



# 近世代数

计算机科学与技术学院

唐琳琳



# 说明

- 作业:

8次课, 4次作业; 每周一上课前提交上周作业。

- 助教: 成炜钰、程祥祥、李敏臻、唐克、余赵昊、韩兆星

- 作业邮箱: mathhomework2025@163.com

- 成绩:

平时作业30%, 期末考试70%。

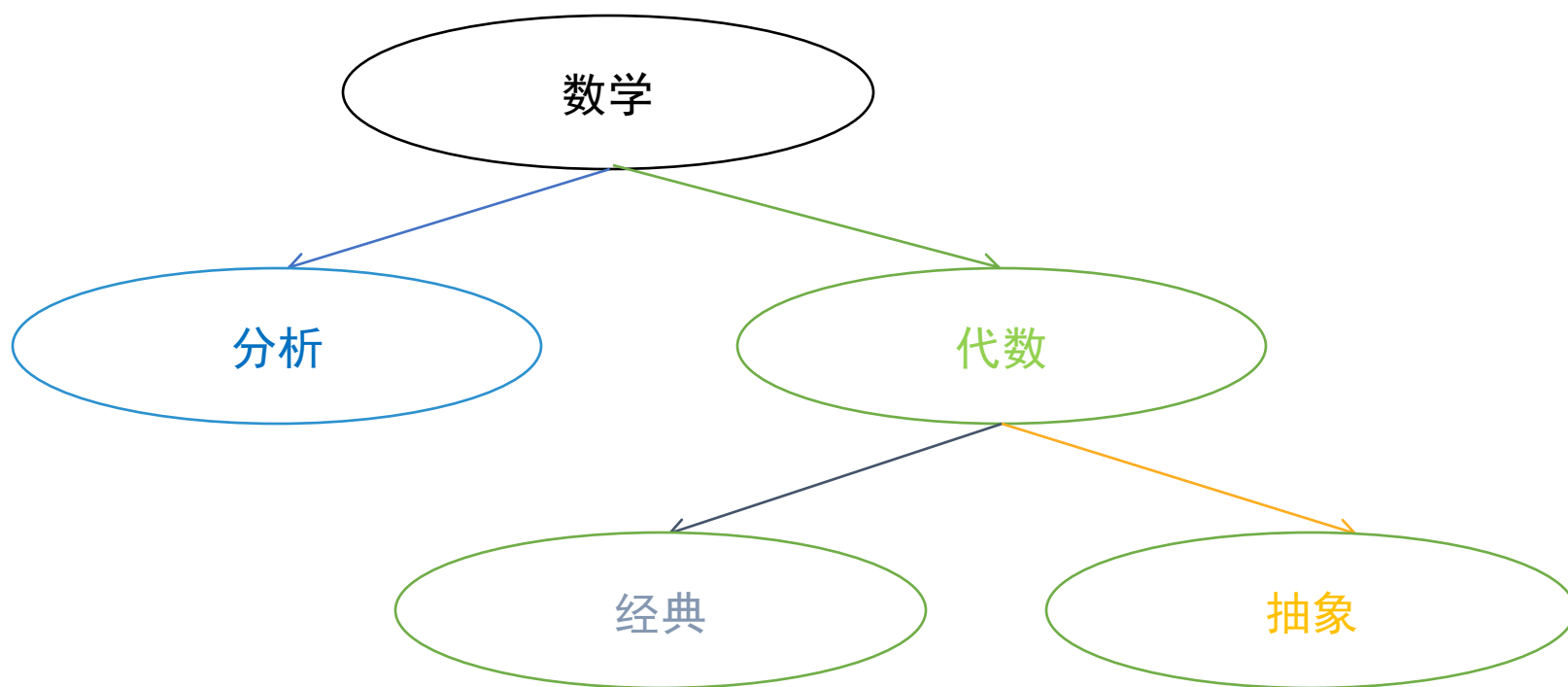
- 2025夏《近世代数》QQ群: 2155013308



扫一扫二维码, 加入群聊

# 第一章 基本概念

- 数学 --- 分析 & 代数
- 代数---经典代数（初等代数、高等代数、线性代数等）  
& 近世代数
- 近世代数---抽象代数



# 第一章 基本概念

- 应用领域:
- 计算机相关科学, 信息技术领域, 现代物理、化学, 现代生物学等
- 1. 人工智能: 图神经网络 (GNN)
- 2. 密码学: 公开密钥算法 (RSA), 同态加密算法
- 3. 5G: RS, OFDM, AKA
- 4. 量子计算: 量子门设计 (Pauli群生成量子电路)、量子纠错 (稳定子码)、量子计算 (对称群与傅里叶分析)
- 5. 现代物理、化学: 晶体结构分类 (230种空间群)、粒子物理 (标准模型的 $SU(3) \times SU(2) \times U(1)$ 规范群)
- 6. 现代生物学: 自由群与同调、DNA序列折叠对称性分析

