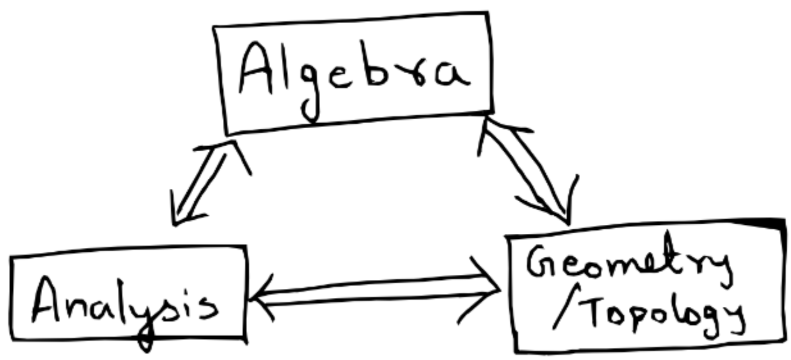
Math111a: Abstract Algebra notes

Mann Malviya

Fall 2024

Lecture 1

The 3 main pillars of modern mathematics,



Some of the features of math which distinguishes it from other areas of knowledge,

- proof (objective truth)
- axiomatization (the axiomatic approach)
- abstraction

These are very well exemplified in the study of Algebra(A.K.A Abstract Algebra).

"Abstract Algebra":Study of various different kinds of "algebraic structures".
Eg: $\underbrace{\text{groups}}_{\text{Math 111a}}$, $\underbrace{\text{rings, fields}}_{\text{Math 111b}}$, $\underbrace{\text{vector spaces}}_{\text{Math 117}}$, modules, algebras.

Each kind of algebraic structure is axiomatized: A set + some operations subject to some axioms.

This Course: Group Theory

Chapter I: Fundamentals

§(I.1) The definition of a group

Definition:

A binary operation(or law of composition) on a set S is a rule which assigns to any pair of elements of S a third element of S. More formally it is a function.

$$m : S \times S \to S$$

$$(a, b) \mapsto m(a, b)$$

where $S \times S = \{(a, b)|a, b \in S\}$ is the set of ordered pairs of elements of S. It maps an ordered pair (a, b) to some element $m(a, b) \in S$.

Example. Addition defines a binary operation on the set $\mathbb{Z}$ of integers.

$$\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$

$$(a, b) \mapsto a + b$$

Example. Multiplication also defines a binary operation on $\mathbb{Z}$.

$$\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$

$$(a, b) \mapsto ab$$

There are many more examples of a similar nature.

Example. Multiplication also defines a binary operation on the set $\mathbb{Z}^+$.

$$\mathbb{Z}^+ \times \mathbb{Z}^+ \to \mathbb{Z}^+$$

$$(a, b) \mapsto ab$$

Non-Example. Multiplication does not define a binary operation on the set $\mathbb{Z}^-$. Easy way to see this is,

$$((-1)(-2) = +2)$$

Example. Addition of matrices defines a binary operation on the set $M_{m\times n}(\mathbb{R})$ of all $m \times n$ matrices with real entries.

$$M_{m\times n}(\mathbb{R}) \times M_{m\times n}(\mathbb{R}) \to M_{m\times n}(\mathbb{R})$$
$$(A, B) \mapsto A + B$$

Example. Multiplication of matrices defines a binary operation on the set $M_n(\mathbb{R})$ of square $n \times n$ matrices with real entries.

$$M_n(\mathbb{R}) \times M_n(\mathbb{R}) \to M_n(\mathbb{R})$$
$$(A, B) \mapsto AB$$

Note that $AB \neq BA$ in general, For example, take $n = 2$,

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \;\&\; B = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$$

$$AB = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}$$

$$BA = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

we can clearly see, $AB \neq BA$.
Thus a binary operation $m : S \times S \to S$ need not be commutative. We can have $m(a, b) \neq m(b, a)$. The order can matter. This shouldn't be too hard to believe as in the case of ordered pairs, $(a, b) \neq (b, a)$ unless $a = b$

Definition:

A <u>group</u> is a set G equipped with a binary operation.

$$G \times G \to G$$

$$(a, b) \mapsto ab$$

Such that the following axioms hold:

(1) The group operation is associative, i.e.,

$$(ab)c = a(bc) \quad \forall a, b, c \in G$$

(2) There exits an element e in G such that,

$$ea = a = ae \quad \forall a \in G$$

(3) For every a in G, there exists an element a^{-1} in G such that,

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

<u>Remark:</u>

- The element e in axiom (2) is <u>unique</u>.
  Indeed, suppose e' were another element satisfying, $e'a = a = ae', \quad \forall a \in G$.

  $$e \underset{\text{(2) for e'}}{=} ee' \underset{\text{(2) for e}}{=} e$$

  This unique element of the group is called the <u>identity element</u> of the group.

- The element a^{-1} in Axiom (3) is also unique and called the <u>inverse</u> of a.
  Suppose a' were an element such that $aa' = e = a'a$

  $$a^{-1} \underset{(2)}{=} a^{-1}e \underset{\text{(3) for a'}}{=} a^{-1}(aa') \underset{(1)}{=} (a^{-1}a)a' \underset{\text{(3) for a}}{=} ea' \underset{(2)}{=} a'$$

  In a sentence: "A group is a set equipped with an associative binary operation which has an identity element and in which every element has an inverse."

