HANDOUT

ABSTRACT ALGEBRA

MUSTHOFA

DEPARTMENT OF MATHEMATIC EDUCATION

MATHEMATIC AND NATURAL SCIENCE FACULTY

2012

BINARY OPERATION

We are all familiar with addition and multiplication of two numbers. Both of them combine two numbers and then give one numbers as the result. In this topic, we abstract this operation.

Definition 2.1 *Let S be non void set. A binary operation* $*$ *on set S is a function* $* : S \times S \rightarrow S$.

Based on the above definition, we know that a binary operation on *S* assigns to each ordered pair of elements of *S* exactly one element of *S*. Binary operations are usually represented by symbols like *, o ,+, × , instead of letter *f*, *g*, *h*, and so on. Moreover the image of (*a*,*b*) under a binary operation * is written $a * b$ instead of * (*a*, *b*)

Example :

a. An ordinary addition (+) and multiplication (×) on the set ℤ of integer and the set ℝ of real number is the most familiar example of binary operation

b. An ordinary subtraction on the set ℤ of integer, the set ℚ of rational number, and the set ℝ of real number is binary operation, but an ordinary subtraction on the set ℕ of natural number is **not binary operation**, because it is not function, for example $5 - 9 = -4 \notin \mathbb{N}$.

c. A function $*$ on the set ℤ of integer defined by $a * b = a + b - 1$ for all a, b $\in \mathbb{Z}$ is binary operation.

d. Let X be any set and A, B both are the subset of X. We know that $A \cap B$, $A \cup B$ and $A - B$ also subset of X. Hence, intersection, union and difference are all binary operation on the set $P(X)$.

Properties of Binary Operation

Based on the definition of binary operation, the following theorem give us detailed explanation about the definition means.

Theorem : If $* : S \times S \to S$ is a binary operation on set S, then the following condition must be satisfied.

(i) if $x \in S$ and $y \in$ S, then $x * y \in S$

(ii) if $x = y \in S$ and $s = t \in S$, then $x * s = y * t$.

(iii) if $x = y \in S$, then $x * z = y * z$ and $z * x = z * y$ for all $z \in S$.

Proof:

if $\alpha : A \to B$ is a function, then $x = y \in \mathrm{A} \Rightarrow \alpha(x) = \alpha(y)$.

(i) If $x \in S$ and $y \in$ S, then $(x, y) \in S \times S$. Since $*$ is a function from $S \times S$ to S, then $*\,(x, y) = x * y \in$ S.

(ii) If $x = y \in S$ and $s = t \in S$, then $(x, s) = (y, t) \in S \times S$. Since $*$ is a function from $S \times S$ to S, then $*\,(x, \mathrm{s}) = *\,(y, t) \Leftrightarrow x * s = y * t$.

(iii) From (ii) and $z = z$ we have $*\,(x,z) = *\,(y, z) \Leftrightarrow x * z = y * z$ and $*\,(z,x) = *\,(z, y) \Leftrightarrow z * x = z * x$.

The above theorem give us an important properties of binary operation. In part (i), it says that the order of $x * y$ is very important. We do not assume that $x * y$ is the same as $y * x$.

Statement (ii) says that if $x = y$ and $s = t$ we can substitute y for x and t for s in the expression $x * s$ and we obtain the expression $y * t$ which is equal to

$x * s$. The last part of the above theorem says that we can multiply both sides of an equation on the right or left by the same element.

Definition : Let $*$ be a binary operation on set S.

(a) The binary operation $*$ is called *associative* if $x * (y * z) = (x * y) * z$, for all $x, y, z \in S$

(b) The binary operation $*$ is called *commutative* if $x * y = y * x$ for all $x,y \in S$

(c) An element $e \in S$ is called *identity* with respect to $*$ if $x * e = e * x = x$ for all $x \in S$.

(d) An element $a \in S$ is called *idempotent* with respect to $*$ if $a * a = a$.

(e) Suppose that there exist an identity element e in S with respect to $*$. For some a $\in$ S, an element $b \in$ S is called *inverse* of a with respect to $*$ if $a * b = b * a = e$.