# 内容:

- 1. 集合
- 2. 映射 & 变换
- 3. 代数运算
- 4. 运算律
- 5. 同态与同构
- 6. 等价关系与集合分类

# 集合

- 定义 —— 是什么（概念） —— 如何表示
- 性质 —— 怎么样（特点）
- 运算 —— 如何处理（原则性过程）
- 定理 —— 有什么规律（规律总结）

## 要点:

定义---注意集合的表示方法（列举、描述、文氏图）

性质---确定性、互异性、无序性

运算---幂等、交换、结合、分配

定理---摩根定律

# 集合

- 定义

- $A, B, C, \dots, G, R, F \dots \setminus a, b, c, \dots, x, y, \dots$

- $x \in A \text{ or } A \ni x ; x \notin A \text{ or } A \not\ni x$

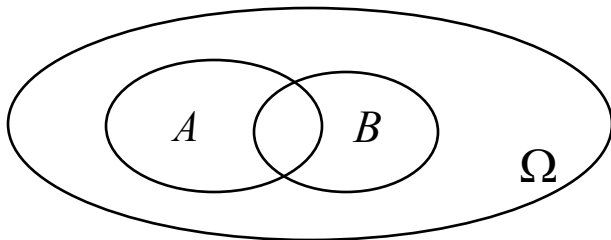
- 例子:

- $\mathbb{Z}, \mathbb{Z}^*, \mathbb{Q}, \mathbb{Q}^*$

- 表示方法:

- $A = \{1, 3, 5\}, B = \{\text{东}, \text{西}\}, C = \left\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots\right\}$

- $E = \{\text{全体自然数}\}, F = \{x \mid x \text{ 是实数且 } x^2 < 1\}$



## • 集合与集合之间的关系&集合运算

➤ 子  $A \subseteq B$   $A \subset B$   $A \not\subseteq B$   $A \not\subset B$

$$A=B \Leftrightarrow A \subseteq B \& B \subseteq A \quad P(A) \quad |A|$$

➤ 交  $A \cap B$   $A=\{0,1,2,3\}$   $B=\{0,2,4\}$   $C=\{4,5,6\}$

$$A \cap B = \{0,2\} \quad A \cap C = \emptyset$$

➤ 并  $A \cup B$   $A=\{0,1,2,3\}$   $B=\{0,1,-2,-3\}$

$$A \cup B = \{-3, -2, 0, 1, 2, 3\}$$

➤ 补  $A - B = \{a | a \in A, a \notin B\}$   $X \subseteq Y, X' = Y - X = \{a | a \in Y, a \notin X\}$

$$\bar{X}$$



下列描述正确的是 ()

- ☐ A  $A \subseteq B \Rightarrow A \subset B$
- ☒ B  $A \not\subseteq B \Rightarrow A \not\subset B$
- ☐ C  $A \not\subset B \Rightarrow A \not\subseteq B$
- ☐ D  $\emptyset$  是任何集合的真子集

提交

# 集合

## • 运算性质

➤  $A \cap A = A$        $A \cup A = A$       幂等性

➤  $A \cap B = B \cap A$        $A \cup B = B \cup A$       交换律

➤  $(A \cap B) \cap C = A \cap (B \cap C)$        $A \cup (B \cup C) = (A \cup B) \cup C$       结合律

➤  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$        $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$       分配律

## 摩根定律

$$A, B \subseteq X \quad \Rightarrow \quad (A \cup B)' = A' \cap B' \quad (A \cap B)' = A' \cup B'$$

- 练习:

