1} * b^{-1}$ (1). Note that (1) holds in every group! i.e. if $(G,*)$ is any group, then for any $a, b \in G, (b * a)^{-1} = a^{-1} * b^{-1}$. Hence $(b * a)^{-1} = a^{-1} * b^{-1}$ if $a, b\ \in G$. Since $b * a \in G$ we have by our hypothesis that $b * a = (b * a)^{-1}$. Since a, b are any elements of G, we have that the group $(G,*)$ is abelian.

Example 5.9.3

If $(G, *)$ is a group and a is a fixed element of G, show tht $Ha = \{x \in G : x * a = a * x\}$ is a subgroup of $(G,*)$.

Solution

We shall use prop. 5.9. Now Ha is non-empty because $e \in Ha$ since $e * a = a * e$ and $e \in G$. Next, if $x^1, x^{11} \in Ha$ then

$x^1 * a = a * x^1$ and $x^{11} * a = a * x^{11}$ and so (by associative law in $(G,*)(x^1 * x^{11}) * a = x^1 * (x^{11} * a) = x^1 * (a * x^{11}) = (x^1 * a) * x^{11} = (a * x^1) * x^{11} = a * (x^1 * x^{11})$. Hence $x^1 * x^{11} \in Ha$. Finally, if $w \in Ha$ then $w * a = a * w$ and so $a = w^{-1} * (a * w) = (w^{-1} * a) * w$, hence $a * w^{-1} = w^{-1} * a$. Thus $w^{-1} \in Ha$. So, Ha is a subgroup of $(G,*)$.

ALTERNATIVELY

Let $Ha = \{x \in G : x * a = a * x\}$

$\Rightarrow e \in Ha$ since $e * a = a * e$ and $e \in G$. Then Ha is non-empty. Next consider two elements $x^1, x^{11} \in Ha$ then $x^1 * x^{11} = (x^1 * x^{11} * a = a * (x^1 * x^{11}) = (a * x^1) * x^{11} = a * (x^1 * x^{11})$ - by associative law. Hence $(x^1 * x^{11}) * a = a * (x^1 * x^{11})$. Thus $x^1 * x^{11} \in Ha$. Ha is closed under binary operation. Next we show inverse law.

Let $w \in Ha \Rightarrow a * w = w * a \,.\, a = (w * a) * w^{-1}$

$$= w * (a * w^{-1}) = (w * a) * w^{-1} = w * (a * w^{-1})$$

$$= w * (w^{-1} * a)$$

$$\Rightarrow w * (a * w^{-1}) = w * (w^{-1} * a)$$

Thus $a * w^{-1} = w^{-1} * a$. Thus $w^{-1} \in Ha$. So Ha is a subgroup of $(G,*)$.

Example 5.9.4

If H and K are subgroups of $(G,*)$. Show that the intersection $H \cap K$ is a subgroup of $(G,*)$.

Proof:

Let $H \cap K = \{x: x \in H \; and \; x \in K\}$ obviously $H \cap K$ is non-empty since $e \in H \; and \; e \in K$ being subgroups implies that $e \in H \cap K$.

Next, let $x^1, x^{11} \in H \cap K \Rightarrow x^1 \in H \; and \; x^1 \in K$ (1) and $x^{11} \in H \; and \; x^{11} \in K$ (2). From (1) $x^1 \in H \cap K \; and \; \Rightarrow x^1 * x^{11} \in H \cap K \Rightarrow x^1 * x^{11} \in H \; and \; x^1 * x^{11} \in K$.

Thus $x^1 * x^{11} \in H \cap K$ so, $H \cap K$ is closed as $*$ being a binary operation.

Next $a \in H \cap K \Rightarrow a \in H \; and \; a \in K$, since $H \; and \; K$ are subgroups, $a \in H \Rightarrow a^{-1} \in K \; and \; a \in K \Rightarrow a^{-1} \in K$. Thus $a^{-1} \in H \cap K$. Thus $H \cap K$ is a subgroup of $(G, \; *)$.

Example 5.9.5

Let G consist of the real numbers $1 \; and \; -1$ only. Show that G is an abelian group under the multiplication of real numbers.

Solution

This is a particular example where G is defined and binary operation defined also.

$G = \{1, -1\}, \qquad *='.'$

Using a table will help us see the results at a glance.

	1	-1
1	1	-1
-1	-1	1

Table 5.2

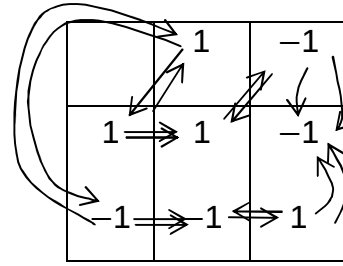

Table 5.3

(i) Clearly G is closed under $'.'$

(ii) Associative law holds, because it simply means operating the results once more which gives back the equality of the results in any direction. The arrows in Table 5.3 shows associativity.

(iii) $1 \in G$. 1 is the multiplicative identity

(iv) 1 is the inverse of -1

Thus $(G = \{-1, 1\},\ .)$ is a group.

Next we show commutatively, the law is $a * b = b * a\ \forall,\ a, b \in G$

Consider $1 . 1 = 1 . 1 = 1$

$-1 . 1 = 1 - 1 . 1 = -1$

Thus $(G = \{-1,\ 1\},\ .)$ is an abelian.

Theorem 5.10

Let H be a non-empty subset of a group G the following are equivalent

(a) H is subgroup of G

(b) For $a,\ b, \in H, ab^{-1} \in H$

(c) (i) For $a, b \in H,\ ab \in H$

(ii) For any $a \in H,\ a^{-1} \in H$

***Proof*:**

$(a) \Rightarrow (b)$. By definition of subgroups, H is a group and so given $b \in H$, its inverse b^{-1} exists in H. So, by closure property $ab^{-1} \in H$, for any $a \in H$.

$(b) \Rightarrow (c)$. Let $a \in H$. Then by $aa^{-1} = e \in H$ where e is the identity element of G. If b is any element of H, then by (b) again, $eb^{-1} = b^{-1} \in H$. So c (ii) is satisfied. Thus given, $a, b \in H$, then, $b^{-1} \in H\ and\ a(b^{-1})^{-1} \in H$ by (b). That is, $ab \in H$. So c(i) is satisfied.

$(c) \Rightarrow (a)$. Suppose (i) and (ii) of (c) are satisfied, then in view of 5.1 we only have to show that associative law holds and that the identity element exists in H. Now for $a, b, c\ in\ H, (a\ b)c$ and $a(bc)$are elements of H by repeated application of (i) and they are equal in H, since they are equal in G. So associative law holds in H. Given any $a \in H$, then by (ii) $a^{-1} \in H$ and by (i) $a\ .\ a^{-1} = e \in H$, where e is the identity element of G. This e is obviously the identity element of H.

