MAT3004 Abstract Algebra I - Lecture Notes

Course Information & Preliminaries

Course: Abstract Algebra I
Textbook:

- Gallian, *Contemporary Abstract Algebra*
- Artin, *Algebra*

Grading:

- Homework: 10%
- Mid-term: 35%
- Final: 55%

Topics:

- Euclidean Algorithm
- Bezout's Theorem

Theorem (Bezout's Identity): If $\gcd(m, n) = g$, then there exists $a, b \in \mathbb{Z}$ such that:

$$am + bn = g$$

Modular Arithmetic $\mathbb{Z}_n$

$$\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$$

Examples:

- $n = 12$: Months in a year
- $n = 24$: Hours in a day

Operations:

$$[a]_n + [b]_n = (\text{remainder of } (a+b) \div n)$$
$$[a]_n \cdot [b]_n = (\text{remainder of } a \cdot b \div n)$$

Example: In a specific modulus (e.g., $\mathbb{Z}_7$):

$$[4] + [6] = [3]$$

(Note: Since $4 + 6 = 10$ and $10 \equiv 3 \pmod 7$)

Introduction

Abstract algebra is a generalization of number systems.

Number Systems:

- $\mathbb{Z}$ (Integers)
- $\mathbb{Q}$ (Rational numbers)
- $\mathbb{R}$ (Real numbers)
- $\mathbb{C}$ (Complex numbers)

They all have addition $(+)$ and multiplication $(\times)$ satisfying certain properties.

Properties:

- **Associativity of Addition:** $(a+b)+c = a+(b+c)$
- **Associativity of Multiplication:** $(ab)c = a(bc)$
- **Commutativity of Addition:** $a+b = b+a$
- **Commutativity of Multiplication:** $a \cdot b = b \cdot a$
- **Distributivity:** $a \cdot (b+c) = a \cdot b + a \cdot c$

Examples of structures:

- $(\mathbb{Z}_n, +, \times)$
- $(\mathcal{M}_{2\times 2}(\mathbb{R}), +, \times)$
  (Set of 2×2 matrices with real entries)

Note: For matrices, $AB \neq BA$ in general for $A, B \in \mathcal{M}_{2\times 2}(\mathbb{R})$.

Groups

Definition: Let S be a set. A **Binary Operation** on S is a map:

$$* : S \times S \to S$$

A subset $T \subseteq S$ is **closed** under $*$ if:

$$*|_{T\times T} : T \times T \to T$$

(Meaning for all $a, b \in T$, $a * b \in T$)

Examples of Closed Sets:

1. $S = \mathbb{Z}$, $* = +$:
   - $T = 2\mathbb{Z}$ (even integers) is closed under $+$.
     Proof: $2a + 2b = 2(a+b) \in 2\mathbb{Z}$.
   - $T = 2\mathbb{Z}+1$ (odd integers) is **NOT** closed under $+$.
     (e.g., $1+1 = 2 \notin T$)

2. $S = \mathbb{Z}, * = \times$:
   - $T = n\mathbb{Z}$ is closed under $\times$.
   - $T = 2\mathbb{Z} + 1$ is also closed under $\times$.
     (Product of two odd numbers is odd)
3. $S = \mathbb{R}^n, * = +$:
   - $W \leq \mathbb{R}^n$ (Subspace) is closed under $+$.
4. $S = \mathcal{M}_{n\times n}(\mathbb{R}), * = +$:
   - Let $T = \mathrm{GL}_n(\mathbb{R})$ (all invertible matrices, i.e., $\det(A) \neq 0$).
   - T is **NOT** closed under $+$.
   - Example: $I + (-I) = 0$, and $0 \notin \mathrm{GL}_n(\mathbb{R})$.
5. $S = \mathcal{M}_{n\times n}(\mathbb{R}), * = \times$:
   - $T = \mathrm{GL}_n(\mathbb{R})$ is closed under $\times$.
   - If A, B are invertible, then (AB) is invertible with $(AB)^{-1} = B^{-1}A^{-1}$.

Definition: Group (G)

A group is a set G with a binary operation $(*)$ satisfying:

1. **Associativity:**
$$(a * b) * c = a * (b * c) \quad \text{for all } a, b, c \in G$$
2. **Identity:** There exists an element $e \in G$ such that:
$$a * e = e * a = a \quad \text{for all } a \in G$$
3. **Inverse:** For all $a \in G$, there exists $a^{-1} \in G$ such that:
$$a * a^{-1} = a^{-1} * a = e$$

Examples:

- $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ are groups $(e = 0)$.
- $(\mathbb{R}^n, +), (\mathcal{M}_{m\times n}(\mathbb{R}), +)$ are groups.
- $(\mathbb{Z}_n, +)$ is a group.

