Group Theory

Lecture 1

05/01/2022

Books:

(1) Algebra — Artin

(2) Abstract Algebra — Dummit & Foote

(3) Contemporary abstract algebra — Gallian

(4) Algebra — Herstein

(5) Basic Algebra Vol I & II — Nathan Jacobson.

One Main purpose is to solve eqn. or find the roots of poly f.n.s.

It is known how to find the roots of a quadratic poly

$$ax^2 + 2bx + c = 0.$$

The roots are of the form

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

We have a compact formula to find the root using basic operations like addition, subtraction multiplication, division, square root.

Q Do we have a compact formula for finding roots of a poly of deg $n \geq 3$?

For deg 3 and deg 4 we have explicit formula for finding the roots using basic operations.

Galois was a French Mathematician (1811 — 1832).

- He was the first to use the word "group" that we study today
- He introduced the concept of finite fields.
- He showed that solvn of a poly eqn is related to the structure of gp permutations associated with the roots of the poly, the Galois gp of the poly.
- He proved a poly of deg ≥ 5 is not solvable.

This will be proved in Galois Theory.

Applications in other areas:

— Algebraic Geometry.

You know how to find the solns. of a system of linear Eqn.s. The method is Gauss Elimination.

Let $f_1 = 0, f_2 = 0, \ldots, f_n = 0$ where $f_i \in k[x_1, \ldots, x_n]$. f_i - poly.

$V(f_1, f_2, \ldots, f_m)$ = The set of common zeros of $f_1, \ldots f_m$

↓

variety.

Q How to find the soln. of a system of eqn.s (not necessarily linear)?

— Gröbner bassis is the tool.

— Solving optimization Problem.

— application in Statistics (algebraic Statistics).

— application in graph Theory

— algebraic top.

top space ⇝ associate a gp (fundamental gp)

homeomorphic ⇝ isomorphic.

— Number Theory

— Coding Theory.

In this course we mainly study

Groups Ring.

(1) $\mathbb{Z}$. $\ni a, b. \Rightarrow a+b \in \mathbb{Z}$.

$\downarrow$

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

$$a+(-a)=0$$

(2) $\mathbb{Q} \ni a, b \Rightarrow a+b \in \mathbb{Q}$

$$a+0=a$$

$$a+(-a)=0.$$

(3) $\mathbb{R} \times \mathbb{C}$. with addition operation.

(4) $\mathbb{Q}$. consider the operation multiplication.

$a, b \in$

$a \cdot b \in \mathbb{Q}$. $\qquad a \cdot \frac{1}{a} = 1$

$a \cdot 1 = a \qquad \mathbb{Q}^{\times}$ = non zero rationals

(5) $\mathbb{Z}^\times \ni a, b$ $\quad a \cdot b \in \mathbb{Z}$.

$a \cdot 1 = a$.

But there doesn't exists any elt $b \in \mathbb{Z}$ s.t $a \cdot b = 1$.

$\mathbb{Z}^\times$ wrt multiplication doesn't have this property.

(6). $GL_n(\mathbb{R}) = \{ A \in M_n(\mathbb{R}) \mid A \text{ is invertible} \}$.

$M_n(\mathbb{R})$ is the set of all $n \times n$ matrices with real entries.

$A, B \in GL_n(\mathbb{R})$. consider matrix multiplication.

$A \cdot B \in GL_n(\mathbb{R})$

$A \cdot Id = A \quad \forall A \in GL_n(\mathbb{R})$

$A \cdot A^{-1} = Id$.

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

$\cup$

A, B $\quad$ $A \cdot B \in SL_n(\mathbb{R})$.

$A \cdot Id = A$.

$A \cdot A^{-1} = Id$.

(8) $O_n(\mathbb{R})$ = The set of orthogonal $n \times n$ matrices.

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

Both of them satisfies the three conditions wrt matrix multiplication operation.

(a) Let T be any set.

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

Consider the composition operation on S_T.

let $f_1, f_2 \in S_T$ then $f_1 \circ f_2 \in S_T$

$$f_1 \circ 1_T = f_1$$

$$f_1 \circ f_1^{-1} = 1_T$$

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

$S_T = S_n$ is called the symmetric gp.

$$S_n = \{ f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\} \mid f \text{ is bijective} \}$$

$$|S_n| = n!$$

A law of composition (binary operation) on a set S is a map $f : S \times S \longrightarrow S$ and $f(a, b)$ for $a, b \in S$ is denoted by $a + b$ or ab, or $a \circ b$ or $a \times b$.

Example: (1) $f: \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$ defined by

$$f(a,b) = a+b.$$

$$f(a,b) = a \cdot b$$

(2) $M_n(\mathbb{R}) \times M_n(\mathbb{R}) \longrightarrow M_n(\mathbb{R})$

$$(A, B) \longmapsto A+B$$

$$(A, B) \longmapsto A \cdot B.$$

Properties of law of composition :

Defn :

(1) A law of composition is said to be associative on 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

$$e \cdot a = a \cdot e = a \quad \forall a \in S.$$

If we write the law of composition with the notation '+' then we write '0' for identity and if we write the law of composition with the notation '.' then '1' is used for multiplicative identity.

(4). Suppose the law of composition have an identity e. Then an elt $a \in S$ is called invertible if $\exists b \in S$ s.t $a \cdot b = b \cdot a = e$.

(Ex) **Remark** (1) There can be at most one identity.

(2) If the inverse of an elt exists then it is unique.

If we write the law of composition with '+' then the inverse of a is denoted by $-a$.

If we write the law of composition with '.' then the inverse of a is denoted by a^{-1}.

Ex. (1) $(a^{-1})^{-1} = a$

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

Defn: A group is a non-empty set G together with a law of composition (or binary operation) which associative and has identity elt and every elt of G has an inverse.

$(G, \cdot)$

Examples of Groups:

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

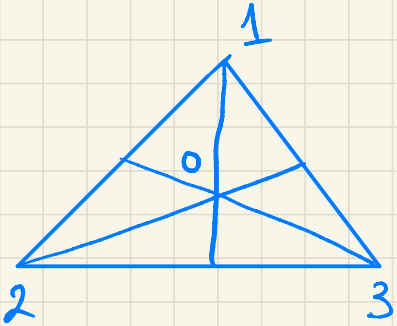
(2) $\mathbb{R}^\times$, $\mathbb{C}^\times$, $\mathbb{Q}^\times$ are group under multiplication

(3) $GL_n(\mathbb{R})$, $SL_n(\mathbb{R})$, $O_n(\mathbb{R})$, $SO_n(\mathbb{R})$ are group under matrix multiplication

(4) S_T is a group under composition.
S_n is a gp with cardinality $n!$.

If a gp G is a finite set then it is called a finite group.

Group Theory was originally studied in order to study the symmetries



we would like to study the symetries. Symmetries means invariance under transformation.

Check that it forms a gp wrt the six transformation :