Lecture # VIII part I

INTRODUCTION TO ALGEBRA, AND ALGEBRAIC STRUCTURES

Our mathematical studies are usually focused on sets equipped with one or more binary operations. Eg. set of integers under + and ×, Logical propositions under conjunction and disjunction. And such operations exhibit similarities in which they can be manipulated.

8.1 Binary Operations, Semigroups, monoids, and Groups:

8.1.1 Binary operations: The most basic setting for mathematical computation is set together with a binary operation. The familiar operations of addition and multiplication are the prototypical binary operations.

Definition: A binary operation $*$ on a set A is a fct $f_* : A \times A \to A$

Exple: define $f_+ ; \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ by $f_+(a,b) = a+b$

or in a abstract form:

Table 8.1

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

The table is symmetric. Same entry for (x,y) and (y,x) which means that $x * y = y * x$. The operation is commutative. we also may verify that $x * (y * z) = (x * y) * z$. The operation is associative.

Definition: A binary operation $*$ on a set A is said to be associative if for every three elements $a, b,$ and c in A, we have $(a * b) * c = a * (b * c)$. It is commutative if for every a and b in A, we have $a * b = b * a$.

Exple: $(\mathbb{R}, \cdot)$, Ass. Com, $(\mathbb{N}, -)$ Not Ass. not Comm., $(\mathbb{R}, -)$ $\overline{A}, \overline{C}$

$(\mathbb{R}, \#)$, $x \# y = |x-y|$, C, $\overline{A}$ because $|2 - |2-3|| = 1$

$||2-2|-3| = 3$, $\begin{array}{c|cc} * & a & b \\ \hline a & b & a \\ b & a & a \end{array}$ C, $\overline{A}$, $(M_n, \cdot)$ M_n set of square matrices.

8.1.2 Semigroups: Let A be a set and let $*$ be a binary associative operation on A. We call A a semigroup under $*$ and denote this Algebraic structure by $(A, *)$.

Exples of semigroups: $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\text{sets}, \cup)$, $(\text{sets}, \cap)$

Now if we looked back into table 8.1, $(A, *)$, we find that that $x * a = x$. The same role is played by the number 1 on the integers $\mathbb{Z}$ under multiplication, $1 \cdot x = x$. The same with $(\mathbb{Z}, +)$ and 0. But in the set of integers there is no element e such that $e - x = x$ but $x - 0 = x$. Therefore the following

Definition: Let $*$ be a binary operation on a set A. Let e be an element of A.

(a) We say that e is a right identity element if for each element x in A, we have $x * e = x$

(b) " " " " " left " " " " " " " " " " " " $e * x = x$

(c) We say that e is an identity if it is both right and left identity element.

Exple: $(\mathbb{Z}, +)$ 0 is both right and left.

Consider the following table 8.2

Table 8.2

	a	b	c
a	a	b	c
b	a	c	b
c	a	b	c

both a and c are left identities

There is no way that there exist one Right identity and one left identity, for the same $(A, *)$, that are distinct.

Proposition 1: Let $(A, *)$ be given. Let e_R be the right identity and e_L be the left identity. Then $e_R = e_L$

Prof: $e_R * e_L = e_R$, $e_R * e_L = e_L \Rightarrow e_R = e_L$.

8.1.3 Monoids:

Definition: Let $(A, *)$ be a semigroup. Let e be an identity in A, we call A a monoid, and denote the algebraic structure $(A, *, e)$.

The most familiar monoids are $(\mathbb{Z}, +, 0)$, $(\mathbb{Z}, \cdot, 1)$

Exple: $(\mathcal{P}(S), \cap, S)$

Let $*$ be a binary operation on a set A, and let B be a subset of A $B \subseteq A$. B is said to be closed under $*$ if for every pair of elements (x, y) in $B \times B$, we have $x * y$ also in B.

Exple: $(\underset{E_e}{\text{Set of even integers}}, +)$, $(\{-2, 0, 2, 4, \dots\}, +)$ closed under $+$

$(\underset{E_o}{\text{Set of odd integers}}, +)$, is not closed. $3 + 5 = 8 \notin E_o$.

Definition: Let $(A, *, e)$ be a monoid, and let B be a subset of A. The set B is a submonoid of A if B is closed under $*$, and e is an element of B.

Exple: $(E_e = \text{set of even integers}, +)$ is a submonoid of $(\mathbb{Z}, +)$

$(E_e, \cdot)$ is not submonoid of $(\mathbb{Z}, \cdot)$

Also: consider $(\mathcal{P}(S), \cap)$ and $(\mathcal{P}(A), \cap)$ $S \subset A$ proper subset.

Both are monoids, $\mathcal{P}(S)$ is not a submonoid. because they don't have the same identity.

Exercise: we wish to obtain the smallest monoid S of $(\mathbb{Z}, +, 0)$ that contains 6 and -4.

Of course S must contain 0 and must be closed. Thus it must contain: $0, 6, -4, 6-4=2, -4+2=-2, -4-2=-6, 6-2=4$

$\Rightarrow E_e$ must be the smallest submonoid of $\mathbb{Z}$ that contains

8.1.4. **Groups:** within the structure of a Monoid $(A, *, e)$ we are guaranteed that we can solve for x in even the simplest equation of the form $a*x = b$ where a, and $b \in B$. For example:

in $(\mathbb{Z}, \cdot, 1)$ $3x = 5$ no integer solution - However in $(\mathbb{Z}, +, 0)$ we can solve always the equation $a+x = b$ for exactly one value of x.

In this section we examine monoids like $(\mathbb{Z}, +, 0)$ in which the equation $a * x = b$ has always a solution. Such structures are called groups.

