محاضرات في جبر الزمر

مدرس المقرر : م.م. ضياء غازي صالح　　　اسم المقرر : جبر الزمر(١)
عدد الوحدات : ٣　　　رقم المقرر : ر٢٢٣
فترة الدراسة : ١٥ اسبوع / (٣ ساعات نظري + ساعة واحدة مناقشة) اسبوعياً

Abstract Group Theory

0.1 Binary Operators

Let A be a set. A *binary operator* on A is a function $* : A \times A \to A$

A binary operator is simply something that takes two elements of a set and gives back a third element of the same set.

Example 1

Let $\mathbb{R}$ be the set of real numbers. Then $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, given by $+(x , y) = x + y$, is a binary operator.

Also $\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, given by $\cdot\,(x , y) = x\,y$, is a binary operator.

In general, in the sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, addition and multiplication are binary operators.

Example 2

Let X be a set and let P(X) be the power set of X. Then union and intersection are binary operators on P(X); for example
$\cap :$ P(X) $\times$ P(X) $\to$ P(X) is defined by $\cap\,(A,B) = A \cap B$, where $A,B \in X$.

Definition 1 (permutation)

A permutation of a set X is a bijective function $\alpha : X \to X$. We call the set of all permutations of X, Sym(X).

Example 3

Let X be a set and let Sym(X) be the set of all permutations of X.
Then $\circ$ is a binary operator on Sym(X),
$\circ :$ Sym(X) $\times$ Sym(X) $\to$ Sym(X)　is defined by　$\circ\,(\alpha,\beta) = \alpha \circ \beta$.

For example , let $X= \{ 1,2,3\}$, the set Sym(X)= S_3 of permutation operations that take 123 into 123, 132, 213, 312, 231, 321. The elements of the set are

$$e = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} \quad , \quad \alpha = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = (123)\,, \quad \beta = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = (132)\,,$$

$$\gamma = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = (23) \;,\; \delta = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = (13) \quad , \quad \sigma = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = (12)\;.$$

The operation $\alpha \circ \beta$ means (for example) ;

$$\alpha \circ \beta = (123) \circ (132) = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} \circ \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = e$$

$$\alpha \circ \gamma = (123) \circ (23) = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} \circ \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = (13) = \delta$$

$$\gamma \circ \alpha = (23) \circ (123) = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} \circ \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = (12) = \sigma \;.$$

This operation on Sym(X) is associative, because composition of functions is always associative. It is also invertible. The identity element for this operation is the identity function . The inverse of a permutation exists because bijective functions are always invertible. However, composition of permutations is not commutative.

Let A be a set and let $*: A \times A \to A$ be a binary operator. As in the above examples, it is customary to write $a * b$ instead of $*\,(a, b)$, where $a, b \in A$. However, we keep in mind that $*$ is a function and that $a * b \in A$.

Let $*: A \times A \to A$ be a binary operator on a set A and let $B \subseteq A$. we say that B is ***closed*** under the operation of $*$ if for every $a, b \in B$, we have $a * b \in B$.

Example 4

Let E be the set of even integers. Then E is closed under the operations of addition and multiplication of integers. Indeed, the sum of even integers is even, and the product of even integers is even.

Let O be the set of odd integers. Then O is closed under multiplication. However, O is not closed under addition, because the sum of two odd integers is even.

Example 5

Let $B = \{a + b\sqrt{2} \in \mathbb{R}\, ;\, a, b \in \mathbb{Q}\}$. Then B is closed under addition and multiplication of real numbers. For example,

If $a + b\sqrt{2}$ and $c + d\sqrt{2}$ are two element of B, then

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

and

$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = (ac + 2bd) + (bc + ad)\sqrt{2} \in B$$

Note that these results are in B because $\mathbb{Q}$ itself is closed under addition and multiplication. Therefore $(ac + 2bd), (bc + ad) \in \mathbb{Q}$.

Example 6

Let X be a set and let $Y \subseteq X$. Then $P(Y) \subseteq P(X)$, and the subset $P(Y)$ is closed under the operations of intersection and union of subset of X.

Example 7

The real numbers have two binary operations, addition and multiplication. Each is commutative and associative. The additive identity is 0, and the multiplicative identity is 1. Every element a has an additive inverse $-a$, and if $a \neq 0$,it has a multiplicative inverse $a^{-1} = {}^{1}/_{a}$.

Example 8

Let X be a set and consider intersection and union of subsets of X. These are operations on $P(X)$ which are commutative and associative. Intersection has an identity element, which is the entire set X, since for $A \subseteq X$, we have $A \cap X = A$. Union also has an identity element, which is $\emptyset$ .Neither of these operations supports inverses.

However, the operation of symmetric difference on P(X), defined by $A \,\Delta\, B = (A \cup B) - (A \cap B)$, is commutative, associative, and invertable .The identity element is $\emptyset$, and the inverse of $A \in$ P(X) is itself.

Example 9

The standard *dot product* on $\mathbb{R}^n$ is defined by

$$\vec{v} \cdot \vec{w} = v_1 \cdot w_1 + v_2 \cdot w_2 + \cdots + v_n \cdot w_n$$

where $\vec{v} = (v_1, v_2, \dots, v_n)$ and $\vec{w} = (w_1, w_2, \dots, w_n)$. Note that for $n > 1$, this is ***not*** a binary operator ! why ?

Example 10

An $m{\times}n$ matrix with entries in $\mathbb{R}$ is an array of elements of $\mathbb{R}$ with m rows and n columns. The entries of a matrix are often labeled a_{ij} , where this is the entry in the i^{th} row and j^{th} column. We may write such a matrix with the notation (a_{ij}).

An $m{\times}n$ matrix $A = (a_{ij})$ may be added to an $m{\times}n$ matrix $B = (b_{ij})$ to give an $m{\times}n$ matrix $A{+}B = D = (d_{ij})$ by the formula $d_{ij} = a_{ij} + b_{ij}$.

An $m{\times}n$ matrix $A = (a_{ij})$ may be multiplied by an $n{\times}p$ matrix $B = (b_{jk})$ to give an $m{\times}p$ matrix $AB = C = (c_{ik})$ by the formula

$$c_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk}$$

thus the ik^{th} entry of C is the dot product of the i^{th} row of A with the k^{th} column of B.

Let $M_n(\mathbb{R})$ be the set of all $n{\times}n$ matrices over $\mathbb{R}$.

Then addition of matrices is a binary operation on $M_n(\mathbb{R})$ which is commutative, associative, and invertible.

Also, multiplication of matrices is a binary operation on $M_n(\mathbb{R})$ which is associative and has an identity. The identity is simply the matrix given by

$$a_{ij} = \begin{cases} 1 & if\ i = j \\ 0 & \text{otherwise} \end{cases} \qquad e = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix}.$$

However, this operation is not commutative, and there are many elements which do not have inverses.

Exercise 1

In each case, we define a binary operation $*$ on $\mathbb{R}$. Determine if $*$ is commutative and/or associative, find an identity if it exists, and find any invertible elements.

(a) $x * y = xy + 1$,

(b) $x * y = \frac{1}{2} xy$.

Exercise 2

Consider the plane $\mathbb{R}^2$. Define a binary operation $*$ on $\mathbb{R}^2$ by

$(x_1, y_1) * (x_2, y_2) = \left(\frac{x_1+x_2}{2}, \frac{y_1+y_2}{2}\right)$

Thus the "product" of two points under this operation is the point which is midway between them. Determine if $*$ is commutative and/or associative, find an identity if it exists, and find any invertible elements.