Example :

1. An ordinary addition on the set of all integer is *commutative* binary operation
2. Multiplication on the set of all square matrix is *non commutative* binary operation
3. An ordinary multiplication on the set of real numbers is *associative* binary operation and an ordinary subtraction on the set of all integer is an example of *non associative* binary operation, since $2 - (3 - 4) \neq (2 - 3) - 4$
4. 0 and 1 respectively are *identity* of binary operation an ordinary addition (+) and multiplication (×) in the set of all real number. The *inverse* of 2 with respect to + is -2 and the *inverse* of 2 with resepect to × is ½ , since we know that $2 + (-2) = (-2) + 2 = 0$ and $2 \times ½ = ½ \times 2 = 1$.
5. An identity $e \in S$ for some binary operation $*$ is *idempotent* since $e * e = e$

Problems

1. Assume that $*$ is a binary operation on the set S. Prove that :
   a. If e_1 and e_2 both are identities with respect to $*$ on S, then $e_1 = e_2$.
   b. If z_1 and z_2 both are zeros with respect to $*$ on S, then $z_1 = z_2$.
2. Check whether the operation given below is binary operation or not:
   a. $a * b = a + b - 10$ for all $a, b \in \mathbb{Z}$.
   b. $a \oplus b = a + b - ab$ for all $a, b \in \mathbb{Q}$.
   c. $a \otimes b = ½ (a + b + ab)$ for all $a, b \in \mathbb{R}$
   d. $a \nabla b = \dfrac{1}{ab}$ for all $a, b \in \mathbb{Q}$.
3. Determine which are the operation in problem 2 is commutative and which are associative.
4. Let $M = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \middle| a, b, d \in \mathbb{Q} \text{ and } ad = 1 \right\}$ and the binary operation is matrix multiplication. Find the identity of M and check the binary operation is associative or not.
5. Let $\mathbb{Q}$ be the set of all rational number and defined an operation $*$ on $\mathbb{Q}$ as follow : $\dfrac{a}{b} * \dfrac{c}{d} = \dfrac{a+c}{b^2+d^2}$.
   a) Show that $*$ is not binary operation on $\mathbb{Q}$
   b) Show by give a specific example that this operation not permit substitusion.

GROUP

Definition: *A non empty set G together with a binary operation $*$ on G is called group, if satisfied the following condition :*

1. *A binary operation $*$ is assosiatif*
2. *There exist $e \in G$ for all $a \in G$, such that $e * a = a * e = a$ (identity)*
3. *For all $a \in G$, there exist $b \in G$ such that $ab = ba = e$ (invers).*

If the binary operation is also commutative, then group *G* is called abelian.

Example :

1. The set of all integer with usual addition
2. $\mathbb{R} \setminus \{0\}$ with usual multiplication
3. Set of all 2 × 2 matrices over integers under matrix addition
4. The set G = { 1, -1} form a group under multiplication

Lemma : If G is group , then the following properties hold in group G :

1. Identity element is unique
2. Inverse of each element is unique
3. For all $a \in G$, $(a^{-1})^{-1} = a$
4. $ab = ac \Rightarrow b = c$ (left cancelation)

   $ab = cb \Rightarrow a = c$ (right cancelation)

Proof :

1. Suppose e_1 and e_2 both are identity in *G*.

   Since e_1 is identity, then $e_1 \, e_2 = e_2 \, e_1 = e_2$ …. (*)

   Since e_2 is identity, then $e_1 \, e_2 = e_2 \, e_1 = e_1$ ….. (**)

   From (*) and (**) we have $e_1 = e_2$.
2. Let *a* be any element of G and suppose *b* and *c* both are inverse of *a*.

   We get $b = b\,e = b\,(\,a\,c\,) = (\,b\,a\,)\,c = e\,c = c$.

