Group Theory

Lecture 1

Books :

(1) Algebra by Artin

(2) Abstract Algebra by Dummit & Foote

(3) Abstract Algebra by Gallion

(4) Algebra by Herstein

(5) Algebra vol I & II by N. Jacabson.

Main objective is to solve poly eqn.s in algebra.

In linear Algebra you learnt Gauss-Elimination method to solve a system of linear equations.

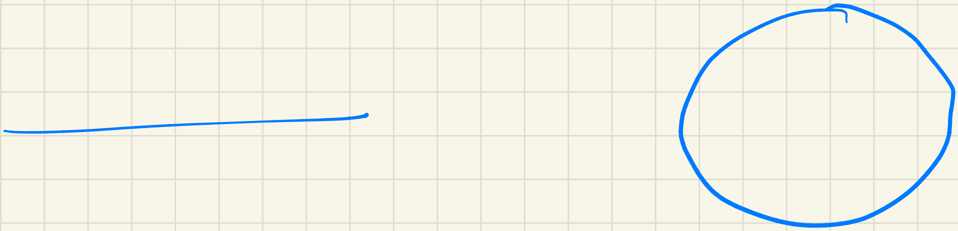
Q How to solve a system of Non-linear eqn.s?

— Gröbner basis is useful.

— In solving optimization problem we use algebra and algebraic geometry

— Application in statistics.

— Application in Graph Theory



Top space $\rightsquigarrow$ group (Fundamental gp).

Homeomorphic $\rightsquigarrow$ isomorphic

- Algebraic top.
- Number theory
- Coding theory

Group theory was introduce to study the symmetry of objects.

$\mathbb{Z}, +$ $\quad a, b \in \mathbb{Z}$

$a+b \in \mathbb{Z}$. $\quad 0 \in \mathbb{Z}, \quad a+0=a.$ $\quad a-a=0,$

$\mathbb{Q}, +$, $\mathbb{R}, +$, $\mathbb{C}, +$, $\pm$

$\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$, $\cdot$; $\quad a \cdot 1 = a$

$a \cdot \frac{1}{a} = 1$

$\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$, $\cdot$ $\quad z \cdot \frac{1}{z} \cdot 1.$

$\boxed{\mathbb{Z}^\times = \mathbb{Z} \setminus \{0\} \quad ; \quad \cdot}$

$a \cdot 1 = a.$

Does $\exists$ an int $\in \mathbb{Z}^\times$ s.t

$a \cdot a' = 1$?

$GL_n(\mathbb{R})$ = Set of all $n \times n$ invertible matrices.

A, B

matrix multiplication.

Identity matrix.

$SL_n(\mathbb{R}) = \{ A \in GL_n(\mathbb{R}) \mid \det A = 1 \}$

wrt matrix multiplication

A has certain properties.

$O_n(\mathbb{R}) = \{ A \in GL_n(\mathbb{R}) \mid A \text{ is orthogonal} \}$

$SO_n(\mathbb{R}) = \{ A \in O_n(\mathbb{R}) \mid \det A = 1 \}$

wrt matrix multiplication

has certain properties.

Let T be any set.

$S_T = \{ f : T \longrightarrow T \mid f \text{ is 1-1 \& onto} \}$.

with composition operation have certain properties

Identity elt is the identity map.

Suppose $T = [n] = \{1, 2, \ldots, n\}$.

then $S_T = S_n$ is called symmetric group. The elements of S_n are called permutations with $n!$ elts.

<u>Group:</u>

A group is a set on which an operation or law of composition is defined with certain properties

A law of composition (or operation) on a set S is a map $f: S \times S \to S$
a, b resp.
for $a, b \in S$ then $f(a,b)$ denoted by
<u>ab</u> or <u>$a \times b$</u> or <u>$a+b$</u> or <u>$a \circ b$</u> etc.

Properties of law of composition:

(1) A law of composition is said to be associative on a set S if $(ab)c = a(bc)$, $\forall a,b,c \in S$.

(2) A law of composition is said to be commutative if $ab = ba$ $\forall a,b \in S$.

(3) An identity for a law of composition is an elt $e \in S$ s.t $ea = ae = a$ $\forall a \in S$ [In $(\mathbb{R},+)$ e is 0. since $0+a = a+0 = a$ $\forall a \in \mathbb{R}$]

(4) Suppose that the law of composition has identity. Then an elt $a \in S$ is called invertible if $\exists$ $a' \in S$ s.t $aa' = a'a = e$.

a' is called the inverse of a.

<u>Defn</u> A group is a non-empty set $\boxed{G}$ together with a law of composition (or binary operation) which is associative and has an identity elt and every elt of G has an inverse.

Moreover if the law of composition is commutative then G is called an abelian group.

Examples of Groups:

(1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are gps under addition.

(2) $\mathbb{R}^\times$, $\mathbb{C}^\times$, $\mathbb{Q}^\times$ are groups under multiplication

(3) $GL_n(\mathbb{R})$, $SL_n(\mathbb{R})$, $O_n(\mathbb{R})$, $SO_n(\mathbb{R})$ are

groups under matrix multiplication.

(4) S_T is a group under composition of maps.