Lecture I: Overview & Introduction to Groups

MATH 5111, 5590H: Honors Abstract Algebra I

Instructor: Maria Angelica Cueto

- Office Number: MW 636 (Math Tower)
- Email: cueto.5@osu.edu

Textbook: Dummit & Foote: "Abstract Algebra", 3rd Edition, Wiley.

§1.1 Overview:

This is part one of a very intense year-long course in Abstract Algebra. We'll cover Chapters 1-9 & 15 from the textbook.

Topics: (1) Group Theory (examples, morphisms, quotients, operations on groups or how to build new groups from old ones, group actions on sets, Sylow Theorems, classification of finite abelian groups, special types: solvable & nilpotent) Weeks 1-7

(2) Ring Theory (structural results, ideals, morphisms, quotients, operations on rings, Noetherian & Artinian rings, examples: PIDs, Euclidean, UFDs, Quadratic integer rings) Weeks 8-12

(3) Polynomial Rings (irreducibility criteria, symmetric polynomials, Hilbert basis Theorem, Gröbner bases) Weeks 13-15

Grading:
- Homeworks (15%) 12 in Total (due weekly), lowest score will be dropped.
- Midterm 1 (15%) Tuesday 9/17 HW 1-4
- ——— 2 (15%) Friday 10/18 HW 4-6
- ——— 3 (15%) Tuesday 11/19 HW 7-10
- Final (40%) Thursday 12/12 10-11:45 am Cumulative, including HW 11

§1.2 Definition of a group:

Definition: A group G is a set together with

- a function $G \times G \longrightarrow G$ called the group operation
  $(a, b) \longmapsto a * b$ (or multiplication)
  ↳ just notation
- an element $e \in G$ called the unit element (or identity, or neutral element)

satisfying the following properties:

(1) Associativity of the group operation:

$$(a*b)*c = a*(b*c) \qquad \text{for every } a,b,c \in G$$

↳ use symbol $\forall$

(2) e is neutral: $\quad e*a = a*e = a \quad \forall a \in G$

(3) Existence of inverses: for every $a \in G$, there exists $b \in G$ such that $a*b = e = b*a$

[In symbols: $\forall a \in G, \ \exists b \in G : \ a*b = e = b*a$]

Definition: $(G, *, e)$ is abelian or commutative if $a*b = b*a$ for all $a, b \in G$.

Notation: b = Inverse of a is written as:

$b = a^{-1}$ if $*$ is not commutative (think of $*$ as multiplication)

$b = -a$ ———— commutative (———— as addition)

§1.3 Some Examples:

Recall: We need a set G, a binary operation on G & a neutral element

EXAMPLES:

(1) $G = \mathbb{Z}$ = set of all integers $= \{\dots, -1, 0, 1, 2, \dots\}$ (abelian)

$a * b = a + b$ (usual addition) ; $e = 0$

Inverse of $a = -a$

(2) $G = \mathbb{R}_{>0}$ = set of all positive real numbers (abelian)

$a * b = ab$ (usual multiplication) ; $e = 1$

Inverse of $a = 1/a$

Note: $G = \mathbb{Q}_{>0}$ is also a group with the same operation

NON-EXAMPLES:

(1) $G = \mathbb{R}_{>0}$ with $a * b = a^b$ (binary operation)

$:= e^{b \ln(a)}$

Euler's constant, not group unit elem.

ISSUE: $a * b = a^b$ is NOT associative!

$a * (b * c) = a^{(b*c)} = a^{(b^c)}$ & these are different in general

$(a * b) * c = (a*b)^c = (a^b)^c$

Example: $a = b = 2$, $c = 3$

$a^{(b^c)} = 2^{(2^3)} = 2^8 = 256$

$\neq$

$(a^b)^c = (2^2)^3 = 4^3 = 64$

(2) $G = \mathbb{R} \cup \{-\infty\}$ $a * b = \max\{a, b\}$, $e = -\infty$

ISSUE: No inverses, except for $a = -\infty$.

EXAMPLE of a non-abelian group:

- $G = GL_2(\mathbb{R})$ = set of 2×2 matrices with real entries & non-zero determinant
- group operation: matrix multiplication
- $e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ (identity matrix)
- Inverse elements $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ab-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

Check: $A \cdot B \neq B \cdot A$ for a suitable pair $A, B \in GL_2(\mathbb{R})$

$A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

$AB = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$ $BA = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$

§ 1.4 Uniqueness properties:

Lemma 1: Neutral elements in groups are unique.