Definition: ① Let $*$ be a binary operation on the set A, and let e be the identity element for $*$. Let a and b be elements of A we say that b is the inverse of a if $a * b = b * a = e$ and we write $b = a^{-1}$

Definition: ② Given a monoid $(A, *, e)$. If every element of A has an inverse then we call $(A, *, e)$ a **group**

Definition: ③ If $(A, *, e)$ is a group and the operation $*$ is commutative, we call A an **abelian group**.

Definition ④ Let $(A, *, e)$ be a group. The **order of the group** is the cardinality of A. It is denoted $|A|$.

Examples: ① $a * x = b \Rightarrow a^{-1} * a * x = a^{-1} * b = e * x = a^{-1} * b$

$$\Rightarrow \boxed{x = a^{-1} * b}$$

② $(\mathbb{Z}, +, 0)$ is an abelian group.

$(\mathbb{Q}, \cdot, 1)$ is not a group.

$*$	a	b
a	a	b
b	b	a

$a*b$?

③ $(\mathbb{Q}^+, \cdot, 1)$ is an abelian group.

④ $(\mathbb{Z}, +, 0)$ and $(\mathbb{Q}^+, \cdot, 1)$ are groups of infinite order.

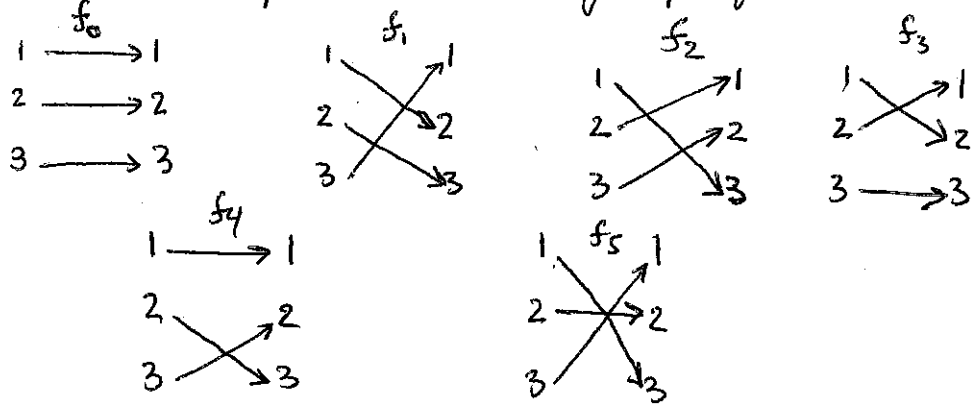
abelian groups of order 4.

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

Let $X_n = \{1, 2, \ldots, n\}$. A permutation is bijection from $X_n \to X_n$.
Let S_n be the set of all bijections $S_n = \{ f : X_n \to X_n, f \text{ is bijective} \}$
and let "$\circ$" denote the composition of functions.

S_n is called the permutation group of the set X_n

Example:



$\circ$	f_0	f_1	f_2	f_3	f_4	f_5
f_0	f_0	f_1	f_2	f_3	f_4	f_5
f_1	f_1	f_2	f_0	f_5	f_3	f_4
f_2	f_2	f_0	f_1	f_4	f_5	f_3
f_3	f_3	f_4	f_5	f_0	f_1	f_2
f_4	f_4	f_5	f_3	f_2	f_0	f_1
f_5	f_5	f_3	f_4	f_1	f_2	f_0

it is a group.

$f_1 \circ f_3 = f_5 \neq f_3 \circ f_1 = f_4$

$f_2^{-1} = f_1$

$$f_1 \circ f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = f_5$$

$$f_3 \circ f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = f_4$$

$$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad f_2^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Solve Cancellation law —

$g \circ f_2 = f_3 \longrightarrow g \circ f_2 \circ f_2^{-1} = g = f_3 \circ f_2^{-1} = f_3 \circ f_1 = f_4$

$f_2 \circ g = f_3 \longrightarrow f_2^{-1} \circ f_2 \circ g = g = f_2^{-1} \circ f_3 = f_1 \circ f_3 = f_5$

In general we denote a group by $(G, \circ)$.

8.1.5 **Subgroups** Let $(G, \circ)$ be a group with respect to a binary operation "$\circ$". A subset H of G $(H \subset G)$ is called a subgroup of $(G, \circ)$, if H is closed under "$\circ$" and ~~$(H, \circ)$ forms a group itself~~ whenever $x \in H$, then x^{-1} also belongs to H.

Exple: ① $(E_e, +, 0)$

② $(\mathbb{Z}_4, +, [0])$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$(\{[0], [2]\}, +)$ is a subgroup of $(\mathbb{Z}_4, +, [0])$ because closed $[0]+[0]=[0]$, $[0]+[2]=[2]$ and inverse exist.

Order of a subgroup is the cardinality of the subset, H.

Notation: Let $x \in G$, and $(G, \circ)$ be a group,

x^k is defined as x operated with itself k time.

if $x \in \mathbb{Z}$, $(\mathbb{Z}, +)$, $x^k = \underbrace{x + x + x + \cdots + x}_{k \text{ times}}$

Sometimes, it may happen that a subgroup is generated by one element. The subgroup is called cyclic subgroup.

$$\langle x \rangle = \{x^0, x, x^2, \ldots, x^{k-1}\}$$

$$= \{e, x, x^2, \ldots, x^{k-1}\}.$$

If $G = \langle x \rangle \Rightarrow (G, \cdot)$ is cyclic group.

Exple: $G = \{1, -1, i, -i\}$

HW # 7. Page 350 # 2, #6
351 # 8
352 # 16, #17
353 # 18
354 # 26.

Page 319 # 4, 10
329 # 6, 8, 10
330 # 14.