3. Let a be any element of G and b is the inverse of a. Then $a\,b = e$ and $ba = e$. It show that $b^{-1} = a$, that is $(a^{-1})^{-1} = a$.
4. $ab = ac \Rightarrow a^{-1}\,a\,b = a^{-1}\,ac \Rightarrow e\,b = e\,c \Rightarrow b = c$
   $ab = cb \Rightarrow ab\,b^{-1} = cb\,b^{-1} \Rightarrow a\,\mathrm{e} = c\mathrm{e} \Rightarrow a = c.$

Theorem: *If a,b are any two elements of a group G, then the equations ax = b and ya = b have unique solutions in G.*

Proof .

Since each element in group G has unique inverse and the product of two elements of G in G then,for all $a,b \in G$, $a^{-1}b \in G$. Substituting $a^{-1}b$ for x in the left hand side of the equation $ax = b$, we have :

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

Thus $x = a^{-1}\,b$ satisfies the equation $ax = b$.

To show that the solution is unique, let x_1 and x_2 both are the solutions.

Then, $ax_1 = b$ and $ax_2 = b \Rightarrow ax_1 = ax_2 \Rightarrow x_1 = x_2$.

The similar way can be used to prove that the equation $ya = b$ has unique solution.

Theorem :*Let G be a group and m, n are any two integer. Then for all a $\in$ G,* $a^m\,a^n = a^{m+n}$ *and* $(a^m)^n = a^{mn}$.

Proof .

Case I. when m and n are positive integer

$$a^m\,a^n = \underbrace{a\;a\;a\;...\;a}_{m}\;\underbrace{a\;a\;a\;...\;a}_{n} = \underbrace{a\;a\;a\;...\;a}_{m+n} = a^{m+n}.$$

Case II. when m and n are negative integer

Let m = -k and n = -h.

$$a^m\,a^n = a^{-k}\,a^{-h} = \underbrace{a^{-1}\;a^{-1}\;a^{-1}\;...\;a^{-1}}_{k}\;\underbrace{a^{-1}\;a^{-1}\;a^{-1}\;...\;a^{-1}}_{h} = \underbrace{a^{-1}\;a^{-1}\;a^{-1}\;...\;a^{-1}}_{k+h} = (a^{-1})^{k+h}$$

$$= a^{-k-h}$$

$$= a^{m+n}.$$

Case III. when *m* is positive and *n* is negative integer.

Let n = - r for some positive integer r. Then,

$a^m\ a^n = a^m\ a^{-r} = \underbrace{a\ a\ a\ \ldots\ a}_{m}\ \underbrace{a^{-1}\ a^{-1}\ a^{-1}\ \ldots\ a^{-1}}_{r} = a^{m-r} = a^{m+n}$.

Hence all in the cases $a^m\ \ a^n = a^{m+n}$.

Problems :

1. In group G, if for all $a, b \in G$, $(ab)^2 = a^2 b^2$, prove that G is abelian.
2. If $a^{-1} = a$ for all *a* in group *G*, prove that *G* is abelian.
3. Let *G* be a group and $a \in G$. Prove that if $a^2 = a$, then *a* is identity.
4. Let *G* be a finite group with identity *e*. Prove that for any $a \in G$, there is a positive integer *n* such that $a^n = e$.

COMPLEX AND SUBGROUP

Definition : *Let G be a group. Any non empty subset H of G is called complex of G.*

Example : Let $G = \mathbb{Z}_{10} = \{ 0, 1, 2, \ldots, 9 \}$.

$H = \{ 0, 5 \}$ is complex of G.

$K = \{ 0, 4, 8 \}$ is complex of G.

As we know in the theory of set, we can define intersection ($\cap$), union ($\cup$) and multiplication on complex as below.

Definition : Let G be a group and H, K both are the complex of G. Then,

(i) $H \cap K = \{ x / x \in H \text{ and } x \in K \}$

(ii) $H \cup K = \{ y / y \in H \text{ or } y \in K \}$

(iii) $HK = \{ hk / h \in H \text{ and } k \in K \}$

(iv) $H^{-1} = \{ h^{-1} / h \in H \}$

(v) $(HK)^{-1} = \{ (hk)^{-1} / h \in H \text{ and } k \in K \}$.

