近世代数

计算机科学与技术学院
苏敬勇

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：李克洲、连芸、李峥岑

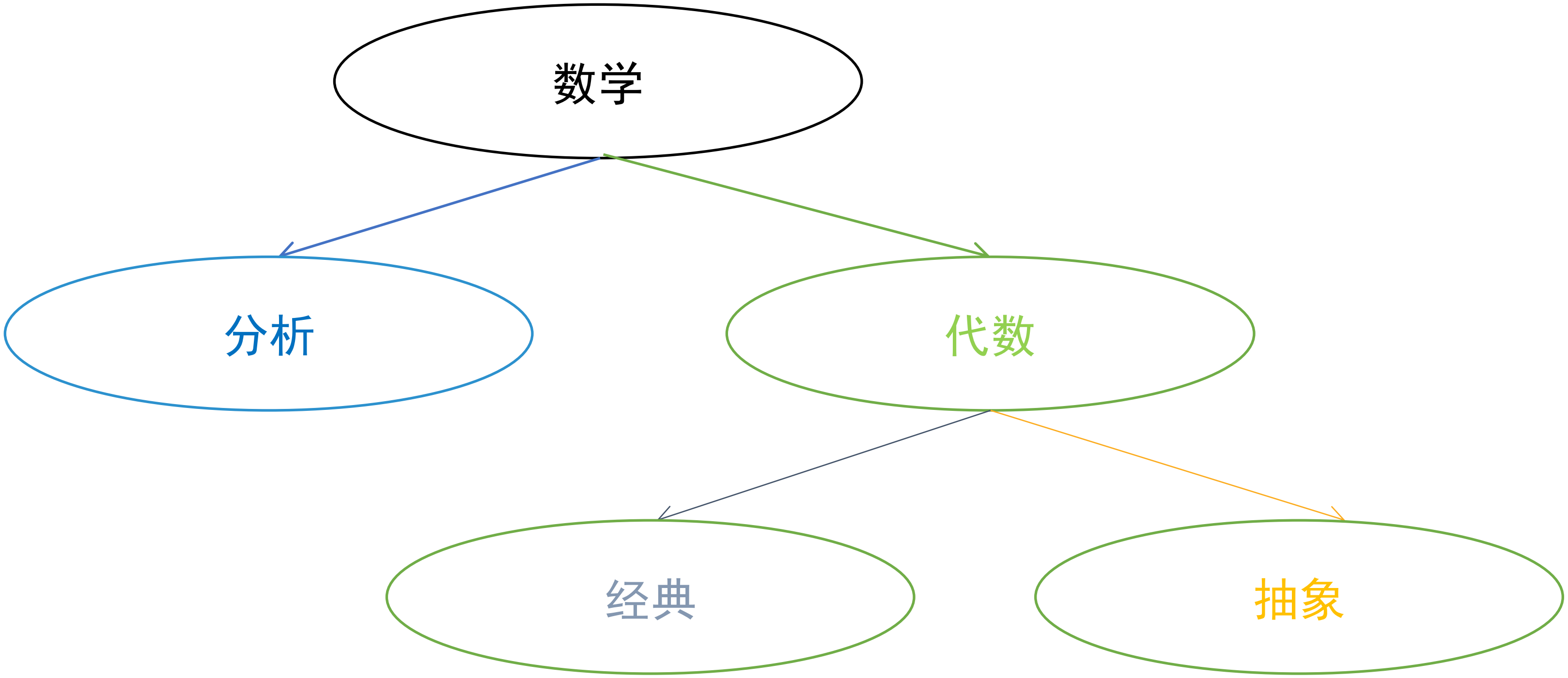
  hit_algebra2021@163.com

- 成绩：平时作业40%，期末考试60%

- 2021秋《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

- 代数系统 --- 一个集合，含有一种或多种代数运算
- 近世代数---研究各种代数系统的一门学科
- 抽象代数---一般来说，不仅研究的集合是抽象的，而且其运算也是抽象的。因此，近世代数吧也常被称作抽象代数。
- 群、环和域---最重要的分支

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^*

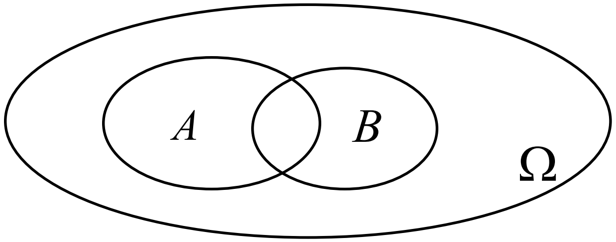
注：$|A|$表示集合A的元素个数，称作势（Cardinality）

- 表示方法:

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

➢描述法：$E=\{全体自然数\}$ $F=\left\{x \middle| x是实数且x^2<1\right\}$

➢文氏图：



集合

- 集合与集合之间的关系&集合运算

➢子 $A \subseteq B$ $A \subset B$ $A=B \Leftrightarrow A \subseteq B \& B \subseteq A$

$P(A)$：A的幂集，A的所有子集的集合

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

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

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

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

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

单选题 1分

设置

下列描述正确的是（ ）

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

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

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

ϕ 是任何集合的真子集

提交

单选题 1分

设置

下列描述正确的是（ ）

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

B $A \not\subseteq B \Rightarrow A \not\subset B$

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

D ϕ 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

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

集合

- 练习:

➢1. 证明分配律

➢2. $A \bigcap B = A \bigcap C \quad \Rightarrow ? \quad B = C \qquad "\bigcup" ?$

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

➢4. 证明摩根定律

映射与变换

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

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

- 例题

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

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

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

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

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

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

映射与变换

- 映射类别

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

$$\Updownarrow$$

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

“满”

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

“单”

➢ 双射 $\varphi: \quad X \to Y$

“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 $\varphi:\quad A\to r(A)$ 是A到B的一个

满射

双射

单射

映射

提交

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 $\varphi: \quad A \to r(A)$ 是A到B的一个

A 满射

B 双射

C 单射

D 映射

提交

- 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：

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

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 $\varphi\left(A\right) = B$

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 ）

从A推向B是在证A成立的充分性

从B推向A是在证A成立的充分性

从A推向B是在证B成立的必要性

从B推向A是在证B成立的必要性

提交

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：

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

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 $|A|=|B|=n$

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

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

目标:

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

$$\Updownarrow$$

$$surjective$$

$$\Updownarrow$$

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

- 推论

设A与B是两个所含元素个数相等的有限集合,则A到B的映射 φ 是双射当且仅当 φ 是满（单）射。

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：

$$\varphi = \tau$$

- 映射的合成（映射的乘法）

设 τ 是集合A 到集合B的一个映射, σ 是集合B到C的一个映射，则显然

$$x \to \sigma(\tau(x)) \ (\forall x \in A)$$

是A到C的一个映射，记为 $\sigma\tau$，称其为映射的合成或映射的乘法，而称$\sigma\tau$为映射 τ 与 σ 的乘积。

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. $X=\{1,2,3,\ldots\}$ $\varphi:\quad x\to x^2$ 单射变换

➢2. $X=\{1,2,3,\ldots\}$ $\varphi:\quad 1\to 2,\quad 2\to 1,\quad n\to n\quad (n=3,4,\ldots)$ 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 $M=\{1,2,\ldots,n\}$， 则 $\varphi\longrightarrow\varphi(1)\varphi(2)\ldots\varphi(n)$

一个双射变换 $\Leftrightarrow$ 全排列

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

“一个n元/阶置换” or “一个n次置换”

映射与变换

- 例题：

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

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

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

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

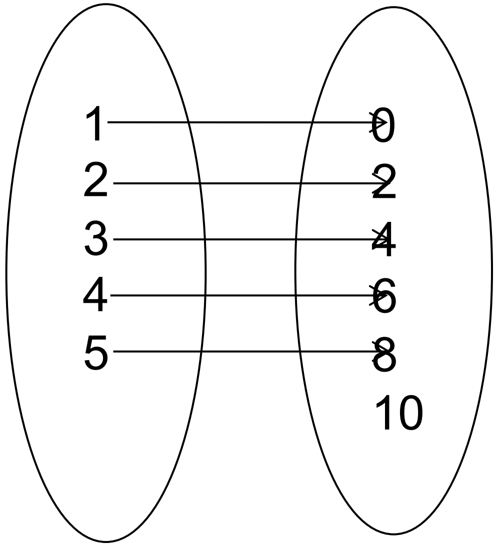
$$=\begin{pmatrix}2&3&1\\3&1&2\end{pmatrix}=\begin{pmatrix}3&1&2\\1&2&3\end{pmatrix}=\begin{pmatrix}3&2&1\\1&3&2\end{pmatrix}$$

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？

$\varphi_1: \quad x \to 2x \qquad\qquad \varphi_2: \quad 1 \to 0, \quad 2 \to 2, \quad 3 \to 4, \quad 4 \to 6, \quad 5 \to 8$



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

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

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

- P3: 1、3
- P8: 5