Exercise 3

Let I be the collection of all open intervals of real numbers. We consider the empty set to be an open interval.

(a) Show that I is closed under the operation of $\cap$ on $P(\mathbb{R})$,

(b) Show that I is not closed under the operation of $\cup$ on $P(\mathbb{R})$.

1.1 Groups

A non-empty set G, is said to form a group if in G there is defined a binary operation, called the product and denoted by '$*$' such that

i. Closure : if $a, b \in G$ implies $a * b \in G$.

ii. Associativity : $a, b, c \in G$ implies $(a * b) * c = a * (b * c)$.

iii. Unit element : There exists an element $e \in G$ such that $a * e = e * a = a$ for all $a \in G$.

iv. Inverse : For every $a \in G$ there exists an element $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.

A group, which contains only a finite number of elements, is called a finite group, otherwise it is termed as an infinite group. By the order of a finite group we mean the number of elements in the group.

The following properties follow from the above definition:

Pro.1. Left cancellation : If $ax = ay$ then $x = y$ for all a in the group.

Proof: $ax = ay$

$\Rightarrow \quad a^{-1}(ax) = a^{-1}(ay)$

$\Rightarrow \quad (a^{-1}a)x = (a^{-1}a)y$

$\Rightarrow \quad ex = ey$

$\Rightarrow \quad x = y$.

Pro.2. Unit element on the right : $ae = a = ea$.

Proof:

$a^{-1}(ae) = (a^{-1}a)e = ee = e = a^{-1}a$

and using the left cancellation law we have $ae = a$.

Pro.3. Inverse element on the right: $aa^{-1} = e = a^{-1}a$.

Proof:

$a^{-1}(aa^{-1}) = (a^{-1}a)\, a^{-1} = ea^{-1} = a^{-1} = a^{-1}e$.

Using the left cancellation law, $aa^{-1} = e$.

Pro.4. Right cancellation : If $xa = ya$ then $x = y$ for all a in the group.
Proof:

$$xa = ya \Rightarrow (xa)\,a^{-1} = (ya)\,a^{-1} \Rightarrow x(aa^{-1}) = y(aa^{-1})$$
$$\Rightarrow xe = ye \Rightarrow x = y\ .$$

We note the importance of associativity in the above proofs.
The following identity is often useful :

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

which follows from $(ab)^{-1}\,(ab) = e \Rightarrow (ab)^{-1}a = b^{-1}$
$\Rightarrow (ab)^{-1} = b^{-1}a^{-1}$.

1.2 Abelian Group(commutative group)

Let G be a group. If $a * b = b * a$ for all $a, b \in G$, we call G an abelian group or a commutative group.

1.3 Subgroup

A subgroup is a set of elements within a group which forms a group by itself. Evidently, the unit element forms a subgroup by itself.

Example 11

Integers under addition. The unit element $e = 0$ and the inverse of an element a is $a^{-1} = -a$. This group is abelian and infinite.

Example 12

Let $\mathbb{Q}$ be the set of rationals. $\mathbb{Q}\setminus\{0\}$ is a group under multiplication. This is an infinite group.

Example 13

A set of all $n\times m$ matrices $M_{n\times m}$ under matrix addition . The unit element is the zero matrix and the inverse of U is $-U$.

This group is abelian and infinite.

Example 14

A set of all $n\times n$ invertable matrices $M_{n\times n}$ under matrix multiplication. The unit element is the unit matrix and the inverse of U is U^{-1}. This group is not abelian and infinite.

Example 15

The set S_3 of permutation operations . The elements of the group are ;

$$e = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \quad (123) = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \quad (132) = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},$$
$$(23) = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \quad (13) = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}, \quad (12) = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}.$$

The operation $\circ$ means (for example) ;

$$(123)\circ(132) = e$$

The group $(S_3, \circ)$ is not abelian and finite. Since . . .

∘	e	(123)	(132)	(23)	(13)	(12)
e	e	(123)	(132)	(23)	(13)	(12)
(123)	(123)	(132)	e	(13)	(12)	(23)
(132)	(132)	e	(123)	(12)	(23)	(13)
(23)	(23)	(12)	(13)	e	(132)	(123)
(13)	(13)	(23)	(12)	(123)	e	(132)
(12)	(12)	(13)	(23)	(132)	(123)	e

Example 16

$\{e\}$ and G are always subgroups of the group G, called the trivial subgroups.

1.4 Center group

Let $(G, *)$ be a group, S be a subset of G, we define the following set ;

Cent.$G = \{ x \in G ;\ x * a = a * x, \forall a \in G \}$

which is called center group .

Remark 1

G abelian group $\Leftrightarrow$ Cent.$G = G$.

Example 17

1- Cent. $S_3 = \{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \}$.

2- Cent. $\mathbb{Z} = \mathbb{Z}$.

Remark 2

Let H_1, H_2 are two subgroups of the group G, then

1- $H_1 \cap H_2$ is a subgroup of G ,

2- $H_1 \cup H_2$ is not necessary a subgroup of G .

In general case , let $H_1, H_2, H_3, \ldots$ are a subgroups of the group G then $\cap_i H_i$ is a subgroup of G .

1.5 Cyclic Groups

Let G be a group , S be a subset of G , we define the following set ;

$\langle S \rangle = \cap\{ H ; H$ is a subgroup of G such that $S \subseteq H \}$

$\langle S \rangle$ is smallest subgroup of G contains S . Which is called the subgroup generated by S . (if S is subgroup then $S = \langle S \rangle$)

If S is finite set , the subgroup $\langle S \rangle$ is finitely generated .

If $S = \{a\}$, then we say that the subgroup $\langle S \rangle = \langle \{a\} \rangle = \langle a \rangle$ is a cyclic group generated by the element a .

A group of n elements is said to be cyclic if it can be generated from one element . The elements of the group must be $a, a^2, a^3, \ldots, a^n = e$. n is called the order of the cyclic group.

A cyclic group is evidently abelian but an abelian group is not necessarily cyclic.

Example 18

Integers under addition , ($\mathbb{Z}$, +) , is a cyclic group generated by 1 , (i.e. $\mathbb{Z} = \langle 1 \rangle$) .
Let $2\mathbb{Z}$ be the set of even integers , ($2\mathbb{Z}$, +) , is a cyclic group generated by 2 .
In general case , ($n\mathbb{Z}$, +) is a cyclic group generated by n , (i. e. $n\mathbb{Z} = \langle n \rangle$) .

Example 19

In general $\mathbb{Q}$ and $\mathbb{R}$ with addition and multiplication operators, ($\mathbb{Q}$, +) , ($\mathbb{Q}\backslash\{0\}$, .) , ($\mathbb{R}$, +) and ($\mathbb{R}\backslash\{0\}$, .) all are not cyclic groups .

Example 20

Example of cyclic group are the subgroup of the permutation group in the **example 15**.The subgroup $(e\ ,(123)\ ,(132))$ is the same as $((123),(123)^2 = (132),(123)^3 = e)$.

Example 21

$\mathbb{Z}_p = \{0,\ 1,\ 2,\ \dots\ ,\ p-1\}$, p a prime , be the set of integers modulo p . $\mathbb{Z}_p\backslash\{0\}$ is a group under multiplication modulo p, ($\mathbb{Z}_p\backslash\{0\},\times_p$) , this is a finite cyclic group of order p-1.

