近世代数

计算机科学与技术学院
唐琳琳

说明

- 作业：

16次课，8次作业；每周一上课前提交上周作业。

- 助教&邮箱：何谦、杨济嘉、刘思含、黄高祥 HQ20S058004@163.com

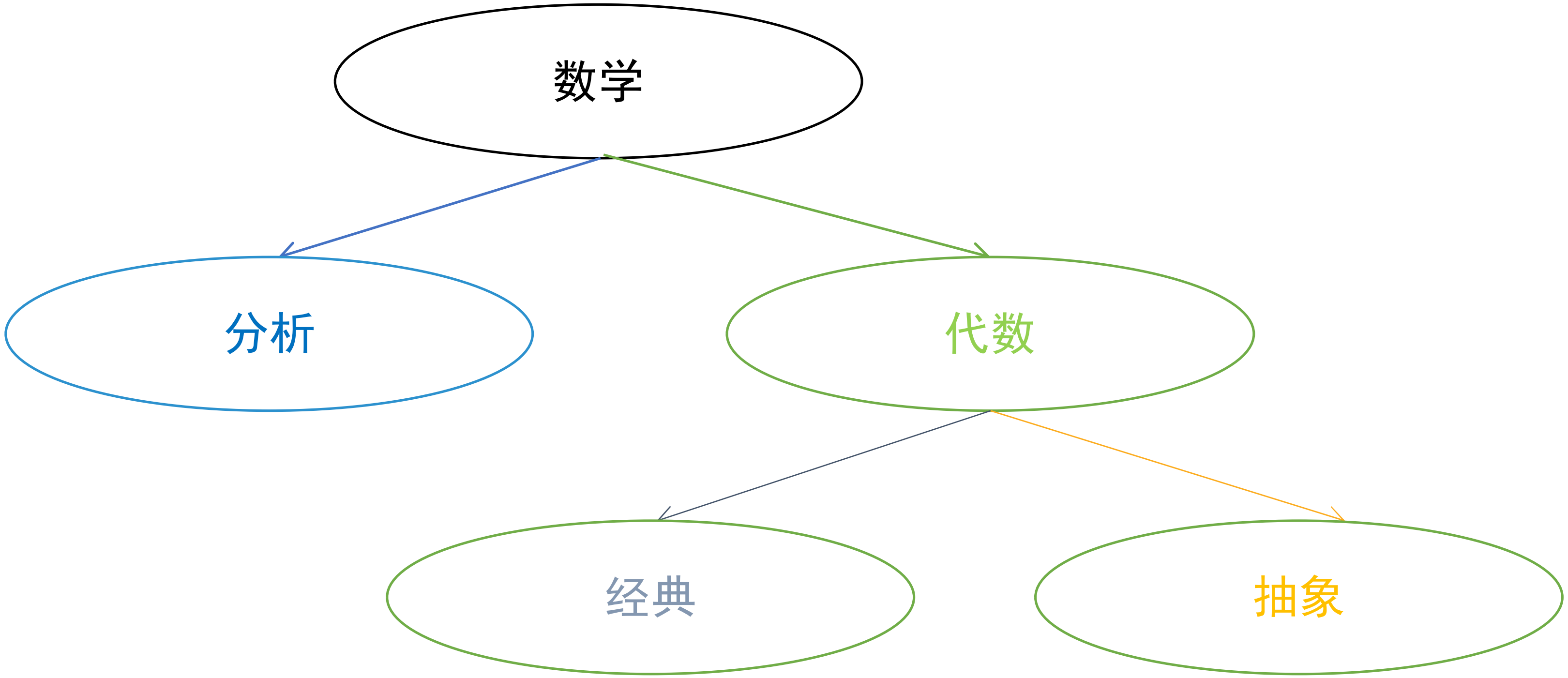
- 成绩：

平时作业40%，期末考试60%。

●2021《近世代数》QQ群：

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, 现代化学等

➢1. 密码学：公开密钥算法（RSA），同态加密算法
➢2. 编码：分组编码, 纠错编码
➢3. 现代物理
➢4. 现代化学

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, ..., G, R, F...\\ a, b, c, ..., x, y, ...

➢$x \in A$ or $A \ni x$; $x \notin A$ or $A \not\ni x$

- 例子:

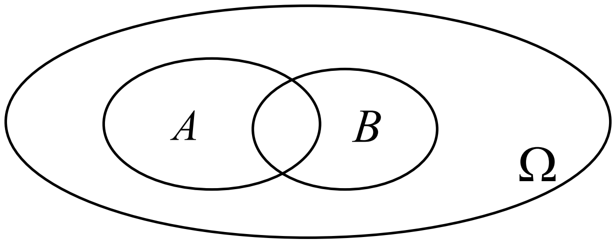
➢Z , Z^* , Q , Q^*

- 表示方法:

➢ $A=\{1,3,5\}$, $B=\{东, 西\}$, $C=\left\{1,\frac{1}{2},\frac{1}{3},\frac{1}{4},\ldots\right\}$

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

➢



集合

- 集合与集合之间的关系&集合运算

➢ 子 $A \subseteq B$ $A \subset B$ $A \nsubseteq B$ $A \not\subset B$

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

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

$$A \cap B = \{0,2\} \qquad A \cap C = \phi$$

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

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

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

$$\overline{X}$$

单选题 1分

设置

下列描述正确的是（）

A $A \subseteq B \Rightarrow A \subset B$

B $A \nsubseteq B \Rightarrow A \not\subset B$

C $A \not\subset B \Rightarrow A \nsubseteq B$

D ϕ 是任何集合的真子集

提交

集合

- 运算性质

➢ $A \cap A = A$ $\quad A \cup A = A$ 幂等性

➢ $A \cap B = B \cap A$ $\quad A \cup B = B \cup A$ 交换律

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

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

摩根定律

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

集合

- 练习:

➢1. 证明分配律

➢2. $A \cap B = A \cap C \Rightarrow ?\ B = C$ $"\cup"?$

➢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， $\forall x \in A$ $\exists$唯一的 $y \in B$

$$\varphi\colon \quad x \to y \quad or \quad \varphi(x) = y$$

- 例题

➢1. A=Q, B=R $\varphi\colon$ $x \to \dfrac{1}{x-1}$ *mapping* ?