Remark 5.10.1

The above is simply a characterization of a subgroup.

Definition 5.11

If H is a subgroup of G and $H \neq G$, $H \neq \{e\}$, then H is called a proper subgroup of G.

Theorem 5.12

Let $(H\alpha\}\alpha \in \Omega$ be a family of subgroups of a group G then

$$\bigcap_{\alpha\in\Omega} H\alpha$$

Is also a subgroup of G.

***Proof* – exercise.**

$$\xi_4$$

COSETS OF A GROUP

Definition 5.13

By a right coset of a subgroup S of a group $(G,*)$ is meant that set $Sa = \{sa : s \in S\}$ where a is a fixed element of G. Similarly, a left coset of a subgroup S of a group $(G,*)$ is $aS = \{as : s \in S\}$ where a is a fixed element of G, multiplicatively. for the addition notation, a right coset of S is $S + a = \{s + a : s \in S\}$ and a left coset $a + S = \{a + s : s \in S\}$.

Theorem 5.14

Each coset (right or left) has the number of elements as S i.e. there is a bijection from S to Sa $(or\ aS)$. Two right cosets $Sa\ and\ Sb$ are either identical or disjoint i.e. $sa = sb\ or\ sa \cap sb = \emptyset$. It is similar for the left cosets.

***Proof*: Exercise**

Remark 5.14.1

If G is abelian the right coset coincides with the left coset.

Definition 5.15

The set of all right cosets of H in G is called the right quotient set of G by H and denoted by G/H. Define the left quotient set of G by H analogously, and denote it by G/H.

Lemma 5.15.1

$$|G|H| = |G|/|H|$$

***Proof*: exercise**

Definition 5.16

Let G be a group and Ha subgroup of G. If G/H is finite set then $|G/H|$ is called the index of H in G i.e. the number of right (or left) cosets of H in G.

Example 5.16.1

Let $G = (Z, +)$. For any $n \in Z, (nZ, +)$ is group of finite index $n\ in\ Z$.

Definition 5.17

Let H be a subgroup of a group G. A subset Y of G is called a right transversal for H in G if Y consists of exactly one element from each right coset of H in G. A left transversal is defined analogously.

Remark 5.17.1

(i) Always recall that we use G and $(G,*)$ interchangeably.

(ii) If G is abelian, just call Y a transversal for H in G.

Example 5.17.1

$Y = \{0, 1, 2, 3, 4\}$ is a transversal for $5Z$ in $(Z, +)$.

Theorem 5.18 (Lagrange's theorem)

The order of a subgroup S of a finite group $(G,*)$ always divides the order of the group $(G,*)$ and $|G| = |S||G|S|$.

Proof:

Suppose $|S| = m$ and $|G|S| = 1$ the right quotient sets of G give a partition of G. Also each coset has 1 element. So $|G| = 1m = |S||G|S|$ as required.

Exercise

1. Prove that if $a,\ b$ are any elements of a group $(G,*)$, then the equation $y * a = b$ has a unique solution in $(G,*)$.
2. From example 5.8.2, show that (ii) and (iv) are subgroups.
3. (i) Show that the set G of all non-zero complex numbers, is a group under the multiplication of complex numbers.

   (iii) Show that $H = \{a \in\in G : a_1^2 + a_2^2 = 1\}$, $(where\ a_1 = Re(a) and\ a_2 = 1m(a))$ is a subgroup of G.
4. Let $(G,*)$ be a group. Let $C = \{c \in G : c * a = a * c\ \forall\ a \in G\}$. Prove that C is subgroup of G. Hence or otherwise show that C is abelian.

   [Note that C is called the center of the group G].

5. If $(G,*)$ is a group such that $(a*b)^2 = a^2 * b^2$ (multiplicatively) for all $a, b\ in\ G$, show that G must be abelian.

PERMUTATIONS / SYMMETRIC GROUP

ξ_1 PERMUTATIONS

Definition 6.1

A permutation is a bijection $\theta: S \to S$, where S is finite. So, a permutation θ of n symbols is a bijection from the set of the n symbols onto itself.

Remark 6.1.1

A permutation is therefore a one – one mapping that is an onto provided the domain is a finite set.

Definition 6.2

A cycle of length of n, written as $(a_1\ a_2\ a_3 \dots a_{n-1}\ a_n)$ is a permutation θ of the form $\begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_{n-1} & a_n \\ a_2 & a_3 & a_4 & \dots & a_n & a_1 \end{pmatrix}$, that is $a_1 \overset{\theta}{\to} a_2 \overset{\theta}{\to} a_3 \dots a_{n-1} \overset{\theta}{\to} a_n \overset{\theta}{\to} a_1$ where $S = \{a_1, \dots, a_n\}$

Definition 6.3 (Symmetric Groups)

The set G of all permutations of n symbols is a group under composition of functions. It is called the symmetric group on n symbols (or n objects) and is denoted by S_n.

Remarks 6.3.1

(i) Let us also conceive the idea of symmetric groups in this way. For any T, recall that the set of all bijective mappings on T is a . This group is called the symmetric group on T or the group of

permutations of T and is denoted by S_T. If T is a finite set having elements we denote S_T by S_n by the symmetric group of degree n. Generally an element of S_n may be regarded as a permutation of integers $\{1, 2, \dots \dots, n\}$.

(ii) In summary: A symmetric group is a set of permutations of n symbols that forms a group under composition.

Definition 6.4

Let S_n be a symmetric group on n objects. If $S = \{a_1, \dots \dots, a_n\}$ then the identity element I of S_n is the permutation. $\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$ i.e. $a_i \xrightarrow{I} a_i \ for\ 1 \leq i \leq n$.

For any $\theta \in S_n, \theta^{-1}: S \to S$ such that $\theta\theta^{-1} = I$ and also $\theta^{-1}\theta = I$.

N.B. We shall also indicate I with ε.

Example 6.4.1

Let $S = \{1,2,3,4,5\}$. Then

$I = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$. If $S = \{1, 2, 3\}$ then

$S_3 = \{I, (1,2), (13), (2,3), (123), (132)\}$ has only six members i.e. 3! (3 factorial members only). In fact, S_n has only $n!$ members.