Exercise 4

1- ($G, *$) is an abelian group $\Leftrightarrow$ $(a * b)^2 = a^2 * b^2 \quad \forall\, a\, ,b \in G$.
2- If ($G, *$) is an group such that $a^2 = e$ $\forall a \in G$ (*e=unit element*) $\Longrightarrow$ ($G, *$) is an abelian group . And the inversion is not true .
3- If ($G, *$) is an group such that $a^2 = e$ $\forall a \in G$ (*e=unit element*) $\Longrightarrow$ Cent.$G = G$.
4- Prove that ; ($\mathbb{Q}\backslash\{0\}$, .) is not cyclic group .
5- Let ($G, *$) and ($\bar{G}, \bar{*}$) are two commutative groups . Define a binary operation $\odot$ on the Cartesian product $G \times \bar{G} = \{\, (a,b); a \in G\, ,b \in \bar{G}\, \}$ as follows ; $(a_1\, ,b_1)\odot(a_2\, ,b_2) = (a_1 * a_2\, ,b_1 \bar{*}\, b_2) \quad \forall\, (a_1\, ,b_1)\, ,(a_2\, ,b_2) \in G \times \bar{G}$
Prove that ; ($G \times \bar{G}$,$\odot$) is a commutative group .

1.6 Order of an Element

Let $a \neq e$ be an element of a group. Form the products $a^2, a^3, \dots$
a^2 must be either e or a different element from a because if $a^2 = a \Longrightarrow a = e$.
If $a^2 \neq e$ we continue forming a^3. By a similar argument, , a^3 must be either e or a different element from a and , a^2. If $a, a^2, a^3, \dots, a^n$ are distinct from each other and , $a^n = e$ then n is called the order of element a . These elements form a cyclic group.

The order of an element $a \in G$, $o(a)$, is defined to be the minimal positive integer n such that $a^n = e$. If no such n exists, we say a has infinite order .

We calls a subgroup H **cyclic** if there is an element $h \in H$ such that $H = \{h^n\ ;\ n \in \mathbb{Z}\}$.

Note that $H = \{h^n\ ; n \in \mathbb{Z}\}$ is always a cyclic subgroup . We denote it by $< h >$.

Thus every group must have at least one cyclic subgroup. In the **example 15** above, (123) and (132) are of order 3 and (12), (13) , and (23) are of order 2.

Example 22

Let $G = \langle g\, ;\, g^8 = 1 \rangle$ be a cyclic group of order 8 .

$H = \langle g^2 \rangle = \{g^2, g^4, g^6, 1\}$ is subgroup of G .

1.7 Normal Subgroups

Let $(G, *)$ be a group. A non-empty subset H of G is said to be a normal subgroup of G , if $H*a = a*H \quad \forall a \in G$ or equivalently

$H = \{a^{-1} * h * a\, ;\; \forall a \in G \;\&\; \forall\, h \in H\}$.

If G is an abelian group or a cyclic group then all of its subgroups are normal in G.

Example 23

The subgroup $H = \{\, e\, , (123)\, , (132)\, \}$ given in **example 15** is a normal subgroup of S_3 .

$S_3 = \{\, e^{-1} = e\, ,\; (123)^{-1} = (132)\, ,\; (132)^{-1} = (123)\, ,\; (12)^{-1} = (12)\, ,\; (13)^{-1} = (13)\, ,\; (23)^{-1} = (23)\, \}$

We must prove that $H \circ a = a \circ H \quad \forall a \in S_3$, it is easy to show the following ;

$He = \{e \circ e\, , (123) \circ e\, , (132) \circ e\} = \{e\, , (123)\, , (132)\}$

$= H = \{e \circ e\, , e \circ (123)\, , e \circ (132)\} = eH$

$H(123) = \{e \circ (123)\, , (123) \circ (123)\, , (132) \circ (123)\} = \{\, (123), (132)\, , e\, \}$

$= H = \{(123) \circ e\, , (123) \circ (123)\, , (123) \circ (132)\} = (123)H$

$H(132) = \{e \circ (132)\, , (123) \circ (132)\, , (132) \circ (132)\} = \{\, (132), e\, , (123)\, \}$

$= H = \{(132) \circ e\, , (132) \circ (123)\, , (132) \circ (132)\} = (132)H$

$H(12) = \{e \circ (12)\, , (123) \circ (12)\, , (132) \circ (12)\} = \{\, (12), (23)\, , (13)\, \}$

$= \{\, (12)\, , (13)\, , (23)\, \} = \{(12) \circ e\, , (12) \circ (123)\, , (12) \circ (132)\} = (12)H$

$H(23) = \{e \circ (23)\, , (123) \circ (23)\, , (132) \circ (23)\} = \{\, (23)\, , (13)\, , (12)\, \}$

$= \{\, (23), (12)\, , (13)\} = \{(23) \circ e\, , (23) \circ (123)\, , (23) \circ (132)\} = (23)H$

$H(13) = \{e \circ (13)\, , (123) \circ (13)\, , (132) \circ (13)\} = \{\, (13)\, , (12)\, , (23)\, \}$

$= \{(13), (23)\, , (12)\} = \{(13) \circ e\, , (13) \circ (123)\, , (13) \circ (132)\} = (13)H$

Notation

Let S_n be the symmetric group of degree n. Then for $n \geq 5$, each S_n has only one normal subgroup, A_n which is of order $\frac{n!}{2}$ called the alternating group.

Exercise 5

Prove that ; there is only one normal subgroup of the group $(S_3, \circ)$.

1.8 Simple Group

If G is a group, which has no normal subgroups then we say G is simple group.

Example 24

Let $\mathbb{Z}_{11} \backslash \{0\} = \{1, 2, \ldots, 10\}$ be the group under multiplication modulo 11. The group $\mathbb{Z}_{11} \backslash \{0\}$ has no subgroups or normal subgroups.

1.9 Congruent

Let G be a group , H a subgroup of G ; for $a , b \in G$ we say a is congruent to b mod H , and written as $a \equiv b \bmod H$ if $ab^{-1} \in H$.

Lemma 1

The relation $a \equiv b \bmod H$ is an equivalence relation .

Proof

We must verify the following three conditions ; for all $a, b, c \in G$,

1- $a \equiv a \bmod H$,
2- $a \equiv b \bmod H \implies b \equiv a \bmod H$,
3- $a \equiv b \bmod H$, $b \equiv c \bmod H \implies a \equiv c \bmod H$.

1- Since H is a subgroup of G , $e \in G$, and since $aa^{-1}=e$, $aa^{-1} \in G \implies a \equiv a \bmod H$.

2- Suppose $a \equiv b \bmod H$ i.e. $ab^{-1} \in H$, but H is a subgroup of G, that is $(ab^{-1})^{-1} \in H \implies (ab^{-1})^{-1} = (b^{-1})^{-1}a^{-1} = ba^{-1}$ and hence $ba^{-1} \in G$ so $b \equiv a \bmod H$.

3- Suppose $a \equiv b \bmod H$, $b \equiv c \bmod H \implies ab^{-1} \in H, bc^{-1} \in H$ but H is a subgroup of G, that is $(ab^{-1})(bc^{-1}) \in H$, now

$ac^{-1}= a(e)c^{-1}= a(b^{-1}b)c^{-1} = (ab^{-1})(bc^{-1}) \implies ac^{-1} \in H$ that is $a \equiv c \bmod H$.