Non-Examples:

- $(\mathbb{Z}, -)$ is **not** a group.
  - Fails associativity: $(a - b) - c \neq a - (b - c)$.
  - Identity issues: If $a - e = a \implies e = 0$, but $e - a = 0 - a = -a \neq a$ (unless $a = 0$).

- $(\mathbb{Z}, \times)$ is **not** a group.
  - Associativity holds? Yes.
  - Identity? 1 works.
  - Inverse? Consider $2 \in \mathbb{Z}$. We need $2 \times 2^{-1} = 1$. But $2^{-1} = 1/2 \notin \mathbb{Z}$.
- $(\mathbb{Q}, \times)$ is **not** a group.
  - Problem: 0. $0 \times ? = 1$ is impossible.
- $(\mathbb{Z}_n, \times)$ is **not** a group (due to 0 and zero divisors).

Fixing the Multiplicative Groups:

- Let $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$, then $(\mathbb{Q}^*, \times)$ is a group.
- Similarly, $(\mathbb{R}^*, \times)$ and $(\mathbb{C}^*, \times)$ are groups.

The Multiplicative Group of Integers Modulo n

$$[0]_n \times ? = ? \times [0]_n = [0]_n \neq [1]_n$$

Question: Is $\mathbb{Z}_n \setminus \{[0]\}$ good enough?
Example ($n = 6$):

$$[2]_6 \times [a]_6 = [a]_6 \times [2]_6 = [1]_6$$

But $[2a]_6$ can only be:

$$[0], [2], [4]$$

(So $[2]_6$ has no inverse).
Definition: Let $\mathbb{Z}_n^* = \{[a]_n \mid \gcd(a, n) = 1\}$.
Examples:

- $\mathbb{Z}_6^* = \{[1]_6, [5]_6\}$
- $\mathbb{Z}_8^* = \{[1], [3], [5], [7]\}$

Claim: Then $(\mathbb{Z}_n^*, \times)$ is a group.

Proof of $(\mathbb{Z}_n^*, \times)$ being a Group

1. **Associativity:**

$$([a][b])[c] = [a]([b][c])$$

   (Since $[(ab)c] = [a(bc)]$).

2. **Identity:**

$$[a] \times [1] = [1] \times [a] = [a]$$

3. **Inverse:** Suppose $[a] \in \mathbb{Z}_n^*$ (so $\gcd(a, n) = 1$).

   By **Bezout's Theorem**:
$$pa + qn = 1$$
   for some $p, q \in \mathbb{Z}$.

   Taking modulo n:
$$[p]_n[a]_n + [q]_n[0]_n = [1]_n$$
$$\implies [p]_n[a]_n = [1]_n$$
   And (since $pa = ap$ in $\mathbb{Z}$):
$$[a][p] = [1]_n$$
   $\therefore [a]^{-1} = [p]$. ✓

More Examples:

- $(\mathcal{M}_{n\times n}(\mathbb{R}), \times)$ is **not** a group. (Identity $e = I_n$, but for any $A \in \mathcal{M}_{n\times n}(\mathbb{R})$, A^{-1} may not exist).
- $(\mathrm{GL}_n(\mathbb{R}), \times)$ is a group.

Abelian Groups & Order

Definition: Commutative Group A group $(G, *)$ is called **commutative** (or **abelian**) if:
$$a * b = b * a \quad \text{for all } a, b \in G$$

Examples:

- $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ are abelian.
- $(\mathbb{Q}^*, \times), (\mathbb{R}^*, \times), (\mathbb{C}^*, \times), (\mathbb{Z}_n^*, \times)$ are abelian.
- $(\mathrm{GL}_n(\mathbb{R}), \times)$ is **<u>NOT</u> abelian**.

Definition: Order of a Group The **<u>order</u>** of a group $(G, \times)$ is:
$$|G| = \# \text{ of elements in } G$$

Examples:

- $|(\mathbb{Z}_n, +)| = n$
- $|(\mathbb{Z}, +)| = |(\mathbb{Q}, +)| = \cdots = \infty$
- $|(\mathbb{Z}_n^*, \times)| = \#\{0 \le a < n \mid \gcd(a, n) = 1\} = \phi(n)$

(Gauss' totient function)