If $\theta = \begin{pmatrix} a_1 & a_2 & \dots & a_{n-1} & a_n \\ a_2 & a_3 & \dots & a_n & a_1 \end{pmatrix}$ then $\theta^n = I$. Note a permutation may or may not be a cycle e.g. $\theta(1) = 2, \theta(2) = 3, \theta(3) = 1, \theta(4) = 5, \theta(5) = 4$

i.e

S = {1,2,3,4,5} and $1 \overset{\theta}{\rightarrow} 2, 2 \overset{\theta}{\rightarrow} 3, 3 \overset{\theta}{\rightarrow} 1, 4 \overset{\theta}{\rightarrow} 5, 5 \overset{\theta}{\rightarrow} 4$

i.e. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$

However I is not also a cyclic permutation.

However, it can be expressed as a product of two cycles (1 2 3) and (4 5), and write θ = (1 2 3)(4 5).

Theorem 6.5

Any permutation $\theta: S \rightarrow S, (S\ finite)$ can be written as a product of cycles, the cycles acting as disjoint subsets of S.

Proof:

If $x_1 \in S$, Let $x_2 = \theta(x_1), x_3 = \theta(x_2)$, and so on. Since S is finite as some state we get $x_n = \theta(x_i)$ with $i < n$ where $n = o(S)$ (i.e. n is the number of points in S). Assuming $x_1, \ldots\ldots, x_{n-1}$ are all distinct.,

If $i \neq 1$, then $\theta(x_{n-1}) = x_i = \theta(x_{i-1})$. Since θ is injective, $x_{n-1} = x_{i-1}$ which contradicts assumption that x_1, for if $\theta^r(x_1) = \theta^s(x_1)$ with $0 < s < r$, we would have $\theta^{r-s}(x_1) = x_1$ with $r - s < r$ contradicting our choice of r that $r_1 = (x_1, x_2, \ldots\ldots x_r)$. We see that r_1 has the effects as θ on all elements of S appearing in this cyclic notation for r_1. Let x^1 be an element of S not appearing in this cyclic notation for r_1. Repeating

the above argument with the sequence $x_1^1, \theta(x^1), \theta^2(x^1), \ldots\ldots$, we arrive at a cyclic r_2. Now r_2 and r_1 are disjoints, for if they had any element y of S in common, they would be identical, since each cycle could be constructed by repeated application of the permutation θ starting at Y. Continuing, we pick an element in S not appearing in the cycle notations of either $r_1 \, or \, r_2$ and construct r_3, and so on. Since S is finite, this process must terminate with one r_m the product $r_1 \, r_2 \ldots r_m$, this clearly has the same effect on each element of S as θ does, so $\theta = r_1 \, r_2 \ldots r_m$. This proves the theorem.

Theorem 6.6

A cyclic permutation φ of n symbols has order n.

Proof:

Let $\varphi = (a_1 \, a_2 \ldots\ldots a_n)$ be a cyclic permutation of n symbols. So φ carries a_i into a_{i+1} $1 \leq i \leq n$, and a_n into a_1. Here φ^2 has the double effect of carrying each a_i into a_{i+2}, and generally φ^K carries a_i into a_{i+k}, where all subscripts are to be reduced modulo n, we have in φ^K the identity I if and only if, a_{i+k} equals a_i, that is iff, $k = 0 \, mod \, n$. The smallest K with $\varphi^K = I$ is then n itself, so φ does have the order n.

Theorem 6.7

The order of any permutation θ is the least common multiple of the lengths of its disjoint cycles.

Proof **:**

Write the permutation θ as the product $\theta = r_1 \dots r_r$ of disjoint cycles r_i (as Thm 6.5) if $i \neq j$, then r_i and r_j are disjoints, hence $r_i r_j = r_j r_j$, and the factors r_i may be rearranged in θ and in its powers, to give $\theta^n = {r_1}^n \dots {r_r}^n$ for all n. Therefore, $\theta^n = I$ iff every ${r_i}^n$ is the identity I^r. By theorem 6.6, this means $\theta^n = I$ n is a common multiple of the lengths of the ${r_r}^s$ from which the conclusion of theorem 6.7 follows

e.g. if $\varphi = (1\,2\,3)(4\,5)(i.e. \varphi(1) = 2, \varphi(2) = 3, \varphi(3) = 1, \varphi(4) = 5, \varphi(5) = 4) then\ \varphi^2 = (1\,3\,2)(4\,5)$

then

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$$

$$\varphi^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix} = (1\,3\,2)$$

$$\varphi^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix} = (4\,5)$$

$$\varphi^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix} = (1\,3\,2)$$

$$\varphi^5 = (1\,2\,3)(4\ 5)\ \ i.e.\ \varphi^5 \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

$$\varphi^6 = I\ \ i.e.\ \varphi^6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

So, the order of $\varphi = (1\,2\,3)(4\,5)$ in S_5 is 6. Since $\theta^n = 1 \Rightarrow n = o(S)$. By theorem 6.7 it is the l.c.m of the lengths of its disjoint cycles. In this case, the L.C.M. of the lengths of (1 2 3) and length of (4 5) which is the LCM of 3 and 2 i.e. 6. Note that disjoint cycles commute e.g. $(1\,2\,3)(4\,5) = (1\,2\,3)(4\,5) = (4\,5)(1\,2\,3)$ of course they may not commute if they have a point in common i.e. if they are not disjoint cycles.

Definition 6.8 (Transposition)

A transposition is a cycle of length 2 e.g. (1 2), (1 5). Thus, a transposition leaves all elements but two fixed, and maps each of these onto the other. Therefore, any cycle is a product of transposition.

Theorem 6.9

Every permutation is a product of transposition. E.g.

$(1\,2\,3) = (1\,3)(1\,2) i.e. \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$(1\,2\,3\,4) = (1\,4)(1\,3)(1\,2)$

Proof:

Since any cycle is a product of transpositions we have theorem 6.9 because any permutations can be written as a product of disjoint cycles.

Definition 6.10

A permutation θ is called even or odd according to whether it can be expressed as the product of an even number of transpositions or the product of an odd number of transpositions respectively. E.g. $(1\,2\,3) = (1\,3)(1\,2)$ is a product of two transpositions and two is even. A transposition is an odd permutation if the no of permutations is odd $(1,2,3,4)$ is odd because it is a product of three transpositions $(1\,2)(1\,3)$ and $(1\,4)$, and three is odd.

Theorem 6.11

If $n \geq 2$, the collection of all even permutations of a finite set of n elements forms a subgroup of order $n!/2$ of the symmetric group S_n. It called the alternating group on n letters (or the alternating group of degree n), and we denote it be A.

Example 6.11.1

(a) Express as products of disjoint cycles the permutations.