1.10 coset

Let $(H, *)$ is a subgroup of the group $(G, *)$ and let $a \in G$, the set $H{*}a=\{h{*}a \,;\, h \in H\}$ is called a right coset of H in G .

In a similar fashion , we can define the left coset $a{*}H$ of H .

Lemma 2

For all $a \in G$, $Ha=\{ x \in G \,;\, a \equiv x \bmod H \}$.

Proof

Let $[a] = \{ x \in G \,;\, a \equiv x \bmod H \}$. we must prove $Ha = [a]$.

First , let $h \in H \implies a(ha)^{-1}= a(a^{-1}h^{-1}) = h^{-1} \in H$ since H is subgroup of G . By definition of congruence mod $H \implies a \equiv ha \bmod H$, that is $ha \in [a]$ for every $h \in H$, and so $Ha \subset [a]$.

second , let $x \in [a]$. Thus, by definition of mod $H \implies ax^{-1} \in H \implies (ax^{-1})^{-1}= xa^{-1} \in H$. That is $xa^{-1}= h$ for some $h \in H$,

$\implies x = (xa^{-1})a= ha \in Ha$, and so $[a] \subset Ha$. Therefore $Ha = [a]$.

Theorem 1

If $(H, *)$ is a subgroup of the group $(G, *)$, then $a*H = H \iff a \in H$.

proof

$(\Longrightarrow)$ we know that $e \in H \Longrightarrow a = a*e \in a*H = H$.

$(\Longleftarrow)$ Let $a \in H \Longrightarrow a*H \subseteq H$ (since H is a subgroup) . Any element $h \in H$ may be written as $h = a * (a^{-1} * h)$. But $a^{-1} * h \in H$ (since a , $h \in H$ and H is a subgroup) $\Longrightarrow h \in a*H$, and therefore $H \subseteq a*H$.

Theorem 2

If $(H, *)$ is a subgroup of the group $(G, *)$, then $a*H = b*H \iff a^{-1} * b \in H$.

proof

$(\Longrightarrow)$ Assume that $a*H = b*H$. Then , if $a* h_1 \in a*H = b*H$ so there exist an $h_2 \in H$ such that $a* h_1 = b * h_2$.

$\Longrightarrow a^{-1} *(a* h_1) * {h_2}^{-1} = a^{-1} * (b * h_2) * {h_2}^{-1} \Longrightarrow h_1 * {h_2}^{-1} = a^{-1} * b$

but $h_1 * {h_2}^{-1} \in H$ (since $(H, *)$ is a subgroup) $\Longrightarrow a^{-1} * b \in H$.

$(\Longleftarrow)$ if $a^{-1} * b \in H$, then by **Theorem 1** we have $(a^{-1} * b)*H = H$,

$\Longrightarrow \forall\, h \in H$, $h = (a^{-1} * b)* h_1$, for some $h_1 \in H \Longrightarrow a* h = b * h_1$.

Thus each product $a* h$ in the coset $a*H$ is equal to an element of the form $b * h_1$, and consequently lies in the coset $b*H$. $\Longrightarrow a*H = b*H$.

Remark

If $(H, *)$ is a subgroup of the group $(G, *)$, then the following statement are equivalent ;

1- $(H, *)$ is a normal subgroup of $(G, *)$,

2- $a*H = H* a$, $\forall\, a \in G$,

3- $a*H* a^{-1} \subseteq H$, $\forall\, a \in G$,

4- $a*h* a^{-1} \in H$, $\forall\, a \in G$, $\forall\, h \in H$.

Theorem 3

If $(H, *)$ is a subgroup of the group $(G, *)$, then $\forall\, a , b \in G$ either $a*H \cap b*H = \emptyset$ or $a*H = b*H$.

Example 25

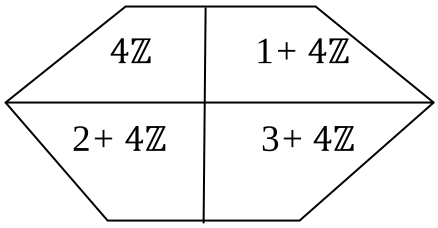
$4\mathbb{Z} = \langle 4 \rangle$ is a subgroup of the group $(\mathbb{Z} , +)$, then from **Theorem 1** we have

$m+ 4\mathbb{Z} = 4\mathbb{Z}$ if $m \in 4\mathbb{Z}$ (*i.e.* $\cdots = -8 + 4\mathbb{Z} = -4 + 4\mathbb{Z} = 4\mathbb{Z} = 0 + 4\mathbb{Z} = 4 + 4\mathbb{Z} = 8 + 4\mathbb{Z} = \cdots$)

$1+ 4\mathbb{Z} = \{\cdots, -7, -3,1,5,9, \cdots\} = -7 + 4\mathbb{Z} = -3 + 4\mathbb{Z} = 5 + 4\mathbb{Z} = 9 + 4\mathbb{Z} = \cdots$

$2+ 4\mathbb{Z} = \{\cdots, -6, -2,2,6,10, \cdots\} = -6 + 4\mathbb{Z} = -2 + 4\mathbb{Z} = 6 + 4\mathbb{Z} = 10 + 4\mathbb{Z} = \cdots$

$3+ 4\mathbb{Z} = \{\cdots, -5, -1,3,7,11, \cdots\} = -5 + 4\mathbb{Z} = -1 + 4\mathbb{Z} = 7 + 4\mathbb{Z} = 11 + 4\mathbb{Z} = \cdots$

$\mathbb{Z}$ 

$\mathbb{Z} = 4\mathbb{Z} \cup 1+4\mathbb{Z} \cup 2+4\mathbb{Z} \cup 3+4\mathbb{Z}$.

Theorem 4

If $(H, *)$ is a subgroup of the group $(G, *)$, the left (right) coset of H in G form a partition of the set G .

Example 26

Let $\mathbb{Z}_{12} = \{0,1, 2, \dots, 10,11\}$ be the group under addition modulo 12. $(\{0,4,8\},+_{12})$ is a subgroup of the group $(\mathbb{Z}_{12},+_{12})$, the left coset of $H = \{0,4,8\}$ in $\mathbb{Z}_{12}$ are

$0 +_{12} H = \{0,4,8\} = 4 +_{12} H = 8 +_{12} H$,
$1 +_{12} H = \{1,5,9\} = 5 +_{12} H = 9 +_{12} H$,
$2 +_{12} H = \{2,6,10\} = 6 +_{12} H = 10 +_{12} H$,
$3 +_{12} H = \{3,7,11\} = 7 +_{12} H = 11 +_{12} H$.

It is clear that $\mathbb{Z}_{12} = \{0,4,8\} \cup \{1,5,9\} \cup \{2,6,10\} \cup \{3,7,11\}$.

Remark

If $(G, *)$ be a finite group , and let $o(G)$=order of $G = n$. $(H, *)$ is a subgroup of the group $(G, *)$ of order k , i.e. $o(H) = k$.
We can then decompose the set G into a union of a finite number of left cosets of H ;

$$G = (a_1 * H) \cup (a_2 * H) \cup \dots \cup (a_r * H) \text{ , for } a_i \in G$$

1.11 index

If H is a subgroup of G , the index of H in G is the number of distinct left cosets of H in G . We shall denote it by $i_G(H)$.