Example :

Based on above example we have

(i) $H \cap K = \{0\}$

(ii) $H \cup K = \{ 0, 4, 5, 8 \}$

(iii) $HK = \{ 0, 3, 9 \}$

(iv) $H^{-1} = \{ 0, 5 \}$; $K^{-1} = \{ 0, 6, 2 \}$.

(v) $(HK)^{-1} = \{ 0, 7, 1 \}$.

If H, K both are complex of G, then we can show that $(HK)^{-1} = K^{-1} H^{-1}$.

$(HK)^{-1} = \{ (hk)^{-1} / h \in H \text{ and } k \in K \}$

$= \{ k^{-1} h^{-1} / k \in K \text{ and } h \in H \}$, since $k, h \in G$.

$= K^{-1} H^{-1}$.

In the above example, we can see that if K is complex of group G and $k_1, k_2 \in K$, then k_1k_2 may be not in K. Now, we will see when the complex has the properties as in the group.

Definition *Let G be a group and H is a complex of G. If H form a group with the same binary operation on G, then H is called subgroup of G.*

Example .

1. Let $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} / a,b,c,d \in \mathbb{R}, ad - bc \neq 0 \right\}$.

   $H = \left\{ \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} / a,d \in \mathbb{R}, ad \neq 0 \right\}$ is subgroup of G.

   $K = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} / a,b,d \in \mathbb{R}, ad \neq 0 \right\}$ is subgroup of G.

2. Let $(G , *) = (\{ 1, 2, 3, 4, 5, 6 \}, \times (\text{mod } 7))$.

   $L = (1, 2, 4 \}$ is subgroup of G .

To check whether a complex of group is subgroup or not, we can check all the three axioms in group. But the following theorems give us more simple methods to check a complex is subgroup or not.

Theorem : *A complex H of group G is subgroup of G if and only if :*

(i) $\forall\ a, b \in H \Rightarrow ab \in H.$

(ii) $\forall\ a \in H \Rightarrow a^{-1} \in H.$

Proof .

If H is subgroup of G, then $ab \in H$ and $a^{-1} \in H$ for all $a, b \in H$. Conversely, let $ab \in H$ and $a^{-1} \in H$ for all $a, b \in H$. Suppose that $a,b, c \in H$. By (i), $(ab)\ c \in$ H and $a\ (\ b\ c\ ) \in$ H. But, $a,b,\ c \in G$, then $(ab)\ c = a\ (\ bc\ )$. Thus the closure and associative properties hold.

Since $ab^{-1} \in H$ for all $a,b \in H$, then $aa^{-1} = e \in H$. Thus H has an identity. The inverse of element of H is in H by (ii). Hence H satisfies all the conditions in group. Therefore H is subgroup of G.

Theorem : *A complex H of group G is subgroup of G if and only if $ab^{-1} \in H$ for all $a, b \in H$.*

Proof .

It clear that if H is subgroup of G, then $ab^{-1} \in H$ for all $a,b \in H$. Suppose that $ab^{-1} \in H$ for all $a,b \in H$. For all $a \in H$, then $aa^{-1} = e \in H$. Thus H has an identity. Now, for any $a \in H$, $ea^{-1} = a^{-1} \in H$. Hence for each element $a \in\ H$ has inverse.

If $a,b,\ c \in H$, then $a,b,\ c \in G$. Hence the associative property hold in H. Finally, since for $a,b \in H$, $a,\ b^{-1}\ \in H$, then we have $a\ (b^{-1}\ )^{-1} = ab \in H$. Hence the closure property hold in H.

Example :

(i) We want to show that $H=\left\{\begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} / \ a, d \in \mathbb{R}, ad \neq 0\right\}$ is subgroup of

$$G = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} / \ a, b, c, d \in \mathbb{R}, ad - bc \neq 0\right\}.$$

Let $h_1 = \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix}, a, d \in \mathbb{R}, ad \neq 0$ and $h_2 = \begin{bmatrix} b & 0 \\ 0 & c \end{bmatrix}, b, c \in \mathbb{R},$ and $bc \neq 0$

$$h_1 h_2^{-1} = \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix}\begin{bmatrix} \frac{1}{\mathrm{b}} & 0 \\ 0 & \frac{1}{c} \end{bmatrix} = \begin{bmatrix} \frac{a}{b} & 0 \\ 0 & \frac{d}{c} \end{bmatrix} \in H\ .$$

Thus H is subgroup of G.