- Axiom (3) is probably the most significant of the axioms because it distinguishes the notion of a group from many other algebraic structures.
  "It implies that in a group, multiplying by any element can be "undone""

  $$a \rightsquigarrow ab \rightsquigarrow (ab)b^{-1} = a(bb^{-1}) = ae = a$$

- The associativity axiom is common but important. However, there do exist non-associative operations in math.
  <u>Example:</u> The cross product $\vec{v} \times \vec{w}$ of vectors in 3-dimensions Euclidean space defines a non-associative binary operation in $\mathbb{R}^3$(see the exercises).

- Suppose we have an ordered sequence $a_1, a_2, ..., a_n$ in a group G that we would like to multiply together. There will be many ways of doing this by successively multiplying pairs of elements together.
  <u>For Example:</u> There are 2 ways of multiplying together a sequence of n=3 elements a,b,c.

  $$a(bc)$$

  $$(ab)c$$

Axiom (1) asserts that the result is the same,

$$(ab)c = a(bc)$$

On the other hand there are 5 ways of multiplying n=4 elements together, a,b,c,d.

$$((ab)c)d$$

$$(a(bc))d$$

$$(ab)(cd)$$

$$a((bc)d)$$

$$a(b(cd))$$

One can show using Axiom (1) that they all coincide.
Eg:

$$\begin{aligned} ((ab)c)d &= (a(bc))d \\ &= a((bc)d) \\ &= a(b(cd)) \end{aligned}$$

Theorem. *(The Generalized Associativity Law) The result of multiplying together an ordered sequence of elements in a group does not depend on the choice of bracketing.*

The proof of this Theorem is a very tedious inductive argument which can be found in books.
Remark: The generalized associativity law allows us to speak of the element.

$$a_1 a_2 ... a_n \in G$$

Without specifying brackets.
Exercise: Show:

- $e^{-1} = e$
- $(ab)^{-1} = b^{-1}a^{-1}$
- $(a_1 a_2 ... a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} ... a_2^{-1} a_1^{-1}$

hint: Use the property that the inverse element is unique. The 3rd exercise requires Induction.
Remark: For any element a in a group G, we define,

$$a^0 = e$$

$$a^1 = a$$

$$a^2 = a \cdot a$$

$$\vdots$$

$$a^n = a(a^{n-1}) = \underbrace{aa...a}_{\text{n times}}$$

for any $n \geq 1$.
Also we define,

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

for any $n \geq 1$.
Thus we have a well-defined element

$$a^n \in G$$

for every integer $n \in \mathbb{Z}$

Definition:

Let a be an element in a group G. If there is some integer $n \geq 1$ such that $a^n = e$, then a is an element of finite order. Otherwise, a is an element of infinite order.

$$... \ a^{-2} \quad a^{-1} \quad a^0 = e \quad a^1 = a \quad a^2 \quad a^3 ...$$

Exercise: Prove:

$$a^n = e \quad \text{iff} \quad a^{-n} = e$$

The order of a is the least +ve integer n such that $a^n = e$, or ∞ if there is no such n.
Example: e is the unique element of order 1.

Definition:

A group G is finite if it has finitely many elements. Otherwise G is infinite.
The order of a group G(either finite or infinite) is its cardinality, i.e., the number of elements in G. We write $|G|$ for the order of G.

Definition:

A group G is said to be abelian (or commutative) if $ab = ba, \quad \forall a, b \in G$

In general, we say that two elements $a, b \in G$ commute if $ab = ba$.

§(I.2) Examples

Example: The set $G = \{e\}$ which has a single element with the only one possible multiplication is a group. It is called the trivial group(a unique group with order 1).
Remark: If $G = \{a_1, a_2, ..., a_n\}$ is a finite group, then we can completely specify the group operation by writing down a multiplication table.

xy	a_1	a_2	...	a_n
a_1	a_1a_1	a_1a_2	...	a_1a_n
a_2	a_2a_1	a_2a_2	...	a_2a_n
:		:		:
a_n		...		a_na_n

Example: Let $G = \{e, a\}$ be the 2-element set with multiplication table.

	e	a
e	ee	ea
a	ae	$aa = e$

This table can be simplified and written as,

	e	a
e	e	a
a	a	e

This is a group of order 2.
Example: Let $G = \{+1, -1\}$ with ordinary multiplication.

	$+1$	-1
$+1$	$+1$	-1
-1	-1	$+1$

This is essentially the same group as the previous example, we have just labelled things differently.
Example: Let $G = \{e, a, b\}$ with

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Is a group of order 3.
Saying a group is abelian is same as saying multiplication table is symmetric about the diagonal.

Exercise: The multiplication table for a finite group must be a latin square, i.e., every element appears exactly once in each row and column.
Example: $G = \{e, a, b, c\}$. The following are 2 groups of order 4:

G_1	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

G_1	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$$G_1 = \langle a | a^4 \rangle$$
$$G_2 = \langle a, b | a^2, b^2, [a, b] \rangle$$

Lecture 2