In case G is a finite group , and $o(G) = n$. H is a subgroup of G , and $o(H) = k$. then $n = k \times i_G(H)$.

Theorem 5 (Lagrange)

The order and index of any subgroup of a finite group divides the order of the group .

Corollary

If $(G, *)$ be a group of order n ,then the order of any element $a \in G$ is a factor of n ; in addition , $a^n = e$.

Proof

Let the element a have order k . By definition , the cyclic subgroup $((a), *)$ generated by a must also be of order k . According to the conclusion of Lagrange's Theorem , k is a divisor of n ; that is $n=rk$ for some $r \in \mathbb{Z}_+$. Hence ,
$a^n = a^{rk} = (a^k)^r = e^r = e$.

Theorem 6

If $(G, *)$ be a finite group of composite order , then $(G, *)$ has nontrivial subgroup .

Corollary

Every group ($G, *$) of prime order is cyclic .

Theorem 7 (Revisited)

Any noncommutative group has at least six elements .

1.12 quotient group (factor group)

If $(H, *)$ is a normal subgroup of ($G, *$) , then we shall denote the collection of distinct cosets of H in G by $G/H = \{a * H \, ; \, a \in G\}$.

A rule of composition $\otimes$ may be defined on G/H by the formula

$$(a * H)\otimes(b * H) = (a * b) * H$$

Theorem 8

If $(H, *)$ is a normal subgroup of ($G, *$) , then ($G/H, \otimes$) forms a group ,

known as the ***quotient group*** (***factor group***) of G by H .

Proof

Let $(a * H), (b * H) \in G/H \Longrightarrow (a * H)\otimes(b * H) = (a * b) * H \in G/H$

Let $(a * H), (b * H), (c * H) \in G/H \Longrightarrow$

$$\begin{aligned}[(a * H)\otimes(b * H)]\otimes(c * H) &= [(a * b) * H]\otimes(c * H) \\ &= \big((a * b) * c\big) * H = (a * (b * c)) * H \\ &= (a * H)\otimes((b * c) * H) \\ &= (a * H)\otimes[(b * H)\otimes(c * H)]\end{aligned}$$

The coset $H = e * H$ is the identity element for the operation $\otimes$, since

$(a * H)\otimes(e * H) = (a * e) * H = a * H = (e * a) * H = (e * H)\otimes(a * H)$

Let $(a * H) \in G/H \Longrightarrow (a^{-1} * H) \in G/H$, since $a \in G$ (G a group)

$(a * H)\otimes(a^{-1} * H) = (a * a^{-1}) * H = (e * H) = H$

And hence ($G/H, \otimes$) is a group .

Example 27

Let $(n\mathbb{Z}, +)$ be a normal subgroup of an integers group $(\mathbb{Z}, +)$,

Then ($\mathbb{Z}/n\mathbb{Z}, \otimes$) is a group ,

where $\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$

$= \{ [0],[1],[2], . . . ,[n\text{-}1] \}$

and $\otimes = +_n$.

And hence ($\mathbb{Z}/n\mathbb{Z}, \otimes$) = $(\mathbb{Z}_n, +_n)$.

Exercise 6

Prove that ; $\left({S_3}/{\langle(123)\rangle} , \circ \right)$ is a group .

1.13 Commutator subgroup (derived subgroup)

Given a group $(G, *)$ and element $a , b \in G$, the commutator of a and b is defined to be the product $a * b * a^{-1} * b^{-1}$.

The symbol $[a,b] = a * b * a^{-1} * b^{-1}$. *i.e.* $a * b = [a,b] * b * a$

The elements a and b commute *if and only if* $[a,b] = e$.

Now , the inverse of a commutator is again commutator ; $[a, b]^{-1} = [b, a]$.

The set $[G,G]$ is defined by , $[G,G]=\{ \prod [a_i, b_i] \ ; a_i, b_i \in G \}$

The system $([G,G] , *)$ forms a group .

Theorem 9

The group $([G,G] , *)$ is a normal subgroup of $(G, *)$.

Remark

The quotient group $\left({G}/{[G,G]} , \otimes \right)$ is called the commutator quotient group .

Theorem 10

Let $(H, *)$ is a normal subgroup of $(G, *)$, then the quotient group $\left({G}/{H} , \otimes \right)$ is commutative *if and only if* $[G,G] \subseteq H$.

Corollary

For any group $(G, *)$ the commutator quotient group $\left({G}/{[G,G]} , \otimes \right)$ is commutative .

1.14 Homomorphisms

Let $(G, *)$ and $(G', *')$ be two groups and f a function from G into G', $f : G \to G'$. Then f is said to be a homomorphism from $(G, *)$ into $(G', *')$ *if and only if* $f(a * b) = f(a) *' f(b)$, $\forall \, a, b \in G$.

$$\begin{tikzcd}
a , b \arrow[r, "*"] \arrow[d, "f"'] & a * b \in G \arrow[d, "f"] \\
f(a) , f(b) \arrow[r, "*'"] & f(a * b) = f(a) *' f(b) \in G'
\end{tikzcd}$$

Remark

If $f : G \to G'$ is a homomorphism , then we say that

1- f is an ***epimorphism*** if f is surjective (onto) .

2- f is a ***monomorphism*** if f is injective (one-to-one) .

Example 28

For any group $(G, *)$, define the function $f: G \to G$ by taking $f(x)=I(x)=x$, $\forall \, x \in G$. It is easy to show that f is a homomorphism .

Example 29

Let $(G, *)$ and $(G', *')$ be two groups , define the function $f: G \to G$ by *f(x)=* e' $\forall\, x \in G$. It is easy to show that f is a homomorphism.

Example 30

Let $(\mathbb{R}, +)$ and $(\mathbb{R} \setminus \{0\}, .)$ be two groups , define the function $f: \mathbb{R} \to \mathbb{R} \setminus \{0\}$ by ; $f(x) = e^x = exp.(x) \quad \forall\, x \in \mathbb{R}$.

It is easy to show that f is a homomorphism ,since

$f(x + y) = e^{x+y} = e^x . e^y = f(x). f(y) \qquad \forall\, x, y \in \mathbb{R}$

Example 31

Let $(\mathbb{Z}, +)$ be the group of integers and $(\mathbb{Z}_n, +_n)$ be the group of integers modulo n . Define $f: \mathbb{Z} \to \mathbb{Z}_n$ by $f(x) = [x]$,

It is easy to show that f is a homomorphism ,since

$f(x + y) = [x + y] = [x] +_n [y] = f(x) +_n f(y)$

Remark

For any group $(G, *)$, define the set of all homomorphisms from G into itself ; $Hom(G) = \{ f: G \to G \text{ , } f \text{ is homomorphism} \}$.

Theorem 11

The pair $(Hom(G), \circ)$ forms a semigroup with identity ,
(where $\circ$ denotes functional composition) .

Proof

1) Let $f, g \in Hom(G)$, $\forall\, a, b \in G$

$$(g \circ f)(a * b) = g\big(f(a * b)\big) = g\big(f(a) * f(b)\big) = g\big(f(a)\big) * g\big(f(b)\big)$$
$$= (g \circ f)(a) * (g \circ f)(b)$$

$\Longrightarrow g \circ f \in Hom(G)$

2) By ***Example 28*** $I(x) = x$, $\forall\, x \in G \Longrightarrow I \in Hom(G)$

3) It is easy to show that , if $f, g, h \in Hom(G)$, then
$(g \circ f) \circ h = g \circ (f \circ h) \in Hom(G)$

Remark

For any group $(G, *)$, define the set of all one-to-one homomorphisms from G onto itself ; $A(G) = \{ f: G \to G \text{ , } f \text{ is epimorphism \& monomorphism} \}$.