(ii) Let G be a group and $Z(G) = \{\ x \in G\ /\ xg = gx$ for all $g \in G\ \}$. Since $e \in Z(G)$, it clear that $Z(G)$ is complex of G. Let $x_1, x_2 \in Z(G)$.

$(x_1\, x_2\,)\, g = x_1\, (\, x_2\, g)$

$= x_1\, (\, g\, x_2\,)$

$= (x_1\, g)\, x_2$

$= (g\, x_1\,)\, x_2$

$= g\, (\, x_1\, x_2\,).$

Hence $x_1\, x_2 \in Z(G)$.

$X_1 \in Z(G) \quad \Rightarrow x_1\, g = g\, x_1$ for all $g \in G$

$\Rightarrow (\, x_1\, g\,)^{-1} = (\, g\, x_1\,)^{-1}$

$\Rightarrow g^{-1}\, x_1^{-1} = x_1^{-1}\, g^{-1}$ for all $g^{-1} \in G$

$\Rightarrow x_1^{-1} \in G.$

Therefore Z(G) is subgroup of G and Z(G) is called **center** of group G.

(iii) Let G be a group and H be a subgroup of G. For some $a \in G$, the set $aHa^{-1} = \{\, aha^{-1} / h \in H \,\}$ is subgroup of G.

Since H is subgroup of G, then $e \in H$, therefore $aea^{-1} = e \in H$. So H is a complex of G.

Now, take any $x, y \in aHa^{-1}$, thus $x = ah_ia^{-1}$ and $y = ah_ja^{-1}$.

$xy^{-1} = (ah_ia^{-1})\, (ah_ja^{-1})$

$= (ah_i)(a^{-1}a)(\, h_ja^{-1})$

$= a(\, hih_i)\, a^{-1}$

$= a\, h_k\, a^{-1}$

$\in aHa^{-1}.$

Hence aHa^{-1} is subgroup of G.

COSET

In the previous chapter we have discussed about subgroup and complex of group. Now, we will discuss a special type of complex called coset.

Definition :*Let H be a subgroup of group G and a is any element of G. Then,*

(i) $Ha = \{ ha/ h \in H \}$ is called **right coset** of H in G.

(ii) $aH = \{ ah/ h \in H \}$ is called **left coset** of H in G.

We know that if H is subgroup of G then H is not empty since $e \in H$. Since $He = H$ and $eH = H$ then H is a coset of G. Therefore no coset of G is an empty set. If group G is abelian, then $aH = \{ ah / h \in H \} = \{ ha/ h \in H \} = Ha$. Hence if G abelian , then the right coset is equal with the left coset.

Some examples of coset are given below :

Example :

Given $G = \mathbb{Z}_{12} = \{ 0, 1, 2, \dots , 11 \}$ under addition modulo 12 .

Let $H = \{ 0, 3, 6, 9 \}$ be a subgroup of G.The all coset of H in G are :

$H + 0 = \{ 0, 3, 6, 9 \}= H + 3 = H + 6 = H +9$

$H + 1 = \{ 1, 4, 7, 10 \} = H + 4 = H + 7 = H+ 10$

$H + 2 = \{2, 5, 8, 11\} = H + 5 = H + 8 = H + 11$

Properties of Coset :

Let G be a group and H be a subgroup of G, then :

1. If $a \in H$, then $Ha = H$ and $aH = H$.
2. If $a,b \in G$, then $Ha = Hb \Leftrightarrow ab^{-1} \in H$
3. If $a,b \in G$, then $aH = bH \Leftrightarrow b^{-1} a \in H$
4. If $a,b \in G$, then $Ha \cap Hb = \varnothing$ or $Ha = Hb$.
5. $G = \bigcup_{a \in G} Ha$

NORMAL SUBGROUP

Definition Let N be a subgroup of a group G. N is called a normal subgroup of G($N \lhd G$) iff $\forall g \in G, gN = Ng$.

