

MATH2022

Usyd Mingyuan Ba

March 14, 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
 $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R} \text{ where } i = \sqrt{-1}\}$ 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 $Z_n = \{0, 1, 2, 3 \dots n - 1\}$

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*

$$\begin{aligned}\forall a, b, c \in F, \quad (a + b) + c &= a + (b + c) \\ \forall a, b, c \in F, \quad (a \cdot b) \cdot c &= a \cdot (b \cdot c)\end{aligned}$$

3. *Commutativity of Addition and Multiplication*

$$\begin{aligned}\forall a, b \in F, \quad a + b &= b + a \\ \forall a, b \in F, \quad a \cdot b &= b \cdot a\end{aligned}$$

4. *Identity Elements*

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

5. *Additive and Multiplicative Inverses*

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

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 $a, b, \text{ and } c \in G$, 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*

$$\begin{aligned} \exists g \in G \text{ such that } G &= \{g^n \mid n \in \mathbb{Z}\} \text{ (for multiplicative groups)} \\ \text{or } G &= \{ng \mid n \in \mathbb{Z}\} \text{ (for additive groups)} \end{aligned}$$

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 $f : X \rightarrow Y$ on the right:

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

and we compose from left to right:

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

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 $f : X \rightarrow Y, g : Y \rightarrow Z$

- **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, something again, $x = y$.
- **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 $\phi : \mathbb{X} \rightarrow \mathbb{X}$, 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.

$$(a_1, a_2, a_3, \dots, a_n) = (a_1 a_2)(a_1 a_3) \dots (a_1 a_n).$$

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

The Alternating Subgroup, $\text{Alt}(n)$, of $\text{Sym}(n)$

- **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 $\text{Sym}(n)$. That is, $\text{Alt}(n) = \{\text{even permutations of } \{1, 2, \dots, n\}\}$.

$$\begin{aligned}
 \text{Sym}(2) &= \{1, (12)\} & A_2 &= \{1\} \\
 \text{Sym}(3) &= \{1, (12), (13), (23), (123), (132)\} \\
 A_3 &= \{1, (123), (132)\} \\
 \text{Sym}(4) &= \{1, (12), (13), (14), (23), (24), (34), (123), (132), \\
 &\quad (124), (142), (134), (143), (234), (243), \\
 &\quad (1234), (1243), (1324), (1342), (1423), \\
 &\quad (1432), (12)(34), (13)(24), (23)(14)\}
 \end{aligned}$$

Week4

1. Elementary matrices: An $n \times n$ matrix is called elementary if it is the result of applying a single elementary row operation to the identity matrix I_n .
2. Effect of multiplication by an elementary matrix: If E is the elementary matrix obtained by applying the elementary row operation ρ to I_n , and A is any matrix with n rows, then the matrix product EA is the matrix obtained by applying ρ to A .
3. Invertibility criterion and algorithm: A square matrix A is invertible if and only if A is a product of elementary matrices, which occurs if and only if the augmented matrix $[A \mid I]$ can be row reduced to $[I \mid B]$, in which case $A^{-1} = B$.
4. Half of the definition of invertibility suffices for square matrices: If A is a square matrix and $AB = I$ or $BA = I$ then $AB = BA = I$, in which case the inverse A^{-1} exists and equals B .

5. Determinants of matrices of dimensions 1,2 and 3: The determinant of a 1×1 matrix $[a]$ is simply the entry a . The determinant of a 2×2 matrix

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ is } \det A = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc. \text{ The determinant of a } 3 \times 3 \text{ matrix } A = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & k \end{bmatrix} \text{ is}$$

$$\det A = |A| = a \begin{vmatrix} e & f \\ h & k \end{vmatrix} - b \begin{vmatrix} d & f \\ g & k \end{vmatrix} + c \begin{vmatrix} d & e \\ g & h \end{vmatrix}$$

called the expansion along the first row, where the smaller determinant arises by ignoring the row and column of the entry being used as a coefficient.

6. Determinants in general: Following the pattern for 3×3 matrices, we may expand along any row or down any column of a given square matrix A of any size, producing the same number, called the determinant of A , denoted by $\det A$ or $|A|$, provided one uses adjustment factors given by the checkerboard patterns

$$\begin{bmatrix} + & - & + \\ - & + & - \\ + & - & + \end{bmatrix}, \quad \begin{bmatrix} + & - & + & - \\ - & + & - & + \\ + & - & + & - \\ - & + & - & + \end{bmatrix}$$

and so on to higher dimensions.

7. Multiplicative property of determinants: If A and B are square matrices of the same size then $\det(AB) = (\det A)(\det B)$.

8. Invertibility criterion using determinants: A square matrix is invertible if and only if its determinant is nonzero.
9. Effects of elementary row and columns operations on determinants: Let A be a square matrix. If B is obtained from A by swapping two rows or swapping two columns then

$$\det B = -\det A.$$

If B is obtained from A by multiplying a row or column by a scalar λ then

$$\det B = \lambda \det A.$$

If B is obtained from A by adding a multiple of one row [column] to another row [column] then

$$\det B = \det A.$$

10. Determinant of the transpose: If A is a square matrix then $\det(A^T) = \det A$.
11. Transpositions: A permutation that interchanges two letters and fixes all other letters is called a transposition.
12. **Even and odd permutations:** A permutation of a finite set is called even if it is a product of an even number of transpositions (and by default the identity permutation is even), and called odd if it is a product of an odd number of transpositions.
13. **No permutation can be both even and odd:** If n is a positive integer then the symmetric group S_n is the disjoint union of A_n , the subset of even permutations (and called the alternating group), and $S_n \setminus A_n$, the complement of A_n , which comprises exactly the subset of all odd permutations.

