CHAPTER 3 SEMIGROUPS & GROUPS

Binary operation

"Binary" means "two." A binary operation is simply an operation that requires two arguments, or "inputs." For example, the arithmetic operations you learn in elementary school (+, -, x, /) are binary operations. So are dot products, cross products, and other arbitrary operations.

Let S be a non-empty set. An everywhere defined function
$f: S \times S \rightarrow S$ is called a binary operation. This takes 2 elements of S, combine them in some manner, and produce a result which is also an element of S.

eg (1)
+ is a binary operation on $\mathbb{Z}$.

For any two integers $\in \mathbb{Z}$, it is possible to find the sum. This function is everywhere defined.
For any two integers, their sum is also an integer. $\mathbb{Z}$ is said to be <u>closed</u> under this operation of **+**.

<u>eg (2)</u>
$\div$ is not a binary operation on $\mathbb{Z}$.

<u>eg (3)</u>
$\cup$ is a binary operation on P(S).

eg (4)

Let A = {0, 1}. We define binary operations $\wedge$ and $\vee$ by the following tables:

$\wedge$	0	1
0		
1		

$\vee$	0	1
0		
1		

In general, we represent a binary operation by *. The result of operating on x and y is represented by x*y, which is called the "product" of x and y.

The binary operation * on S is said to be <u>associative</u> if $(x*y)*z = x*(y*z) \quad \forall\, x, y, z \in S$
Then we may write $x*y*z$ without parentheses.

<u>eg (5)</u>

The binary operation * on S is said to be <u>commutative</u> if
$x*y = y*x \quad \forall\, x, y \in S$.

<u>eg (6)</u>

Semigroups

A non-empty set S, together with a binary operation * defined on it, is called a semigroup if this operation is associative, ie

$$(x*y)*z = x*(y*z) \quad \forall\ x, y, z \in S$$

Because of associativity of * in a semigroup, brackets are not essential.

eg. Writing a*b*c*d is as good as writing (a*b)*(c*d) or (a*(b*(c*d))).

eg (7)

Let S = $\mathbb{Z}^+$, the set of all positive integers. Let the binary operation * be the usual addition **+**. **+** is associative:

eg (8)

Let L be a lattice. The operation $\vee$ is associative:

$(a \vee b) \vee c = a \vee (b \vee c)$

eg (9)

Let A be a set of symbols. A^* is the set of all finite strings formed using symbols in A. Let & be the binary operation of concatenation (joining of 2 strings). This & is associative:

Identity

An element e of a semigroup S is called an identity element if

$$x*e = e*x = x \quad \forall\, x \in S.$$

eg (10)

In a lattice L, $a \vee 0 = a$ and $0 \vee a = a$ $\forall a$.

0 is the identity for $[L, \vee]$.

What is the identity for $[L, \wedge]$?

Theorem

If a semigroup has an identity element, then it is unique. (ie there is only one identity element.)

Monoid

A semigroup that has an identity element is called a monoid.

eg (11)

$[\mathbb{Z}, \mathbf{+}]$ is a monoid. The identity element is ___

$[\mathbb{Z}^+, \mathbf{+}]$ is a semigroup, but not a monoid: _______

eg (12)

$[P(S), \cup]$ is a monoid.

$\cup$ is associative: ________________________________

The identity element is ________________________________

eg (13)

Consider the free semigroup [A^*, &] defined in eg(9).

Let $\wedge$ be the null string (empty string). Then

α & $\wedge$ = ___ and $\wedge$ & α = ___ $\forall\, \alpha \in A^*$.

& is associative, with $\wedge$ as identity element.

So, [A^*, &] is a monoid. This is called the free monoid generated by A.

eg (14)

Let B = {0,1}. Define a binary operation $\oplus$ by the following "addition table":

$\oplus$	0	1
0		
1		

Group

A set G with a binary operation $*$ is called a group if

(1) $*$ is associative: $(a * b) * c = a * (b * c)$ $\forall a, b, c \in G$

(2) There is an identity element e such that

$e * a = a$ and $a * e = a$ $\forall a \in G$

(3) For every $a \in G$, there is an element a' such that
$a * a' = e$ and $a' * a = e$

This a' is called the inverse of a. This is usually denoted by a^{-1}.
For convenience, we sometimes write ab for $a*b$.

eg (15)

$(\mathbb{Z}, \mathbf{+})$ is a group under the usual addition, **+**.

eg (16)

$(\mathbb{Z}, \times)$ under the usual multiplication is

eg (17)

The set of all nonzero real numbers under ordinary multiplication is a group.

eg (18) Let B = {0,1}. Define binary operation $\oplus$ by the "multiplication table" shown:

$\oplus$	0	1
0		
1		

(B, $\oplus$) is a group with identity = ______

Write the inverse of each element:

Some Theorems

(1) The inverse of any element in a group is unique.