Example :

1. All subgroups of abelian groups are normal.
2. S_3={(1), (1 2), (1 3), (2 3), (1 2 3), (1 3 2)}, is a symmetry group of three. N={(1), (1 2 3), (1 3 2)} is a subgroup of S_3.
   (1 2) N = {(1 2), (2 3), (1 3)} = (1 3) N = (2 3) N

   N (1 2) = {(1 2), (1 3), (2 3)} = N (1 3) = N (2 3)

   The facts above showed that every left coset N are equal to every right coset N, so $N \lhd S_3$.
3. $M = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in R \text{ } and \text{ } ad \neq bc\right\}$ with matrix multiplication are an abelian group.
   $N = \left\{\begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix} \middle| k \in R \text{ } and \text{ } k \neq 0\right\}$. Show that N is a subgroup of M. If $A = \begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix} \in N$ and $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M$, then
   $AB = \begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ka & kb \\ kc & kd \end{pmatrix}$ and
   $BA = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix} = \begin{pmatrix} ka & kb \\ kc & kd \end{pmatrix}$.
   Because AB = BA , $\forall B \in N$ and $\forall B \in M$, so BN = NB, $\forall B \in M$, such that N normal subgroup of M

Remember:

1. From definition above gN=Ng *doesn't mean* that $n \in N$ then gn = ng.
2. If G is a group, then G and each {e} is a trivial normal subgroup of G.
3. Group G ≠ {e} that doesn't have normal subgroup called *simple group.*

from definition above, $N \lhd G$ iff $\forall g \in G, gN = Ng$. gN = Ng can be replaced by gNg^{-1}= N with gNg^{-1}={gNg^{-1}|n∈N}. So gN = Ng can be replaced by $\forall n \in N, gNg^{-1} \in N$. Such that, we get theorem :

Theorem : N subgroup of G , then $N \lhd G$ iff $\forall g \in G$ and $\forall n \in N, gNg^{-1} \in N$.

Proof:

Let $\lhd G$, then gN = Ng , $\forall g \in G$ such that gNg^{-1} = N.

If $n \in N$, then

$$gng^{-1} \in gNg^{-1}$$

$$gng^{-1} \in N \text{ , } \forall g \in G$$

otherwise,

If $\forall g \in G$ and $\forall n \in N$, $gng^{-1} \in N$, then

$$(gng^{-1})g \in Ng$$

$$gn \in Ng$$

because $gn \in gN$ then

$$gN \subset Ng$$

from $gng^{-1} \in N$, $\forall g \in G$, because $g^{-1} \in G$, then

$$g^{-1}n(g^{-1})^{-1} = g^{-1}ng \in N$$

$$g(g^{-1}ng) \in gN$$

$$gn \in gN$$

But $ng \in Ng$ then

$$Ng \subset gN$$

so

$$gN = Ng$$

Example :

1. $M = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \ \in R \ and \ ad \neq bc\right\}$ with matrix multiplication are a group. If $N = \left\{\begin{pmatrix} p & q \\ r & t \end{pmatrix} \middle| p, q, r, t \ \in Q \ and \ pt - qr = 1\right\}$then $N \subset M$
   N is a subgroup of M, because if $, B \in N$, then $|AB| = |A||B| = 1$ and $|A^{-1}| = 1$, that is $AB \in N$ and $A^{-1} \in N$. Further, if $C \in M$ then $|C| \neq 0$ and $|C^{-1}| = \frac{1}{|C|}$ such that $|CAC^{-1}| = |C||A||C^{-1}| = |C||A|\frac{1}{|C|} = |A| = 1$
   that's mean $CAC^{-1} \in N$. So $N \lhd M$
2. $D_4 = \{I, R_1, R_2, R_3, M_1, M_2, M_3\}$ is a dihedral group level of four. R_i and M_j are isometric transformation of a square.
   R_i = ¼ rotation anticlockwise
   M_j = reflection of side axis and the diagonal of square. $H = \{I, R_1, R_2, R_3\}$ is a subgroup normal of D4.