(i) $\theta(1) = 4, \theta(2) = 6, \theta(3) = 5, \theta(4) = 1, \theta(5) = 3, \theta(6) = 2$

(ii) $(1\,2\,3\,4\,5)(6\,7)(1\,3\,5\,7)(1\,6\,3)(1\,3\,5\,7)(6\,7)(1\,2\,3\,4\,5)$

Find the order of each of them

Solution

(a) (i)

$\theta = (1\,4)(2\,6)(3\,5)$

By theorem 6.7. the order of $\theta \in S_6$, is the L.C.M of 2, 2, 2, which is 2

(ii) $\varphi\ is \begin{pmatrix}1&2&3&4&5&6&7\\6&2&1&4&5&3&7\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7\\3&2&5&4&7&6&1\end{pmatrix}$

$\begin{pmatrix}1&2&3&4&5&6&7\\1&2&3&4&5&7&6\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7\\2&3&4&5&1&6&7\end{pmatrix}$

In S_7 which is $\begin{pmatrix}1&2&3&4&5&6&7\\2&5&4&7&1&6&3\end{pmatrix}$

i.e. $(1\,2\,5)(3\,4\,7) \Rightarrow$ disjoint sets with no things in common. Therefore, the order of φ is the L.C.M of 3 and 3 which is 3.

N.B: Disjoint permutations commute, the order of the permutations is therefore immaterial.

Example 6.11.2

Compute in S_9, $a^{-1}ba$, where $a = (1\,2)(1\,3\,5)$ and $b = (1\,5\,7\,9)$

Solutions

(i)

Now

$a = \begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&1&3&4&5&6&7&8&9\end{pmatrix}$

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\3 & 2 & 5 & 4 & 1 & 6 & 7 & 8 & 9\end{pmatrix}$$

$$= \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\3 & 1 & 5 & 4 & 2 & 6 & 7 & 8 & 9\end{pmatrix}$$

$$\therefore a^{-1} = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\end{pmatrix}$$

$$= \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\2 & 5 & 1 & 4 & 3 & 6 & 7 & 8 & 9\end{pmatrix}$$

Since $aa^{-1} = a^{-1}a = 1$

And

$$a = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\3 & 1 & 5 & 4 & 2 & 6 & 7 & 8 & 9\end{pmatrix}$$

$$b = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\5 & 2 & 3 & 4 & 7 & 6 & 9 & 8 & 1\end{pmatrix}$$

Hence $a^{-1}ba$

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\2 & 5 & 1 & 4 & 3 & 6 & 7 & 8 & 9\end{pmatrix}$$

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\5 & 2 & 3 & 4 & 7 & 6 & 9 & 8 & 1\end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 5 & 4 & 2 & 6 & 7 & 8 & 9 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 3 & 7 & 4 & 5 & 6 & 9 & 8 & 2 \end{pmatrix}$$

$\therefore$ (2 3 7 9) = $a^{-1}ba$

Example 6.11.3

Given the permutation a = (1 2)(3 4) b = (1 3)(5 6), find a permutation $x \in S$ such that $ax = b$

Solution

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 3 & 5 & 6 \end{pmatrix}$$

$$b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 4 & 6 & 5 \end{pmatrix}$$

$$x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \end{pmatrix}$$

Then

$ax = b$

$x = a^{-1}b$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \end{pmatrix} =$$

$$\begin{pmatrix} 2 & 1 & 4 & 3 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 4 & 6 & 5 \end{pmatrix}$$

$\therefore\ x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 2 & 3 & 6 & 5 \end{pmatrix}$

$i.e.$ (1 4 3 2)(5 6)

Definition 6.12

Let $\beta = \begin{pmatrix} 1 & 2 & \dots & n \\ b_1 & b_2 & \dots & b_n \end{pmatrix} \in S_n$

$$\text{Sign } \beta = \begin{cases} 1 \; if \; \beta \; is \; even \\ \\ -1 \; if \; \beta \; is \; odd \end{cases}$$

Example 6.12.1

Show that $(2\ 4\ 6)^3 = (1\ 3)^2 = \varepsilon$

To show

$$(2\ 4\ 6)^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 6 & 5 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 6 & 5 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 6 & 5 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \varepsilon$$

$$(1\ 3)^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 4 & 5 & 6 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 4 & 5 & 6 \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \varepsilon$$

Thus $(2\ 4\ 6)^3 = (1\ 3)^2 = \varepsilon$.

Remarks 6.12.2

(i) A cycle of length 2 squared gives an identity permutation. And a cycle of length 3 cubed also gives an identity permutation.

(ii) A transposition of length 2 is a cycle of length 2.

(iii) All transpositions are special kind of cycles but all cycles are not transpositions.

Exercise

(i) Prove that $|S_n| = n!$

(ii) Prove that for b in S_n, sign $b = sign\ b^{-1}$

ξ_2

CYCLIC SUBGROUPS

Definition 6.13

Let G by a group and $S \subseteq G$. $< S >$ is called the subgroup of G generated by S, or S is said to generate $< S >$. If S is a finite set then $< S >$ is said to be finitely generated.

Definition 6.14

Let $< S >$ be a subgroup generated by S and $S = \{a\}$, a singleton subset of G. Then $< a >$ is called a cyclic subgroup of G generated by a.

Definition 6.15

Let $< a >$ be a cyclic subgroup of G. A group G is said to be cyclic if $G =< a >$ for some element $a \in G$.

Example 6.15.1

(i) $(Z, +)$ is a cyclic group generated by {1}, i.e. $Z =< 1 >$.

(ii) $(Z_n, +)$ is a cyclic group generated by {[1]}, i.e. $Z_n = < [1] >$

Example 6.15.2

Show that S_3 is generated by $(1\ 2)(1\ 2\ 3)$

i.e. $S_3 =< \{(1\ 2), (1\ 2\ 3)\} >$

Solution

$S_3 = \{\varepsilon, (1\ 2), (2\ 3), (1\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$

Now we only need to show that every element of S_3 can be written as products of powers of $(1\ 2), (1\ 2\ 3)$

Recall: $(1\ 2)^2 = (1\ 2\ 3)^3 = \varepsilon$

Next: $(1\ 2) = (1\ 2)(1\ 2\ 3)$

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

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

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

Thus S_3 is generated by $(1\ 2),\ (1\ 2\ 3)$.

Remark 6.15.3

Observed that $< S >$ is the smallest of all subgroup of G containing S. i.e. $< S >$ is the intersection of all subgroups of G containing S.