Proof: Assume e, e' are two neutral elements in a Group $(G, *)$.

Then $e \underset{\substack{\downarrow \\ e' \text{ is neutral}}}{=} e * e' \underset{\substack{\downarrow \\ e \text{ is neutral}}}{=} e'$ $\square$

Lemma 2: Inverses in groups are unique.

Proof: Pick an element x of a group $(G, *)$ & assume y, y' are both inverses of x. Then:

$$y \underset{\substack{\downarrow \\ e \text{ Neutral}}}{=} y * e \underset{\substack{\downarrow \\ y' \text{ inverse}}}{=} y * (x * y') \underset{\substack{\downarrow \\ \text{Asso}}}{=} (y * x) * y' \underset{\substack{\downarrow \\ y \text{ inverse}}}{=} e * y' \underset{\substack{\downarrow \\ e \text{ Neutral}}}{=} y'$$

$\square$

Lemma 3: If $(G, *, e)$ is a group & $x \in G$ satisfies $x * x = x$, then $x = e$.

Proof:

$$e \underset{\substack{\downarrow \\ x^{-1}\text{ inverse}}}{=} x^{-1} * x \underset{\substack{\downarrow \\ \text{hypothesis}}}{=} x^{-1} * (x * x) \underset{\substack{\downarrow \\ \text{Assoc}}}{=} (x^{-1} * x) * x = e * x \underset{\substack{\downarrow \\ e\text{ Neutral}}}{=} x$$

$\square$

§1.5 More examples:

Sometimes, groups are given as "symmetries of a structure". In these cases, associativity is automatic!

EXAMPLE 1: Symmetric groups

"Structure" = a finite set $X = \{1, 2, \ldots, n\}$ ← some positive integer

"symmetries" = bijections on X $\sigma : X \longrightarrow X$

Notation: S_n = symmetric group on n letters ($\mathfrak{S}_n$, $\mathfrak{S}_n$)

$S_n :=$ set of all bijections $X \xrightarrow{\sigma} X$

group operation = compose two maps

$$\begin{tikzcd} X \arrow[r, "\sigma"] \arrow[rr, bend right, "\tau\sigma"'] & X \arrow[r, "\tau"] & X \end{tikzcd} \qquad \tau * \sigma = \tau \circ \sigma \quad (\text{write } \tau\sigma)$$

Hence, S_n = permutations of n symbols

Ex: $|S_n|$ = number of elements of S_n

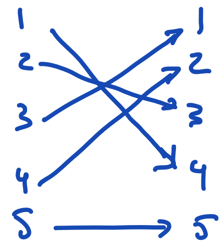
$= n!$ $(= 1 \cdot 2 \cdot 3 \cdots n)$

Ex: S_3 has 6 elements. For instance,

$\sigma(1) = 2$, $\sigma(2) = 1$, $\sigma(3) = 3$ & $\tau(1) = 3$, $\tau(2) = 1$, $\tau(3) = 2$

Various ways of writing permutations

①
$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 3 & 1 & 2 & 5 \end{array} \in S_5 \quad \rightsquigarrow$$



4 3 1 2 5 1-line notation

② cyclic notation $\sigma = (1\,4\,2\,3) \in S_4$ means

$$\begin{tikzcd} 1 \arrow[r] & 4 \arrow[r] & 2 \arrow[r] & 3 \arrow[lll, bend left] \end{tikzcd}$$

$\sigma(1) = 4$ $\quad$ $\sigma(3) = 1$

$\sigma(2) = 3$ $\quad$ $\sigma(4) = 2$

We distinguish on line notation & ③ from context.

Example (1) $\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 3 & 1 & 2 & 5 \end{array}$ is $(1\,4\,2\,3)(5)$

(2) id on S_5 is $(1)(2)(3)(4)(5)$

Remark: Usually we'll omit cycles of length 1 in the notation. If we do so, we need to remember the n.

Eg $(1\,4\,2\,3)$ in S_4 is $\begin{array}{cccc} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 3 & 1 & 2 \end{array}$

$(1\,4\,2\,3)$ in S_6 is $\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 3 & 1 & 2 & 5 & 6 \end{array}$

identity will be written as product of no cycles.