3. $M = \left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| a, b, c \ \in R \ and \ ac \neq 0\right\}$ with matrix multiplication are a group. $N = \left\{\begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix} \middle| d \ \in R \right\}$ is a subgroup of M

if $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in M$ so $A^{-1} = \begin{pmatrix} \frac{1}{a} & -\frac{b}{ac} \\ 0 & \frac{1}{c} \end{pmatrix}$ if $D = \begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix} \in N$ so

$$ADA^{-1} = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \frac{1}{a} & -\frac{b}{ac} \\ 0 & \frac{1}{c} \end{pmatrix}$$

$$= \begin{pmatrix} 1 & \frac{ad}{c} \\ 0 & 1 \end{pmatrix}$$

It show that $A^{-1} \in N$, such that $N \lhd M$.

HOMOMORPHISM

Definiton

Let G be a group . A mapping f : G → G is called homorphism if for all a, b in G, f(ab) = f(a) f(b).

From this definition, we can say that homomorphism is a mapping that preserve operation of group

Example:

$(R^+, \times)$ is a group of positive real numbers under multiplication, and (R, +) is a group of real numbers under addition.

$\phi : R^+ \to R$ defined by $\phi\ (x) = \ln x, \forall\ x \in R^+$.

Since, if $a,b \in R^+$, $\phi\ (ab) = \ln ab = \ln a + \ln b = \phi\ (a) + \phi\ (b)$, then ϕ is a homomorphism.

Definition

1. Two group G and G’ is called homomorphic, if there is a homomorphism from G onto G’.
2. Two group G and G’ is called isomorphic, if there is isomorphism from G onto G’.

Theorem (Cayley Theorem)

Every finite group G isomorphic with a subgroup of subgroup of symmetric group S_n.

Based on this definition, we can say that every finite group can be written as a permutation group

Theorem

If f is homomorphism of group G to group G', then

1. $f(e) = e'$, e and e' consecutively are identity element of G and G'
2. $f(a^{-1}) = f(a)^{-1}$, $\forall\, a \in$ G

Proof:

Let f be a homomorphism from G to G'. for all $a \in$ G , $ae = a$, then $f(ae) = f(a)$, that is $f(ae) = f(a)\, e'$.

By cancelation properties in G′, we get $f(e) = e'$

Also, for all $a \in$ G , $aa^{-1} = e = a^{-1}a$, then $f(aa^{-1}) = f(e) = f(a^{-1}a)$, then $f(a)\, f(a^{-1}) = e = f(a)$. So, $f(a^{-1}) = f(a)^{-1}$.

Theorem

If f is a homomorphism of group G to group G', then the image f is subgroup G'.

Definition

If f is a homomorphism of group G to group G', then kernel of f (denoted by I) defined by

$$\text{I} = \{x \in \text{G} \mid f(x) = e'\}$$

Theorem

If f is homomorphism of group G to group G', then kernel of f is subgroup normal of G

Proof:

Let kernel of f is I = $\{x \in \text{G} \mid f(x) = e'\}$, then I $\subset$ G and since $f(e) = e'$, then $e \in$ I.

I $\neq \phi$.

Then I is a complex of G.

If a,b $\in$ I, then $f(a) = f(b) = e'$, then

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

It means $ab^{-1} \in$ I. So, I is subgroup of G.

If $k \in \mathrm{I}$ and $a \in \mathrm{G}$, then

$f(aka^{-1}) = f(a)\, f(k)\, f(a^{-1}) = f(a)\, e'\, f(a)^{-1} = f(a)\, f(a)^{-1} = e'$

It means $aka^{-1} \in \mathrm{I}$, so $\mathrm{I} \lhd \mathrm{G}$.

Theorem

If f is homomorphism of group G to group G' with kernel K, then the set of domain of $x \in \mathrm{G}'$ by f in G is right coset Ka with $a \in \mathrm{G}$ and $f(a) = x$