MATH2022

Usyd Mingyuan Ba

March 13, 2024

1 Week1

1.1 Arithmetics

- Addition
  Operations Used: $+, \times$
  Limits: $-, /$
- Integers
  Operations Used: $+, \times, -$
  Limits: $/$
- The Rational Numbers
  $\mathbb{Q} = \{\frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0\}$
  Operations Used: $+, -, \times, /$
  Limits:
- The Real Numbers
  Operations Used: $+, -, \times, /$
  Limits: $i = \sqrt{-1}$
- The Complex Number
  $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R} where i = \sqrt{-1}\}$ Operations Used: $+, -, \times, /$
  Limits:
- Modular Arithmetic
  Let $n \in \mathbb{Z}^*$ and let Z_n be the set of remainders after dividing by n.
  So $Z_n = \{0, 1, 2, 3...n - 1\}$

1.2 Fields

A **field** $(F, +, \cdot)$ is a set F equipped with two operations: addition $(+)$ and multiplication $(\cdot)$, satisfying the following axioms:

1. *Closure under Addition and Multiplication*

$$\forall a, b \in F, \quad a + b \in F$$
$$\forall a, b \in F, \quad a \cdot b \in F$$

2. *Associativity of Addition and Multiplication*

$$\forall a, b, c \in F, \quad (a + b) + c = a + (b + c)$$
$$\forall a, b, c \in F, \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$$

3. *Commutativity of Addition and Multiplication*

$$\forall a, b \in F, \quad a + b = b + a$$
$$\forall a, b \in F, \quad a \cdot b = b \cdot a$$

4. *Identity Elements*

$$\exists 0 \in F \text{ such that } \forall a \in F, \quad a + 0 = a$$
$$\exists 1 \in F \text{ with } 1 \neq 0, \text{ such that } \forall a \in F, \quad a \cdot 1 = a$$

5. *Additive and Multiplicative Inverses*

$$\forall a \in F, \quad \exists -a \in F \text{ such that } a + (-a) = 0$$
$$\forall a \in F \text{ with } a \neq 0, \quad \exists a^{-1} \in F \text{ such that } a \cdot a^{-1} = 1$$

6. *Distributivity of Multiplication over Addition*

$$\forall a, b, c \in F, \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

1.3 Group Definition

A **group** $(G, *)$ is a set G together with a binary operation $*$ that combines any two elements a and b to form another element $a * b$. The binary operation satisfies the following four properties:

1. *Closure*: For every $a, b \in G$, the result of the operation $a * b$ is also in G.

$$\forall a, b \in G, \quad a * b \in G$$

2. *Associativity*: For every $a, b, andc \in G$, the equation $(a * b) * c = a * (b * c)$ holds.

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

3. *Identity Element*: There exists an element $e \in G$, called the identity element, such that for every element $a \in G$, the equation $e * a = a * e = a$ holds.

$$\exists e \in G \text{ such that } \forall a \in G, \quad e * a = a * e = a$$

4. *Inverse Element*: For each $a \in G$, there exists an element $b \in G$ such that $a * b = b * a = e$, where e is the identity element.

$$\forall a \in G, \quad \exists b \in G \text{ such that } a * b = b * a = e$$

A group is called **abelian** (or **commutative**) if, in addition, the binary operation is commutative, that is, $a * b = b * a$ for all $a, b \in G$.

Notes:

1. As in the case of fields, the identity element and the inverse can be shown to be unique.
2. Our notation might imply that this operation is multiplication, but it could just as easily be addition or another operation.

1.4 Cyclic Groups

A **cyclic group** G is a special type of group that can be entirely generated by a single element $g \in G$. This element g is called a generator of the group. The main characteristic that distinguishes cyclic groups from general groups is the ability to generate all elements of the group by repeatedly applying the group operation to the generator.

1. *Generator*

$$\exists g \in G \,\text{such that}\, G = \{g^n | n \in \mathbb{Z}\} \,\text{(for multiplicative groups)}$$
$$\text{or} \quad G = \{ng | n \in \mathbb{Z}\} \,\text{(for additive groups)}$$

2. *Uniqueness*

Every element of G can be uniquely expressed as g^n for some $n \in \mathbb{Z}$.