Theorem 6.16

Let S be a subset of a group G. Suppose $< S >$ is the subset of G consisting of all finite products of elements of S and their inverses. Then $< S >$ is a subgroup of G.

Proof: **- exercise**

Theorem 6.17

The order of an element a in a group G is equal to the order of $< a >$, the cyclic subgroup of G generated by a.

Proof:

Recall that the order of $a \in G$ is n the smallest positive integer such that $a^n = e$. Since a cyclic subgroup of length two

need to be squared to give an identity element. Using remarks 6.12.2 (i) we conclude the proof.

To verify. In $G = S_2, < (12) >$ is a cyclic group of order $(12)^2 = \varepsilon, n = 2$ – the order coincides.

Example 6.17.1

In $G = S_3$, show that a cyclic subgroup of S_3 is of order 3.

Solution

In G, $< (1\,2\,3) >$ is a cyclic subgroup. But $(1\,2\,3)^3 = \varepsilon$ (identity element).

$\Rightarrow$ the order is (such that), the smallest positive integer that (1 2 3) be raised to give an identity element.

Theorem 6.18

Any subgroup of a cyclic group is cyclic.

Proof:

Let $G =< a >$ and $H \leq G$. Suppose r is the smallest positive integer such that $a^r \in H$. If $a^m \in H$, then $m = qr + s$ where $0 \leq s < r$. So, $a^m = (a^r)^q\, a^s$ i.e. $a^s = (a^r)^{-q}\, a^m \in H$. Thus $s = 0$ since $s < r$ and r is the smallest positive integer such that $a^r \in H$. i.e. $m = qr$ i.e. $H =< a^r >$. So, H is cyclic.

Theorem 6.19

Let $G =< a >$ by a cyclic group.

(i) If G is finite of order n, then the distinct subgroup of G are precisely the cyclic subgroups of G generated by a^d where d divides n.

(ii) If G is infinite then any a^r where r is any integer, generates a^r subgroup of G.

Proof:

In above, it was shown $H = < a^r >$ where $r|n$ it suffices to show that for any d which divides, powers of a^d form a subgroup of G. But it is trivial verifying that the equivalent theorem above (third part) holds.

(iii) One only has to verify that powers of a^r form a subgroup using the third part of the equivalent theorem above. Generally we write C_n for a cyclic group of order n.

Example 6.19.1

(i) Let $C_6 = < a >$. Since divisors of 6 are $1, 2, 3, 6$, the subgroups of C_6 are $\{\varepsilon\}, \{\varepsilon, a^2\}, \{\varepsilon, a^3\}, c_6$

(ii) Let $G = (Z, +)$. Since G is an infinite cyclic group, any integer generates a cyclic subgroup. So any subgroup of G has the form $(mZ, +)$, for any integer m.

Exercise

1. Let $n = 3$, $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

Then compute the following: (i) $\beta^{-1}\,\alpha$ (ii) $\alpha\,\beta^{-1}$ (iii) $\alpha^{-1}\beta$ (iv) $\alpha\,\beta\,\alpha^{-1}$

2. Let

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 7 & 8 & 6 & 5 & 1 & 4 \end{pmatrix} \in S_8$$

(i) Write α as a product of disjoint cycles

(ii) Write α as a product of transpositions if possible.

3. Represent $(1\ 4)(1\ 2\ 3)(4\ 5)(1\ 4)$ as a product of disjoint cycles and find its order.

4. Express $(1\ 2)(1\ 2\ 3)(1\ 2)$ as a product of disjoint cycles

5. Prove that there is no a in S_8 such that $a^{-1}(1\ 2\ 3)a = (1\ 3)(5\ 7\ 8)$.

6. Find the inverse of $(1\ 2\ 3)$ in S_9

MORPHISMS OF GROUPS, FACTORS AND NORMAL SUBGROUPS

In this chapter group morphisms or homomorphisms are introduced. Homomorphism is a mapping or function with an algebraic structure imposed on it. it can be injective (mono) and surjective (epi). For the sake of definition we state as below

ξ_1

HOMOMORPHISMS OF GROUPS

Definition 7.1

Let θ be a mapping from a group $(G, .)$ to a group $(H, *)$. Then θ is said to be a Homomorphism if for any $x, y \in G$. $\theta(x . y) = \theta(x) * \theta(y)$ holds θ is called a homomorphism.

Definition 7.2

A homomorphism that is injective (mono) is called a monomorphism.

Definition 7.3

A homomorphism that is surjective (epi) is called an epimorphism.

Definition 7.4

A homomorphism that is both injective and surjective is called an isomorphism.

Definition 7.5

A homomorphism of a group into itself is called an endomorphism

Definition 7.6

An endomorphism that is bijective is called an automotphism.

Example 7.7

Let G be the group of all real number under ordinary addition, and let H be the group of non-zero positive real numbers under multiplication. Then $\theta : G \to H$ given by $\theta(x) = e^x \; \forall \; x \in G$ is an isomorphism.

To show:

Consider $x, \; y \in G$, we have that

$\theta(x + y) = e^{x+y} = e^x . e^y = \theta(x) \; . \; \theta(x)$. Hence θ is a homomorphism.

Next, we show that it is bijective. (i.e. that θ is both injective and surjective) suppose that $\theta(x_1) = \theta(x_2) \; \forall \; x_1 \; x_2 \in G$.

Then $e^{x_1} = e^{x_2}$ (1)

Divide (1) by e^{x_2}

$$\frac{e^{x_1}}{e^{x_2}} = 1$$

$$\Rightarrow e^{x_1 - x_2} = e^0$$

$$\Rightarrow x_1 - x_2 = 0$$

Thus $x_1 = x_2$. Therefore θ is injective. If $a \in H$ then $a = e^{\log_e a}$

$= \theta(\log_e a)$ and $\log_e a \in G$.

So, $\theta(G) = H$.

Example 7.8

Let G be the group $(\{1, i, -1, -i\}, .)$ of the four complex numbers $1, i, -1 \; and \; -i$, under multiplication of complex numbers; and let H be the group $(\{1, -1\}, .)$ of the two complex $1 \; and \; -1$, under the same binary operation as G. Show whether θ is an isomorphism.

Define $\theta : G \to H \; by \; \theta(1) = 1, \theta(i) = -1, \theta(-1) = 1,$ and $\theta(-i) = -1$

Obviously, θ is a homomorphism. (But in pure mathematics, the obvious may not be sufficient, we go to show)

To show:

.	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Table 7.1

θ	1	-1	i	$-i$
1	1	1	-1	-1
-1	1	1	-1	-1
i	-1	-1	1	1
$-i$	-1	-1	1	1

Table 7.2

Observe that all elements in table 7.2 are elements in H, and that there are two sets of identical results : rows 1, 2, and rows 3, 4.