➢2. A=Q, B=Q $\varphi\colon$ $\dfrac{a}{b} \to a+b$ *mapping*?

➢3. A=$\{1,2,3\}$， B=$\{2,4,8,16\}$ $\varphi\colon$ $x \to 2x$ *mapping*?

➢4. A=$\{1,2,3\}$， B=$\{0,4,9,10\}$ $\varphi\colon$ $1 \to 0$， $2 \to 0$， $3 \to 9$

➢5. $A = \{1,2,3,\ldots\}, B = Q$ $\varphi\colon$ $x \to x^2$

➢6. $A = \{all \quad n-vectors \quad on \quad F\}, B=F$ $\varphi\colon$ $(a_1, a_2, \ldots, a_n) \to a_1 \quad (a_i \in F)$

映射与变换

- 映射类别

➢满射　　$\varphi\colon \quad A \to B, \quad \forall y \in B, \exists x \in A, \quad st. \quad \varphi(x) = y$

$$\Updownarrow$$

$$\varphi(A)=\mathrm{B}$$

“满”

➢ 单射　　$\varphi\colon \quad A \to B, \quad \forall x_1, x_2 \in A, x_1 \neq x_2 \quad \Rightarrow \quad \varphi(x_1) \neq \varphi(x_2)$

“单”

➢ 双射　　$\varphi\colon \quad X \to Y$

“满”&“单”　“双”

多选题 1分

设置

A为数域F上的n阶方阵集合，B={0,1,...,n}，则法则 φ: $A \to r(A)$ 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 φ 为集合A到集合B的一个映射，$A_1 \subseteq A, B_1 \subseteq B$ 。则：

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

分别称他们为 A_1 在 φ 下的像；B_1 在 φ 之下的逆像。

A到B的映射 φ 是满射的充分必要条件是 $\varphi(A) = B$

$$\Leftrightarrow$$

多选题 1分

设置

对“充分必要条件” “ ⇔ ” 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 φ 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

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

便是集合B到集合A的一个双射。称 φ^{-1} 为 φ 的逆映射。

特别的有：

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

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 φ 为A与B两有限集之间的双射，则：

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

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 $|A|=|B|=n$

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

$$\varphi\text{:}\quad x_i \to y_{k_i}\quad (i=1,\dots,n,1\le k_i\le n)$$

目标:

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

$$\Updownarrow$$

$$surjective$$

$$\Updownarrow$$

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

映射与变换

- 两个映射相等的概念

设 φ ，τ 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. $X=\{1,2,3,\dots\}$ φ: $x\to x^2$ 单射变换

➢2. $X=\{1,2,3,\dots\}$ φ: $1\to 2,\quad 2\to 1,\quad n\to n\quad (n=3,4,\dots)$

双射变换

➢3. ...

映射与变换

- 定理

➢ 任意n元有限集共有$n!$个双射变换。

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

一个双射变换 $\Leftrightarrow$ 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：

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

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

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

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

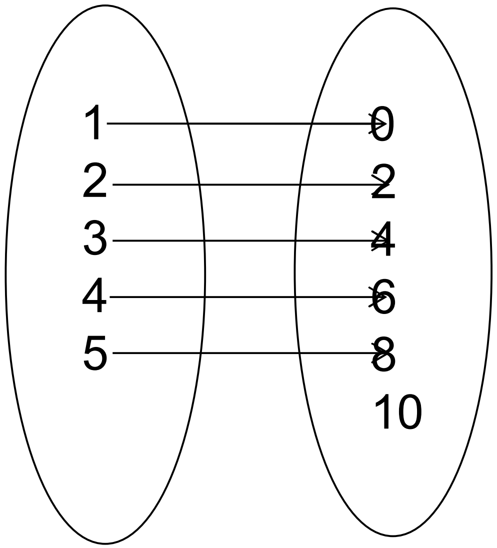
$$=\begin{pmatrix}2&3&1\\3&1&2\end{pmatrix}=\begin{pmatrix}3&1&2\\1&2&3\end{pmatrix}=\begin{pmatrix}3&2&1\\1&3&2\end{pmatrix}$$

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？

φ_1:　$x \to 2x$　　　φ_2:　$1 \to 0,\quad 2 \to 2,\quad 3 \to 4,\quad 4 \to 6,\quad 5 \to 8$



映射与变换

- 练习

➢2. $X=\left\{A_{n\times n}\left|a_{ij}\in F,1\le i,j\le n\right.\right\}$ F为一数域，判断以下从X到F的法则

$$\varphi:\quad A\to\left|A\right|$$

映射?　　　　满射?　　　　单射?

➢3. $\varphi_5\left(\varphi_3\left(\varphi_1\left(1\right)\right)\right)=?$

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

作业

- P5: 1、3
- P11: 5