The cyclic nature of G implies that it possesses a structure that can be systematically described by the powers (or multiples) of a single element, making cyclic groups particularly simple to understand and work with.

1.5 Symmetric Groups

A **symmetric group** S_n on a set of n symbols is the group consisting of all possible permutations of these symbols, with group operation being the composition of these permutations. The symmetric group on n symbols is denoted as S_n and plays a crucial role in various areas of mathematics due to its fundamental nature in the study of permutations.

1. **Recap**
   definitions: A bijection is a mapping that is injective (one to one) and surjective (onto).

   Important Convention
   We write the action of $f : X \to Y$ on the right:

   $$x \mapsto xf \ (\forall x \in X)$$

   and we compose from left to right:

   $$fg : X \to Z \text{ (where } f : X \to Y,\ g : Y \to Z)$$

   Instead of using $f \circ g(x) = f(g(x))$, we use $x(fg) := (xf)g$
   We apply f on x first, then g

2. Proof that: *The composite of two bijection is also a bijection*
   Let $f : X \to Y, g : Y \to Z$

   - Injective: Need to show that if $x(fg) = y(fg)$ then $x = y$
     Suppose $x(fg) = y(fg)$.Then $(xf)g = (yf)g$ by definition,So $xf = yf$ since g is injective,samething agagin, x = y.

   - Surjective: Need to show that the range of $x(fg)$ equals to Z

3. **Permutations**

   - For a finite set of size n, there are n! permutations (write $|X| = n$), The set of permutations of X is denoted $Sym(X)$ or S_x,So,$|Sym(X)| = n!$

4. THEOREM:
   The set of permutations on a set X, Sym(X), is a group under composition of permutations. We call it the Symmetric Group on X:

   - **closure** The composite of two bijections is also a bijection.
   - **associative** Composition of bijections is associative.
   - **Identity element** The identity map is a bijection.
   - **Inverse element** The inverse of a bijection is a bijection

2 Week2

Week 3

Matrix Recap

- **Elementary Matrices and Invertibility**
- **Determinants, Properties**

Odd and Even Permutations

- **Transposition**
  Definition: A transposition is a permutation $\phi : \mathbb{X} \to \mathbb{X}$, which interchanges two distinct elements $a, b \in \mathbb{X}$ leaving all other elements unchanged. Thus,

  $$\phi = (ab).$$

  Fact: All cycles are a product (composition) of transpositions.

  $$(a_1, a_2, a_3, \ldots, a_n) = (a_1a_2)(a_1a_3)\ldots(a_1a_n).$$

  Corollary: Every permutation of a finite set is a product (composition) of transpositions.

- **Even/Odd**
  Definition: We call a permutation even (or odd) if it is a product of an even (or odd, respectively) number of transpositions.
  - $(123) = (12)(13)$ is even.
  - $(1234) = (12)(13)(14)$ is odd.
  - $(1) = (12)(12) = (13)(13)$ is even.

  Properties:
  - Single transpositions are self-inverse: $(ab)(ab) = 1$.
  - A permutation and its inverse have the same parity.

- **Permutation Matrix**
  Definition: A permutation matrix is the result of applying a permutation to the rows of the identity matrix.

  $$\phi = (132) = (13)(12) = R_1 \leftrightarrow R_3, R_1 \leftrightarrow R_2.$$

  Hence, $\mathrm{Det}(M) = \mathrm{Det}(E_1E_2) = \mathrm{Det}(E_1)\mathrm{Det}(E_2) = (-1)^2 = 1$.

The Alternating Subgroup, Alt(n), of Sym(n)

- **Subgroup**
  Definition: A subgroup, H, of a group, G, is a subset of G which is also a group under the same operation. We write $H \leq G$ or $H < G$ if H is a proper subset of G.

  Proof a subgroup:

  - It is non-empty
  - It is closed under the operation.
    Associativity: Inherited from G
    Identity: $\exists a \in G, a^k = e$
    Inverse: $a^k = e \rightarrow aa^{k-1} = e = a^{k-1}a$

- **Alternating Group**
  Definition: The alternating group (on n letters) is the set of even permutations in $Sym(n)$. That is, $Alt(n) = \{\text{even permutations of } \{1, 2, \ldots, n\}\}$.