Row 1, 2

$\theta(1 . 1) = \theta(1) = 1 = \theta(1) . \theta(1)$

$\theta(1 . -1) = \theta(-1) = 1 = \theta(1) . \theta(-1)$

$\theta(1 . i) = \theta(i) = -1 = \theta(1) . \theta(i)$

$\theta(1 . -i) = \theta(-i) = -1 = \theta(1) . \theta(-i)$

Row 3, 4

$\theta(i . 1) = \theta(i) = -1 = \theta(i) . \theta(1)$

$\theta(i . -1) = \theta(-i) = -1 = \theta(i) . \theta(-1)$

$\theta(i . i) = \theta(i^2) = \theta(-1) = 1 = \theta(i) . \theta(i)$

$\theta(i . -i) = \theta(-i^2) = \theta(1) = 1 = \theta(i) . \theta(i)$

Hence, θ is actually a homomorphism.

Next, let show whether θ is injective:

$\theta(1) = 1\ and\ \theta(-1) = 1\ but\ 1 \neq -1$ also

$\theta(i) = -1\ and\ \theta(-i) = -1\ but\ i \neq -i$

So, θ is not injective.

Thus θ is a homomorphism but not an isomorphism.

Theorem 7.9

In a group homomorphism $\theta : G \to H$, then

(i) Identity element of G is mapped to the identity element of H, and

(ii) Inverses are mapped to inverses.

$i.e.(a)\ \theta(e_G) = e_H$ where e_G is the identity element of G and e_H is the identity element of H and $(b)\ \theta(x^{-1}) = (\theta(x))^{-1}$

Proof:

Since $e_G \cdot e_G = e_G$ we have $\theta(e_G \cdot e_G) = \theta(e_G)$ and so by the definition of homomorphism $\theta(e_G)\theta(e_G) = \theta(e_G)$. Hence $\theta(e_G) = \theta(e_G)$

$(\theta\ e_G)^{-1} = \theta(e_G)\ (\theta e_G)^{-1}$

Thus $\theta(e_G) = e_H$

(iii) If $x \in G$ then $xx^{-1} = e_G$ and so $\theta(xx^{-1}) = \theta(e_G)$. Hence by definition $\theta(x)\big(\theta(x^{-1})\big) = \theta(e_G) = e_H$, by (i), so, $\theta(x^{-1}) = (\theta(x)^{-1}$

Theorem 7.10

If $\theta : G \to H$ is a group homomorphism, then the set ker $\theta = \{x \in G : \theta(x) = e_H\}$ is a subgroup of G called the kernel of θ, and the set $Im\ \theta = \{\theta(x): x \in G\}$ is a subgroup of H called the image of θ.

Proof:

If $x,\ y \in ker\ \theta\ then\ \theta(x) = e_H\ and\ \theta(y) = e_H$.

Hence $\theta(xy) = \theta(x)\theta(y) = e_H$. So $x\ y \in$ ker θ. If $x \in$ ker θ, then $\theta(x) = e_H$, and so $\theta(x^{-1}) = (\theta(x))^{-1} = {e_H}^{-1} = e_H$.

So, ker θ is a subgroup of G. Next, let us prove that $Im\ \theta$ is a subgroup of H. Since $\theta(e_G) = e_H, e_H \in Im\theta$.

Now, if $a,\ b \in Im\ \theta$ then $a = \theta(x)$ and $b = \theta(y)$ for some $x, y \in G$. So, $ab = \theta(x)\theta(y) = \theta(xy) \in Im\ \theta$, Since $x, y \in G$. Also $a^{-1} = (\theta(x))^{-1} = \theta(x^{-1}) \in Im\ \theta$, since $x^{-1} \in G$. So, $Im\ \theta$ is a subgroup of H.

Theorem 7.11

The composition of two homomorphisms $\theta : G \to H, \varphi : H \to K$ is a homomorphism.

Proof:

Let $.,*,+$ be the group operations in G, H, K respectively. If $x, y \in G$ then $\varphi\theta(x\ .\ y) = \varphi\big(\theta(x\ .\ y)\big) = \varphi\big(\theta(x) * \theta(y)\big) = \varphi\big(\theta(x)\big) + \varphi(\theta(y))$ and so $\varphi\theta$ is a homomorphism. i.e. $\varphi\theta = \varphi\theta(x) + \varphi\theta(y)$

Example 7.12

In example 7.8, ker $\theta = \{1, -1\}$, $e_H = 1$, $and\ e_G = 1$

ξ_2

RINGS, SUBRINGS

ξ_1

RINGS

So far, we have been looking at a set on which a single binary operation is defined, in this chapter we will be considering a set on which two binary operations are defined simultaneously.

Definition 8.1

A non-empty set R is said to be a ring if in R there are defined two distinct binary operations, denoted by $'+'$ and $'.'$ respectively such that

(i) R is a commutative group under $'+'$ (addition)

(ii) R is a semigroup under $'.'$ (multiplication) and

(iii) The left and right distributive laws hold in R i.e. $\forall\ a, b, c \in R$, we have that $a\,.\,(b + c) = a\,.\,b + a\,.\,c$ and $(b + c).a = b\,.a + c\,.\,a$

We shall denote a ring by $(R,\ +,\ .)$

Remarks 8.1.1

(i) Recall that the concepts of commutative (abelian) groups and semigroups are discussed in chapter five.

(ii) Observe that a Ring has nine properties.

Definition 8.2

if $(R, +, .)$ is a ring such that $a . b = b . a$ holds for any elements $a, b \in R$, then $(R, +, .)$ is called a commutative ring.

Definition 8.3

If $(R, +, .)$ is a ring such that there is an identity element 1 in R such that $a . 1 = a = 1 . a$ for every element $a \in R$, then we say that $R, +, .)$ is a ring with unit (identity) element $'1'$.

The identity element of $(R, +)$ is denoted by 0.

Remark 8.2.1

If $(R, +, .)$ is a ring with unit element 1, then $1 \neq 0$.

Example 8.3

1. The set Z of all integers under the usual addition $' + '$ and multiplication $'.'$ of integer is a commutative ring with elements 1 i.e. $(Z, +, .)$ is a commutative ring with unit element I. The integer 0 is the additive identity element.
2. The set of even integers under $' + '$ and $'.'$ in $(Z, +, .)$ is a commutative ring but it has no unit element.
3. The set Q of all rational numbers under the usual addition and multiplication of real numbers is a

commutative Ring with identity (unit) element 1. (The rational number).