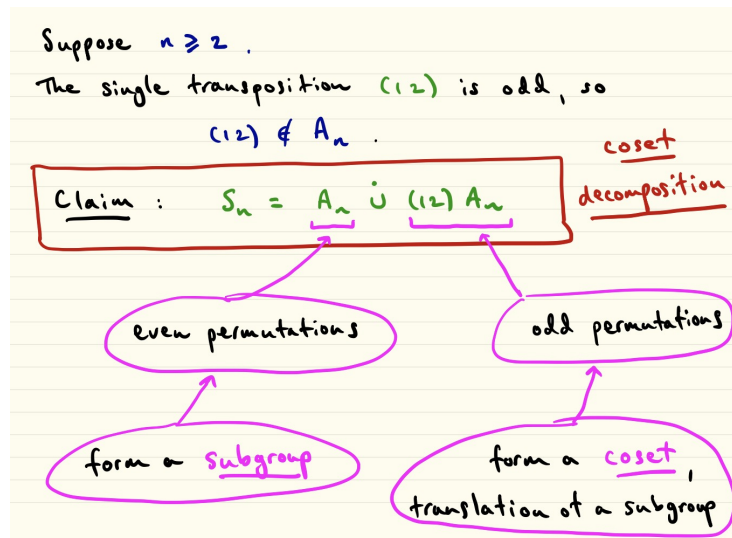
14. **Cosets:** For a Symmetric Group $S_n, n \geq 2$,

- **Symmetric Group and Cosets:** The symmetric group, denoted as S_n , represents the group of all permutations of n elements. Within this group, a *coset* is a form of subset created by multiplying a group element by every element within a subgroup. Specifically, for a subgroup H in a group G , and any element $g \in G$, we define:

- A *left coset* of H in G with respect to g as $gH = \{gh : h \in H\}$.
- A *right coset* of H in G with respect to g as $Hg = \{hg : h \in H\}$.

Important properties of cosets include:

- Cosets of a subgroup partition the group.
- All left (or right) cosets of a subgroup have the same cardinality as the subgroup itself.



15. Conjugates of permutations: If α and β are any permutations of a given set then the conjugate of α by β is the permutation $\beta^{-1}\alpha\beta$, denoted by α^β , using exponential notation. We denote by $\alpha^{-\beta}$ the inverse of α^β , so that $\alpha^{-\beta} = \beta^{-1}\alpha^{-1}\beta$, the conjugate of α^{-1} by β (not to be confused with $\beta\alpha\beta^{-1}$, which is $\alpha^{\beta^{-1}}$, the conjugate of α by β^{-1}).

16. **Properties on Conjugation:** Let $(S, *)$ be a set with an associative binary operation, $*$, and an identity element, e .

- *multiplicative* $(ab)^c = a^c b^c$

$$(ab)^c = c^{-1}(ab)c = (c^{-1}ac)(c^{-1}bc) = a^c b^c$$

- $(a^b)^{-1} = (a^{-1})^b$

Note that: $a^{b^{-1}}$ is the conjugate of a by b^{-1}

17. Effect of conjugation on the cycle decomposition of a permutation: If α and β are permutations and $(a_1 \ a_2 \ \dots \ a_k)$ is a cycle in the cycle decomposition of α then $(a_1\beta a_2\beta \dots a_k\beta)$ is a cycle in the cycle decomposition of the conjugate α^β .

18. **More on Conjugation:**

Suppose $\alpha, \beta \in \text{Sym}(n)$, we want to write decomposition of α^β from the cycle decomposition of α .

- **Lemma:** If $(a_1, a_2, a_3, \dots, a_k)$ is cycle in α , then $(a_1\beta a_2\beta a_3\beta \dots a_k\beta)$ is a cycle in α^β . ($a_k\beta$ means $\beta(a_k)$)

Proof

Suppose $i \in \{1, 2, 3, \dots, k-1\}$, Then

$$(a_i\beta) \rightarrow (a_i\beta)(\beta^{-1}a\beta) = a_i\beta\beta^{-1}a\beta = a_i a\beta = a_{i+1}\beta$$

Similarly

$$(a_k\beta) \rightarrow (a_k\beta)(\beta^{-1}a\beta) = a_k\beta\beta^{-1}a\beta = a_k a\beta = a_1\beta$$

\rightarrow stands for "maps to".

This proof only shows that the conjugate of a cycle is in (one of) α^β .

But in fact:

$$(a_1 a_2 a_3 \dots a_k)^\beta = (a_1 \beta a_1 \beta \dots a_k \beta) (*)$$

Which means the conjugate of a cycle a_i is exactly a $a_i\beta$.

- **Corollary:** To find α^β , just replace every a_i , in each cycle with $a_i\beta$

Proof: If $\alpha = a_1 a_2 a_3 \dots a_k$ for cycles a_i , the conjugate

$$\begin{aligned} \alpha^\beta &= a_1^\beta a_2^\beta a_3^\beta \dots a_k^\beta \text{ --- multiplicativity} \\ &= (a_1 \beta a_1 \beta \dots a_k \beta) \text{ --- see } * \text{ above} \end{aligned}$$