Theorem 12

The system $(A(G), \circ)$ is a subgroup of the symmetric group $(sym(G), \circ)$ (where $\circ$ denotes functional composition) .

Hint : let $f \in A(G)$ we must prove $f^{-1} \in A(G)$

If $\bar{a}, \bar{b} \in G \Longrightarrow \exists\, a, b \in G$ such that $\bar{a} = f(a)$ and $\bar{b} = f(b)$,since $f \in A(G)$

Therefore $f^{-1}(\bar{a} * \bar{b}) = f^{-1}\big(f(a) * f(b)\big) = f^{-1}\big(f(a * b)\big) = a * b$
$= f^{-1}(\bar{a}) * f^{-1}(\bar{b})$.

Theorem 13

If $f: (G, *) \to (G', *')$ is a homomorphism , then

1- $f(e) = e'$,

2- $f(a)^{-1} = f(a^{-1}) \;\; \forall\, a \in G$.

Example 32

Let $(\mathbb{Z}, +)$ be the group of integers , define $f: \mathbb{Z} \to \mathbb{Z}$ by $f(x)= 2x$, it is clear that f is a homomorphism .

Example 33

Let $(\mathbb{R} - \{0\}\ ,\ .)$ and $(\{1,-1\}, *)$ be two groups , where

$*$	1	-1
1	1	-1
-1	-1	1

Define

$f: (\mathbb{R} - \{0\}\ ,\ .) \to (\{1,-1\}, *)$ by $f(x) = \begin{cases} 1 & if\ x > 0 \\ -1 & if\ x < 0 \end{cases}$

it is clear that f is a homomorphism .

Example 34

A group of all 2×2 invertable matrices $M_{2\times2}$ under matrix multiplication. The unit element is the unit matrix and the inverse of A is A^{-1}. This group is not abelian .

Define $f: (M_{2\times2}, \times) \to (\mathbb{R} - \{0\}\ ,\ .)$ by

$f(A)=|A|$ (where $|A|= a_{11}a_{22} - a_{21}a_{12}$)

it is easy to show that f is a homomorphism .

Theorem 14

If $f: (G, *) \to (G', *')$ is a homomorphism , then

1- If $(H, *)$ is a subgroup of $(G, *)$, then $(f(H), *')$ is a subgroup of $(G', *')$.
2- If $(H', *')$ is a subgroup of $(G', *')$, then $(f^{-1}(H'), *)$ is a subgroup of $(G, *)$.

Hint :

$f(H)=\{f(h)\ ;\ h \in H\}$, $f^{-1}(H')=\{a \in G\ ;\ f(a) \in H'\}$

and

$f(a) *' f(b)^{-1} = f(a) *' f(b^{-1}) = f(a * b^{-1}) \in f(H)$, $\forall\ a, b \in H$

Let $a, b \in f^{-1}(H')$

$\Rightarrow f(a * b^{-1}) = f(a) *' f(b^{-1}) = f(a) *' f(b)^{-1} \in H'$

That is $a * b^{-1} \in f^{-1}(H')$.

Corollary *

1- If $(H', *')$ is a normal subgroup of $(G', *')$, then $(f^{-1}(H'), *)$ is a normal subgroup of $(G, *)$.
2- Let $f(G)= G'$, if $(H, *)$ is a normal subgroup of $(G, *)$, then $(f(H), *')$ is a normal subgroup of $(G', *')$.

Remark

Let $f: (G, *) \to (G', *')$ be a homomorphism , define the set
$ker.f = \{ a \in G\ ;\ f(a)= e'\}$ which is called the ***kernel*** of f .

Theorem 15

If $f: (G, *) \to (G', *')$ is a homomorphism , then
f is *monomorphism* *if and only if* $ker.f = \{e\}$.

proof

$(\Longrightarrow)$ we know that $e \in ker.f$. Suppose $\exists\ a \in ker.f$ so that $f(a)= e'$

but $f(a)= e' = f(e) \Longrightarrow a = e$.

($\Leftarrow$) suppose $ker.f = \{e\}$. Let $a, b \in G$ and $f(a) = f(b)$
$\Rightarrow f(a) *' f(b)^{-1} = f(b) *' f(b)^{-1} \Rightarrow f(a) *' f(b^{-1}) = f(b) *' f(b^{-1})$
$\Rightarrow f(a * b^{-1}) = f(b * b^{-1}) = f(e) = e' \Rightarrow a * b^{-1} \in ker.f = \{e\}$
$\Rightarrow a * b^{-1} = e \Rightarrow a = b$.

Theorem 16

If $f : (G, *) \to (G', *')$ is a homomorphism , then
The pair $(ker.f , *)$ is a normal subgroup of $(G, *)$.

Proof

We know $(\{e'\}, *')$ is a normal subgroup of $(G', *')$, and
$ker.f = \{ a \in G ; f(a) = e' \} \Rightarrow ker.f = f^{-1}(e')$ so from ***Corollary ****
we have $(ker.f , *)$ is a normal subgroup of $(G, *)$.

Example 35

Let $f : (\mathbb{Z}, +) \to (\mathbb{R} - \{0\} , .)$ defined by ; $f(n) = \begin{cases} 1 & if\ n \in \mathbb{Z}_e \\ -1 & if\ n \in \mathbb{Z}_o \end{cases}$
it is clear that f is a homomorphism , and
$ker.f = \{ a \in G ; f(a) = e' \} = \{ n \in \mathbb{Z} ; f(n) = 1\} = \mathbb{Z}_e$.
It is clear that $(ker.f , *) = (\mathbb{Z}_e, +)$ is a normal subgroup of $(\mathbb{Z}, +)$,
and $(f(\mathbb{Z}), .) = (\{1, -1\} , .)$ is a subgroup of $(\mathbb{R} - \{0\} , .)$.

Theorem 17

If $(H, *)$ is a normal subgroup of $(G, *)$, then the mapping
$f_H : (G, *) \to ({}^{G}/_{H}, \otimes)$ defined by $f_H(a) = a * H$, $\forall a \in G$

f_H is a homomorphism from $(G, *)$ onto $({}^{G}/_{H}, \otimes)$, and $ker.\, f_H = H$.

Hint :

It is clear that f_H is a homomorphism which is onto , since
$f_H(a * b) = (a * b) * H = (a * H) \otimes (b * H) = f_H(a) \otimes f_H(b)$
and ${}^{G}/_{H} = \{a * H \ ; \ a \in G\}$ so

$\forall\ x \in {}^{G}/_{H} \ \exists\, a \in G$ such that $f_H(a) = a * H = x$

Now $ker.\, f_H = \{ a \in G ; f_H(a) = e * H = H \}$
$= \{ a \in G ; a * H = H \} = H$, since $(H, *)$ is a normal subgroup .

Theorem 18

If $(H, *)$ is a normal subgroup of $(G, *)$, then there exist a group $(G', *')$, and a homomorphism f from $(G, *)$ onto $(G', *')$,such that $ker.f = H$.