ξ_2

SUBRINGS

Definition 8.4

A subring of a ring $(R, +, .)$ is a subset S of R which is a ring under the induced binary operations $'+'$ and $'.'$ from the whole ring $(R, +, .)$. For example, example 8.3 (2) above is a subring of $(Z, +, .)$.

Example 8.5

The set of all 2 × 2 matrices with rational entries, is a non-commutative ring with unit element $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Example 8.6

The set Z_6 of integers modulo 6 is a ring under addition and multiplication modulo 6 (i.e. in Z_6, $'+'$ is defined by $\bar{\imath} + \bar{\jmath} = \bar{k}$ where $\bar{k}$ is the remainder of the integer $i + j$ on division by 6. For $\bar{\imath}, \bar{\jmath}, \bar{k} \in Z_6$

$= \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$. $\bar{\imath} . \bar{\jmath} = \bar{m}$ where $\bar{m}$ is the remainder of the integer $\bar{\imath} . \bar{\jmath}$ on division by 6 e.g. $\bar{2} . \bar{3} = \bar{0}$ $(Z, +, .)$ has a unit element as $\bar{1}$, and $\bar{0}$ is its additive identity element).

Example 8.7

The set Z_n, where $n \geq 2$ is an integer, is a ring under addition and multiplication defined as in example 8.6 above where $Z_n = \{\bar{0}, \bar{1}, \ldots, (\overline{n-1})\}$ with unit element $\bar{1}$ and its additive identity element is $\bar{0}$.

Definition 8.8

If $(R, +, .)$ is a commutative ring, a non-zero element of R is said to be a zero-divisor of $(R, +, .)$, if $\exists$ a non-zero element $b \in R$ such that $a \,.\, b = 0$ where 0 is the additive identity element of $(R, +)$ e.g. In $(Z_6, +, .)$, $\bar{3}$ is a zero divisor of $\bar{2}$ because $\bar{3} \neq \bar{0}$ and $\bar{2} \,.\, \bar{3} = \bar{0}$. In $(Z_4, +, .)$, $\bar{2}$ is a zero divisor of $\bar{2}$ since $\bar{2} \,.\, \bar{2} = \bar{0}$

Definition 8.9 (Integral Domain)

A commutative ring is called an integral domain if it has no zero-divisor e.g. The $(Z, +, .)$ is an integral domain but $(Z_6, +, .)$ is not an integral domain. $(Z_7, +, .)$ is an integral domain.

Remark 8.9.1

(i) In fact $(Z_p, +, .)$ is an integral domain if p is prime.

(ii) A ring R is called an INTEGRAL DOMAIN if whenever $a, b \in R$ and $a \,.\, b = 0$ then either $a = 0$ or $b = 0$. Examples are $Z, Q, R \; and \; C$.

Definition 8.10 (Division Ring)

A ring is said to be a division ring if its non-zero element form a group under multiplication i.e. $(R, +, .)$ is a division ring if $(R\{0\}, .)$ is a group where 0 is the additive identity element.

ξ_3

FIELDS

Definition 8.11

By a field $(F, +, .)$ we mean a commutative division ring, i.e. $(F\backslash\{0\}, .)$ is a commutative group where 0 is the additive element of the $(F, +, .)$

Remark 8.11.1

Detail about the definition of a field will be given in section three.

Preposition 8.12

Let $(R, +, .)$ be a ring. Then for every $a \in R$ we have $a.0 = 0 = 0.a$

Proof:

If $a \in R$ then (by the distributive laws)

$a.0 = a.(0 - 0) = a.\ 0 - a.0 = 0$ and

$0.\ a = (0 - 0).a = 0.a - 0.a = 0.$

This proves the proposition 8.12

Definition 8.13

A subfield is defined as a subset which is a field under the binary operation from the given field.

Definition 8.14

Let us consider a division ring that is not a field, let Q_t be the set.

$Q_t =$

$\{\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k : \alpha_0, \alpha_1, \alpha_2, \alpha_3 \; are \; all \; real \; number\}$. If $\alpha = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k, \; \beta = \beta_0 + \beta_1 i + \beta_2 j + \beta_3 k \in Q_t$ we say that $\alpha = \beta$ if, and only if, $\alpha_r = \beta_r$ for $r = 0, 1, 2, 3$ and define $' + '$ (addition) by $\alpha + \beta = (\alpha_0 + \beta_0) + (\alpha_1 + \beta_1)i +$

$(\alpha_2 + \beta_2)j + (\alpha_3 + \beta_3)k$ and $'.'$

(multiplication by)

$\alpha . \beta = (\alpha_0\beta_0 - \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3) + (\alpha_0\beta_1 + \alpha_1\beta_0 + \alpha_2\beta_3 - \alpha_3\beta_2)i + (\alpha_0\beta_2 + \alpha_2\beta_0 - \alpha_3\beta_1 - \alpha_1\beta_3)j + (\alpha_0\beta_3 + \alpha_3\beta_0 + \alpha_1\beta_2 - \alpha_2\beta_1)k$

i.e. we must multiply as if we are multiplying real numbers subject to the following conditions

$i^2 = -1, j^2 = -1, k^2 = -1, \; ijk = -1$ and

$i \; j = -j \; i = k, \qquad j \; k = -kj = i, ki = -ik = j$

Then $(Q_1, +, \; .)$ is a division ring with the zero element 0 as $0 + 0i + 0j + 0k$ and unit element 1 as $1 + 0i + 0j + 0k$, the additive inverse of $\alpha = \alpha_0 + \alpha_1 i + a_2 j + a_3 k \in Q_t$ is $\alpha = (-\alpha_0) + (-\alpha_1)i + (-\alpha_2)j + (-\alpha_3)k$ while multiplicative inverse $(\alpha)^{-1} \; is \; \frac{\alpha_0}{A} - \frac{\alpha_1 i}{A} - \frac{\alpha_2 j}{A} - \frac{\alpha_3 k}{A} \in Q_t$ for $\alpha \neq 0$, where

$A = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 \quad (A \neq 0, since\ \alpha \neq 0$

So, the non-zero elements of the ring $(Q_1, +, .)$ form a group under $'.'$. Hence $(Q_1, +, .)$ is a division ring. It is not a field, since $i\,j \neq j\,i$ for example, $i, j \in Q_t$ and $i \neq 0,\ j \neq 0$.

Definition 8.15

A finite division ring must be a field. The division ring $(Q_1, +, .)$ is called the real quaternions (of Hamilton).

Theorem 8.16

A finite integral domain must be a field.