(2) Cancellation law: $ab = ac \Rightarrow b = c$

$ba = ca \Rightarrow b = c$

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

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

Subgroup

A subset H of G is called a <u>subgroup</u> of G if

(1) for any $a, b \in H$, $a*b \in H$;

(2) $e \in H$;

(3) for any $a \in H$, $a^{-1} \in H$.

eg (19)

Let $G = [\mathbb{Z}, +]$

Let H be the set of all even integers, $H \subseteq G$.

Let H_2 be the set of all odd integers,

Product of Groups

Suppose $(G_1, *_1)$ and $(G_2, *_2)$ are 2 groups.

$G_1 \times G_2 = \{(g_1, g_2): g_1 \in G_1, g_2 \in G_2\}$

$G_1 \times G_2$ is a group under the operation $*$ defined by

$(g_1, g_2) * (h_1, h_2) = (g_1 *_1 h_1, g_2 *_2 h_2)$

eg (20)

Let B = {0,1}, $\oplus$ as defined in previous example. (B, $\oplus$) is a group.

The product group $B^n = \{(b_1, b_2, \ldots, b_n) : \text{each } b_i \in B\}$ with binary operation $\oplus$:

For convenience, we may write $b_1b_2b_3\ldots b_n$ for $(b_1, b_2, b_3, \ldots b_n)$

For the case n = 2, binary operation table for B^2 is as below:

$\oplus$	00	01	10	11
00				
01				
10				
11				

The identity element of $(B^2, \oplus)$ is

Here, every element is the inverse of itself:

Left Coset and Right Coset

Let H be a subgroup of a group G.

For $a \in G$, $aH = \{ah : h \in H\}$ is called a left coset of H.

$Ha = \{ha : h \in H\}$ is called a right coset of H.

If $H = \{h_1, h_2, \ldots, h_m\}$, $aH = \{ah_1, ah_2, ,\ldots, ah_m\}$

$Ha = \{h_1a, h_2a, ,\ldots, h_ma\}$

eg (21)

Consider the group $(B^2, \oplus)$. Let $H = \{00, 01\}$

Show that H is a subgroup of B^2.

Write down all the left cosets of H.

(00)H =

Here, every left coset = the corresponding right coset as the operation $\oplus$ is commutative.

We see that:

(1) Every coset has the same number of elements as H.
(2) Cosets are either identical or disjoint.
    (ie. Distinct cosets have no common elements.)

The 2 statements above are true in general, that is, valid for any group G and any subgroup H.

The set of all distinct cosets form a partition of the group G.

Let G/H represent the set of all left cosets (may also use right cosets)
Define a binary operation $\otimes$ on the cosets by

This "operation by representative" is well defined (giving consistent results) if H has the property that every left coset is the same as the corresponding right coset. (A subgroup H with this property is called a normal subgroup.)
The binary operation $\otimes$ is associative:

The identity of $\otimes$ is ___.
The inverse of aH is _____.
G/H under the binary operation $\otimes$ is a group. This is called the quotient group of G relative to H.

Eg (22)
Write the binary operation table for the quotient group of B^2 relative to the subgroup H in the preceding example.

$\otimes$	(00)H	(10)H
(00)H		
(10)H		

Extra example 1

Show that the binary operation on $\Re$ defined by $x * y = 2 + xy$ is commutative but not associative.

Extra example 2

Determine whether the description of $*$ is a valid definition of binary operation on the set. Justify your answer.

(i) On $\mathbb{Z}$, where $x * y = \frac{x}{y}$

(ii) On $\mathbb{Z}^+$, where $x * y = x^y$

(iii) On $\mathbb{Z}$, where $x * y = \frac{2x}{y}$

(iv) On $\mathbb{Z}^+$, where $y * z = 4y - z$

(v) On $\mathbb{R}^+ - \{0\}$, where $x * y = x^{-y}$

Extra example 3

A binary operation * is defined on the set $S = \{a, b, c\}$ by the following table:

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

By evaluating $(c*a)*b$ and another suitable expression, show that $[S, *]$ is not a semigroup.

Extra example 4

The set of all integers, $\mathbb{Z}$, is a group under the usual addition. Let H be the set of all multiples of 5 (including negative multiples). Show that H is a subgroup of $[\mathbb{Z}, +]$.

Extra example 5

:

Determine whether the following binary operation * gives a group structure on $\mathbb{R}^+$

Let * be defined on $\mathbb{R}^+$ by $a * b = \sqrt{ab}$.

Extra example 6

Let $G = \{0, 1, 2, 3, 4, 5\}$ and * be a binary operation on G defined as
$a * b$ = the remainder when $a + b$ is divided by 6.
The binary operation table is given below:

	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

It is known that * is associative and $[G, *]$ is a group.

(i) Briefly state what is meant by saying that * is associative.

(ii) Determine whether * is commutative.

(iii) State the identity element of $[G, *]$.

(iv) State the inverse of each element in $[G, *]$.

(v) Give an example of a subgroup of $[G, *]$ consisting of 2 elements.