Hint :

We take $(G', *')$ to be the quotient group $({}^{G}/_{H}, \otimes)$, and $f = f_H$ in above

Theorem 17 .

1.15 Isomorphisms

Two groups $(G, *)$ and $(G', *')$ are said to be ***isomorphic*** , denoted $(G, *) \cong (G', *')$, if there exists a one-to-one homomorphism f of $(G, *)$ onto $(G', *')$. Such a homomorphism f is called an ***isomorphism*** (*epimorphism & monomorphism*) .

Example 36

Let two groups $(\mathbb{Z}_4, +_4)$ and $(G, *)$, where $G = \{ 1, -1, i, -i \}$ and the operation $*$ be defined by the table ;

$*$	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

1) Defined function $f : (\mathbb{Z}_4, +_4) \rightarrow (G, *)$ by $f(0)=1$, $f(1)=i$, $f(2)=-1$, $f(3)=-i$. Consequently $(\mathbb{Z}_4, +_4) \cong (G, *)$.
2) Defined function $g : (\mathbb{Z}_4, +_4) \rightarrow (G, *)$ by $g(0)=1$, $g(1)=-i$, $g(2)=-1$, $g(3)= i$. Consequently $(\mathbb{Z}_4, +_4) \cong (G, *)$.

Example 37

Let $(G, *)$, where $G = \{ e ,a ,b ,c \}$ And the operation $*$ be defined by the table ; $(G, *)$ known as Klein's four-group .

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

1) Defined the function $f : (\mathbb{Z}_4, +_4) \rightarrow (G, *)$ by $f(0)=e$, $f(1)=a$, $f(2)=b$, $f(3)=c$, it is easy to show that f is not homomorphism , since $f(1 +_4 3)= e \neq b = f(1) * f(3)$.
2) Defined the function $g : (\mathbb{Z}_4, +_4) \rightarrow (G, *)$ by $g(0)=e$, $g(1)=b$, $g(2)=c$, $g(3)=a$, it is easy to show that g is not homomorphism , since $g(1 +_4 3)= e \neq c = g(1) * g(3)$.
3) Defined the function $h : (\mathbb{Z}_4, +_4) \rightarrow (G, *)$ by $h(0)=e$, $h(1)=b$, $h(2)=a$, $h(3)=c$, it is easy to show that h is a not homomorphism , since $h(1 +_4 3)= e \neq a = h(1) * h(3)$.

Exercise 38

Show that $(\mathbb{Z}_4, +_4) \ncong (G, *)$, where $(G, *)$ Klein's four-group .

Hint :

Suppose that $(\mathbb{Z}_4, +_4) \cong (G, *)$, so there is an isomorphism say $f : (\mathbb{Z}_4, +_4) \rightarrow (G, *)$ and hence $f(x +_4 y) = f(x) * f(y) \quad \forall\, x, y \in \mathbb{Z}_4$

i.e. $f(x +_4 x) = f(x) * f(x) = e = f(0) \xRightarrow{f \text{ is } 1-1} x +_4 x = 0 \quad \forall\, x \in \mathbb{Z}_4$, contradiction .

Remark

A standard procedure for showing that two groups are not isomorphic is to find some property of one , not possessed by the other , which by its nature would necessarily be shared if these groups were actually isomorphic .

In the present case , the group $(\mathbb{Z}_4, +_4)$ and the Klein's four-group are differentiated by the fact the former is a cyclic group whereas the latter is not .

Example 39

Let ($G, *$) , where $G = \{ e ,a ,b ,c \}$
And the operation $*$ be defined by the table ;
It is clear that ($G, *$) is a cyclic group , since
$\langle a\rangle = \langle c\rangle = G$
And we know that the group ($\mathbb{Z}_4, +_4$) is cyclic ,
since $\langle 1\rangle = \langle 3\rangle = \mathbb{Z}_4$

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

1) Defined the function $f : (\mathbb{Z}_4, +_4) \to (G, *)$ by
$f(0)=e$, $f(1)=a$, $f(2)=b$, $f(3)=c$, it is easy to show that f is isomorphism ,
hence $(\mathbb{Z}_4, +_4) \cong (G, *)$

2) Defined the function $g : (\mathbb{Z}_4, +_4) \to (G, *)$ by
$g(0)=e$, $g(1)=c$, $g(2)=b$, $g(3)=a$, it is easy to show that g is isomorphism ,
hence $(\mathbb{Z}_4, +_4) \cong (G, *)$.

Example 40

The two groups $(\mathbb{Z}, +)$ and $(\mathbb{Q}\backslash\{0\} , .)$ are not isomorphic .
Suppose there exists a one-to-one onto function $f : (\mathbb{Z}, +) \to (\mathbb{Q}\backslash\{0\} , .)$
with the property $f(a+b)=f(a). f(b) \quad \forall\, a , b \in \mathbb{Z}$.
let $x \in \mathbb{Z}$, such that $f(x)=-1$, then $f(2x)=f(x+x)=f(x). f(x)=(-1).(-1)=1$
$\Longrightarrow 2x=0$ (since f is a homomorphism) $\Longrightarrow x=0$
i.e. $f(0)=-1$ and $f(0)=1$, contradicting , because f is one-to-one .

Theorem 19

Every finite cyclic group of order n is isomorphic to $(\mathbb{Z}_n, +_n)$ and every infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$.

Hint :

1) Defined $f : \langle a\rangle \to (\mathbb{Z}_n, +_n)$ by $f (a^k) = [k] , 0 \le k < n$,
where $\langle a\rangle = \{ e , a , a^2, . . . , a^{n-1} \}$.

2) Defined $f : \langle a\rangle \to (\mathbb{Z}, +)$ by $f (a^n) = n \ , \forall\, n \in \mathbb{Z}$
where $\langle a\rangle = \{ e , a , a^2, . . . , a^n, . . . \}$.

Corollary

Any two cyclic groups of the same order are isomorphic .

Remark

Let ($G, *$) be any group and $a \in G$.
defined a function $f_a : G \to G$ by $f_a(x) = a * x , \forall\, x \in G$,
and let $F_G = \{ f_a ; a \in G \}$.
The system $(F_G,\circ)$ to form a group , (where $\circ$ denotes functional composition) .

Example 41

Let $(\mathbb{Z}_4, +_4)$ be the group of integers modulo 4 and $(\langle a\rangle, *)$ be any finite cyclic group of order 8 .
Assume $f : (\mathbb{Z}_4, +_4)\to (\langle a\rangle, *)$ is define as ; $f(0)=f(2) = e$, $f(1)=f(3)= a^4$.

i) Prove that f is a homomorphism ,

ii) Describe the subgroup $(ker. f , +_4)$ and $(f (\mathbb{Z}_4), *)$.

Example 42

Let $(\mathbb{Z}_6, +_6)$ be the group of integers modulo 8 and $(\langle a \rangle, *)$ be any finite cyclic group of order 12 . Assume $f: (\mathbb{Z}_6, +_6) \to (\langle a \rangle, *)$
is define as ; $f(0)=f(3) = e$, $f(1)=f(4)= a^4$, $f(2)=f(5)= a^8$.

i) Prove that f is a homomorphism ,

ii) Describe the subgroup $(ker.f, +_6)$ and $(f(\mathbb{Z}_6), *)$,

iii) If $H=\{e, a^4, a^8\}$, show that the pair $(f^{-1}(H), +_6)$ is a subgroup of $(\mathbb{Z}_6, +_6)$.