Proof:

Let D be a finite integral domain in order to prove that D is a field. We must produce an element $1 \in D$ such that $a \,.1 = a = 1\,.a$ since it is commutative, and for every non-zero element a in D we should produce an element $b \in D$ such that $a\,.\,b = 1$ then the non-zero elements of D would form a commutative group with respect to $'.'$ and so D would be a field.

Since D has only a finite number of elements, say n, let them be the distinct points $x_1, x_2, \ldots\ldots, x_n$. If a is non-zero element of D, consider the element $x_1\,.\,a, x_2\,.\,a, \ldots\ldots, x_n\,.\,a$ they are all in D, since $'.'$ is closed being a binary operation, we claim that they are all distinct; for if $x_i\,.\,a = x_j\,.\,a, (i \neq j)$ then $(x_i - x_j)\,.\ a = 0$ and since $D$is an integral domain and $a \neq 0$ we

must have $x_i - x_j = 0$ and so $x_i = x_j,\ a$ contradiction. Thus $x_1 \ . \ a,\ x_2 \ . \ a, \ldots, x_n \ . \ a$ are n distinct elements in D, and so the map $x_i \xrightarrow{\varphi} x_i \ . a (1 \leq i \leq n$ is an injective function on a finite set D to itself, hence it must be surjective as well. So every element $y \in D$ can be written as $y = x_i \ . \ a$ for some $x_i \in D$, then $y = x_i \ . \ a$ for some $x_j \in D$ and so $y \ . \ x_{i0} = (x_i \ . a) . x_{i0} = x_i . (a \ . \ x_i) = x_i \ . \ a = y$. Thus x_{i0} is a unit element for D, and we write it as 1. Now $1 \in D$, so there is an element $b \in D$ such that $1 = b \ . a$. hence D is a field.

Corrollary 8.17

If P is a prime number, then ring Z_P of integers modulo P is a field.

Proof:

Since Z_P is finite we need only show that $(Z_P, +, \ .)$ is an integral domain. Since Z_P behaves like Z, we need only that $(Z_P, +, \ .)$ has no zero divisors if $\bar{a}, \bar{b} \ \in Z_P$ and $\bar{a} \ . \bar{b} = \bar{0}$ then p must divide the ordinary integral ab, and so being a prime must divide a and b. Hence

$\bar{a} = \bar{0} \ or \ \bar{b} = \bar{0}$. So, the ring $(Z_P, +, \ .)$ has no zero-divisors. Hence it is an integral domain. So being finite $(Z_P, +, \ .)$ is a field (by theorem 8.16)

Definite 8.18

A field having only a finite number of points is called a finite field.

ξ_4

RING HOMOMORPHISMS

Definition 8.19

A mapping Q from a ring $(R_1, +_1, \ o_1)$ onto $(R_2, +_2, \ o_2)$ is said to be a ring homomorphism if for any element $a, b \in R$, we have

(i) $\varphi(a +_1 \ b) = \varphi(a) \ +_2 \ \varphi(b)$ and

(ii) $\varphi(a \ o_1 \ b) = \varphi(a) \ o_2 \ \varphi(b)$

Remark 19.1

The operations belonging to R_1 are indicated by subscript 1, and R_2 by subscripts 2.

Theorem 8.20

If φ is a ring homomorphism of $(R_1, +_1, \ o_1)$, onto $(R_2, +_2, \ o_2)$ then,

(i) $\varphi(0_1) = 0_2$. $(i.e: 0_1 \rightarrow 0_2)$, and

(ii) $\varphi(-a) = -(\varphi(a))$ for every element $a \in R_1$

Definition 8.21

If φ is a ring homomorphism of R_1 into R_2, then the kernel of φ denoted by ker φ_1 is the set of all element $a \in R_1$ such that $\varphi(a) = 0_2$.

Theorem 8.22

If φ is a ring homomorphism of R_1 and R_2 then

(a) ker φ is a sub group of R_1 under addition .

(b) If $a \in$ ker φ and $r \in R$, then both ar and ra belong to ker φ.

Proof:

Since φ is in particular, a group homomorphism of R_1 into R_2 as additive groups, ker φ is a subgroup of R_1 under addition. To prove (b), suppose that $a \in$ ker φ and $r \in R_1$. Then $\varphi(a) = 0_2$ and so $\varphi(ar) = \varphi(a)\varphi(r) = 0_2\varphi(ar) = 0_2 \Longrightarrow ar \in$ ker φ. Similarly $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0_2 = 0_2$. Hence ar and ra belong to ker φ.

Example 8.23

Let R, R^1 be rings. Define $\varphi(a) = 0 \; \forall \; a \in R$. Then φ is a ring homomorphism, and ker $\varphi = R$. The map φ is called the zero homomorphism.

Example 8.24

Let R be a ring. If $R^1 = R$, define $\varphi(x) = x \; \forall \; x \in R$. then φ is a ring homomorphism of R into itself, and ker $\varphi = \{0\}$.

Example 8.25

Let $J(\sqrt{2})$ be the set of all real numbers of the form $m + n\sqrt{2}$, where m, n are integers $(i.eJ(\sqrt{2} = \{m + n\sqrt{2} : m, n \in Z\})$. Then $J(\sqrt{2})$ is a ring under the usual addition and

multiplication of real numbers with the zero element as $0 + 0\sqrt{2}$ and unit element $1 + 0\sqrt{2}$.

Define $\varphi: J(\sqrt{2}) \to J(\sqrt{2})$ by $\varphi(m + n\sqrt{2}) = m - n\sqrt{2}$. Then φ is a ring homomorphism of $J(\sqrt{2})$ onto $J(\sqrt{2})$ and ker $\varphi = \{0\}$.

Example 8.26

Let J be the ring of all integers, and J_n be the ring of integers modulo n $(i.e. J = Z \; and \; J_n = Z_n)$. Then φ is a ring homomorphism of J onto J_n, and ker φ consists of all multiples of n $(i.e.$ ker $\varphi = \{rn : r \in Z\})$.

Definition 8.27

Two rings R_1 and R_2 are said to be isomorphic if there is a ring homomorphism φ of R_1 into R_2 that is bijective.

$(i.e. \; \varphi : R_1 \to R_2 \; is \; 1-1 \; and \; onto)$, and we say that φ is a ring isomorphism of R_1 onto R_2.

Exercise

Let a, b, c be elements of a ring R.

(a) Prove that the following identities are valid

(i) $a(b - c) = ab - ac$

(ii) $(a - b)^2 = a^2 - ab - ba + b^2$

(b) Is $(a - b)(a + b) = a^2 - b^2$? Justify you answer.