- 1. 证明分配律

- 2.  $A \cap B = A \cap C \Rightarrow ? \quad B = C \quad "U"?$

- 3.  $|A| = n \Rightarrow |P(A)| = 2^n$

- 4. 证明摩根定律

# 映射与变换

- 定义

- 集合  $A, B$ ,  $\forall x \in A \quad \exists$  唯一的  $y \in B$

$$\varphi: x \rightarrow y \quad \text{or} \quad \varphi(x) = y$$

- 例题

➤ 1.  $A=Q, B=R \quad \varphi: x \rightarrow \frac{1}{x-1} \quad \text{mapping?}$

➤ 2.  $A=Q, B=Q \quad \varphi: \frac{a}{b} \rightarrow a+b \quad \text{mapping?}$

➤ 3.  $A=\{1,2,3\}, B=\{2,4,8,16\} \quad \varphi: x \rightarrow 2x \quad \text{mapping?}$

➤ 4.  $A=\{1,2,3\}, B=\{0,4,9,10\} \quad \varphi: 1 \rightarrow 0, 2 \rightarrow 0, 3 \rightarrow 9$

➤ 5.  $A=\{1,2,3,\dots\}, B=Q \quad \varphi: x \rightarrow x^2$

➤ 6.  $A=\{\text{all } n\text{-vectors on } F\}, B=F \quad \varphi: (a_1, a_2, \dots, a_n) \rightarrow a_1 \quad (a_i \in F)$

# 映射与变换

## • 映射类别

### ➤ 满射

$$\varphi: A \rightarrow B, \quad \forall y \in B, \exists x \in A, \quad st. \quad \varphi(x) = y$$

“满”

c

$$\varphi(A) = B$$

### ➤ 单射

$$\varphi: A \rightarrow B, \quad \forall x_1, x_2 \in A, x_1 \neq x_2 \Rightarrow \varphi(x_1) \neq \varphi(x_2)$$

“单”

### ➤ 双射

$$\varphi: X \rightarrow Y$$

“满”&“单” “双”

A为数域F上的n阶方阵集合,  $B=\{0,1,\dots,n\}$ , 则  
法则  $\varphi: A \rightarrow r(A)$  是A到B的一个

☒ A 满射

☐ B 双射

☐ C 单射

☒ D 映射

提交

# 映射与变换

- 满射充分必要条件

设  $\varphi$  为集合  $A$  到集合  $B$  的一个映射,  $A_1 \subseteq A, B_1 \subseteq B$ 。则:

$$\varphi(A_1) \subseteq B, \quad \varphi^{-1}(B_1) \subseteq A$$

分别称他们为  $A_1$  在  $\varphi$  下的像;  $B_1$  在  $\varphi$  之下的逆像。

$A$ 到 $B$ 的映射  $\varphi$  是满射的充分必要条件是 



对“充分必要条件” “ $\Leftrightarrow$ ” 理解正确的是（例如A成立的充分必要条件是B成立 或者说 A成立当且仅当B成立）

- ☐ A 从A推向B是在证A成立的充分性
- ☒ B 从B推向A是在证A成立的充分性
- ☐ C 从A推向B是在证B成立的必要性
- ☒ D 从B推向A是在证B成立的必要性

提交



- 逆映射

设  $\varphi$  是从集合  $A$  到集合  $B$  的一个双射, 且  $\varphi(x) = y (x \in A, y \in B)$ , 则显然法则

$$\varphi^{-1}: y \rightarrow x, \text{ 即 } \varphi^{-1}(y) = x$$

便是集合  $B$  到集合  $A$  的一个双射。称  $\varphi^{-1}$  为  $\varphi$  的逆映射。

特别的有:

$$(\varphi^{-1})^{-1} = \varphi$$

# 映射与变换

- 两有限集 $A, B$ 之间可以建立双射的充分必要条件：

$$|A| = |B|$$

$\Rightarrow$  若  $\varphi$  为 $A$ 与 $B$ 两有限集之间的双射，则：

$$|\varphi(A)| = |A|, \quad \varphi(A) = B$$

于是得：  $|A| = |\varphi(A)| = |B|$

$\Leftarrow$  若  $|A| = |B|$  ，则不难构造出一个一一映射，此映射即为 $A$ 与 $B$ 之间的双射。

# 映射与变换

## • 定理 1

$$|A|=|B|<\infty, \quad \varphi \text{ 是满射} \Leftrightarrow \varphi \text{ 是单射}$$