Theorem 20 (Cayley theorem)

If $(G, *)$ be any group , then $(G, *) \cong (F_G, \circ)$.

Hint :

Define the mapping $f: G \to F_G$ by the rule $f(a) = f_a \ \forall a \in G$.

1) f is onto , since let $f_a \in F_G$ then $a \in G$ such that $f(a) = f_a$
2) f is one-to-one , suppose $f(a) = f(b) \implies f_a = f_b$
$\implies a * x = b * x , \forall x \in G$
but $e \in G \implies a = a * e = b * e = b$.
3) f is a homomorphism , since $f(a * b) = f_{a*b} = f_a \circ f_b = f(a) \circ f(b)$.

Exercise 7

Described the following functions . Is a homomorphism or not ;

1) $f: (\mathbb{Z}, +) \to (\mathbb{Q}, +)$ where $f(x) = \frac{2}{3}x$,
2) $f: (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ where $f(x) = n\,x$,
3) $f: (\mathbb{R}\backslash\{0\}, .) \to (\mathbb{R}^+, .)$ where $f(x) = |x|$,
4) $f: (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ where $f(x) = x^2$.

Exercise 8

Let $(\mathbb{Z}_8, +_8)$ be the group of integers modulo 8 and $(\langle a \rangle, *)$ be any finite cyclic group of order 12 . Assume $f: (\mathbb{Z}_8, +_8) \to (\langle a \rangle, *)$ is define as ;

$f(0)=f(4) = e$, $f(1)=f(5)= a^3$, $f(2)=f(6)= a^6$, $f(3)=f(7)= a^9$.

1- Prove that f is a homomorphism ,
2- Describe the subgroup $(ker.f, +_8)$ and $(f(\mathbb{Z}_8), *)$,
3- If $H=\{e, a^6\}$, show that the pair $(f^{-1}(H), +_8)$ is a subgroup of $(\mathbb{Z}_8, +_8)$.

1.15 The fundamental theorems

Let $f: (G, *) \to (G', *')$ is an onto homomorphism ($f(G)= G'$) from $(G, *)$ onto $(G', *')$

Theorem 21 (Factor theorem)

Let $(H, *)$ is a normal subgroup of $(G, *)$ such that $H \subseteq ker.f$. then there exist a unique homomorphism $\overline{f}: (G/_H, \otimes) \to (G', *')$ with the property

$f = \overline{f} \circ f_H$. (f_H maintain in ***Theorem 17***)

$$\begin{tikzcd} (G,*) \arrow[r, "f"] \arrow[d, "f_H"'] & (G',*') \\ ({}^{G}/_{H},\otimes) \arrow[ur, dashed, "\bar{f}"'] & \end{tikzcd}$$

Hint :

Defined $\bar{f} : ({}^{G}/_{H}, \otimes) \rightarrow (G', *')$

by $\bar{f}\,(a * H) = f(a)\,,\, a \in G$

1) It is well-defined , since

suppose $a * H = b * H$ for $a, b \in G \Longrightarrow a^{-1} * b \in H \subseteq ker.f$

$\Longrightarrow f(b) = f\,(a * a^{-1} * b) = f(a) * f(a^{-1} * b) = f(a) * e' = f(a)$.

2) $\bar{f}$ is a homomorphism , since

$\bar{f}\,[(a * H) \otimes (b * H)] = \bar{f}\,[(a * b) * H] = f\,(a * b) = f(a) *' f(b)$

$= \bar{f}\,(a * H) *' \bar{f}\,(b * H)$.

3) For each $a \in G$, $f(a) = \bar{f}\,(a * H) = \bar{f}\,(f_H(a)) = (\bar{f} \circ f_H)\,(a)$.

Corollary

The function $\bar{f}$ is one-to-one *if and only if* $ker.f \subseteq H$.

Theorem 22 (fundamental theorem)

If $f :\ (G, *) \rightarrow (G', *')$ is onto homomorphism ($f(G) = G'$) . then

$$({}^{G}/_{ker.f}\ , \otimes) \cong (G', *')\ .$$

Hint :

Defined $h : ({}^{G}/_{ker.f}\ , \otimes) \rightarrow (G', *')$

by $h(a * ker.f\ ) = f(a)$, $a \in G$.

Corollary

If $f :\ (G, *) \rightarrow (G', *')$ is a homomorphism . then

$$({}^{G}/_{ker.f}\ , \otimes) \cong (f(G), *')\ .$$

Example 43

Let $f : (\mathbb{Z}, +) \rightarrow (\mathbb{R} - \{0\}\ , .)$ defined by ; $f(n) = \begin{cases} 1 & if\ \ n \in \mathbb{Z}_e \\ -1 & if\ \ n \in \mathbb{Z}_o \end{cases}$

it is clear that f is a homomorphism , and

$ker.f = \{\, a \in G\ ;\ f(a) = e' \} = \{\, n \in \mathbb{Z}\ ;\ f(n) = 1\} = \mathbb{Z}_e$.

It is clear that ($ker.f$, $*$) $= (\mathbb{Z}_e, +)$ is a normal subgroup of $(\mathbb{Z}, +)$,

and ($f(\mathbb{Z})$, .) = ($\{1, -1\}$, .) is a subgroup of $(\mathbb{R} - \{0\}\ , .)$.

So that $\left({}^{\mathbb{Z}}/_{\mathbb{Z}_e}\ , \otimes\right) = ({}^{\mathbb{Z}}/_{ker.f}\ , \otimes) \cong (f(\mathbb{Z}), .) = (\{1, -1\}\ , .)$

Example 44

Let $(\mathbb{Z}, +)$ be the group of integers and $(\mathbb{Z}_n, +_n)$ be the group of integers modulo n . Define $f : \mathbb{Z} \rightarrow \mathbb{Z}_n$ by

$f(x) = [x]$ is onto homomorphism (***see example 30***)

$ker.f = \{ x \in \mathbb{Z} \,;\, f(x)= [0]\} = \{ x \in \mathbb{Z} \,;\, [x]= [0]\} = \{ x \in \mathbb{Z} \,;\, x \in n\mathbb{Z} \}= n\mathbb{Z}$.

Therefore

$$\left(\mathbb{Z}/_{n\mathbb{Z}} \ ,\otimes \right) = (\mathbb{Z}/_{ker.f} \ ,\otimes) \cong (\mathbb{Z}_n, +_n) .$$

Exercise 9

Consider the two groups ($\mathbb{Z}$, +) and ({1, -1, i, -i } , .) . show that the mapping defined by $f(n) = i^n$ for $n \in \mathbb{Z}$ is a homomorphism which is onto, and determine *ker.f* ? attain ***fundamental theorem*** ?

المصادر

١ -مقدمة في نظرية الزمر . د. عادل غسان نعوم ، د. باسل عطا الهاشمي ، د. محمد صالح بابان ، جامعة بغداد – ١٩٨٢ .

2- Abstract Algebra , D. M. Burton , Brown Publishers – 1988 .
3- Topics in Algebra , I. N. Herstein , John Wiley & Sons -1975 (2nd edition) .
4- Group Theory , J. S. Milue , 2010 .
5- Smarandache Special Definite Algebraic Structures , W. B. Vasantha Kandasamy , InfoLearnQuest and the author , 2009 .