设  $|A|=|B|=n$

$$A=\{x_1, x_2, \dots, x_n\} \quad B=\{y_1, y_2, \dots, y_n\}$$

$$\varphi: \quad x_i \rightarrow y_{k_i} \quad (i=1, \dots, n, 1 \leq k_i \leq n)$$

目标:

$$\varphi(A)=B \Rightarrow x_i \neq x_j, y_{k_i} \neq y_{k_j}$$

c

*surjective*

c

$$\varphi(A)=B \Leftarrow x_i \neq x_j, y_{k_i} \neq y_{k_j}$$

# 映射与变换

- 两个映射相等的概念

设  $\varphi$  ,  $\tau$  是集合  $A$  到集合  $B$  的两个映射,

若  $\forall x \in A$  , 都有

$$\varphi(x) = \tau(x)$$

则:

$$\varphi = \tau$$

# 映射与变换

- 定义

集合 $A$ 到其自身的映射，叫做集合 $A$ 的一个变换。

➤ 满射 “满射变换”

➤ 单射 “单射变换”

➤ 双射 --- 一一映射 “双射变换” or “一一变换”

➤ identity transform  $I(x) = x$  “恒等变换”

# 映射与变换

- 例题:

➤1.  $X = \{1, 2, 3, \dots\}$       $\varphi: x \rightarrow x^2$      单射变换

➤2.  $X = \{1, 2, 3, \dots\}$       $\varphi: 1 \rightarrow 2, 2 \rightarrow 1, n \rightarrow n \ (n = 3, 4, \dots)$

双射变换

➤3. ...

- 定理

➤ 任意 $n$ 元有限集共有 $n!$ 个双射变换。

设  $M = \{1, 2, \dots, n\}$ , 则  $\varphi \rightarrow \varphi(1)\varphi(2)\dots\varphi(n)$

一个双射变换  $\iff$  全排列

$$\varphi = \begin{pmatrix} 1 & 2 & \dots & n \\ \varphi(1) & \varphi(2) & \dots & \varphi(n) \end{pmatrix}$$

“一个 $n$ 元/阶置换” or “一个 $n$ 次置换”

# 映射与变换

- 例题：

$$M = \{1, 2, 3\}$$

$$\varphi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \varphi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \varphi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$\varphi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \varphi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \varphi_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

$$\begin{aligned} \varphi_4 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 3 \\ 3 & 2 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 3 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 2 & 1 \\ 1 & 3 & 2 \end{pmatrix} \end{aligned}$$



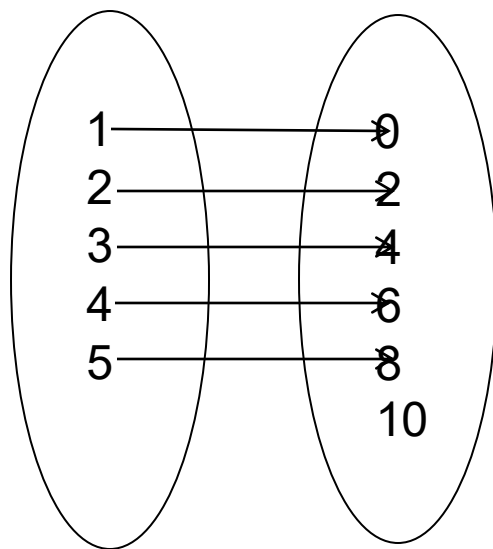
# 映射与变换

## • 练习

➤ 1.  $A = \{1, 2, 3, 4, 5\}$ ,  $B = \{0, 2, 4, 6, 8, 10\}$ , 以下两个是否是A到B的单射？

$$\varphi_1: x \rightarrow 2x$$

$$\varphi_2: 1 \rightarrow 0, \quad 2 \rightarrow 2, \quad 3 \rightarrow 4, \quad 4 \rightarrow 6, \quad 5 \rightarrow 8$$



# 映射与变换

## • 练习

➤2.  $X = \{A_{n \times n} \mid a_{ij} \in F, 1 \leq i, j \leq n\}$   $F$ 为一数域, 判断以下从 $X$ 到 $F$ 的法则

$$\varphi: A \rightarrow |A|$$

映射?

满射?

单射?

➤3.  $\varphi_5(\varphi_3(\varphi_1(1))) = ?$

$$\varphi_6(\varphi_4(\varphi_2(2))) = ?$$

# 作业

- P5: 1、 3
- P11: 5