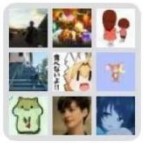
清華大學
Tsinghua University

离散数学II

刘世霞
shixia@tsinghua.edu.cn

课程群



群聊: 2024春-离散数学2课程群

该二维码7天内(3月7日前)有效，重新进入将更新

教师信息

- 教师：刘世霞，负责代数结构部分，1学分

  Email: shixia@tsinghua.edu.cn

  Office Tel: 62795459，13521593099

  办公室：东主楼10区407#

  研究方向： 可解释人工智能、大数据可视分析

- 教师： 周旻，负责图论部分，2学分

  Email: mzhou@tsinghua.edu.cn

  Office Tel: 62773275，15811001910

  办公室： 东配楼11区307#

  研究方向： 软件工程、形式化方法、静态分析、系统建模

助教信息

- 代数结构

  助教 杨维铠

  vicayang496@gmail.com 13051670559

- 图论

  助教 肖冬

  xiaodong14ry@163.com 15201152906

  助教 许智威

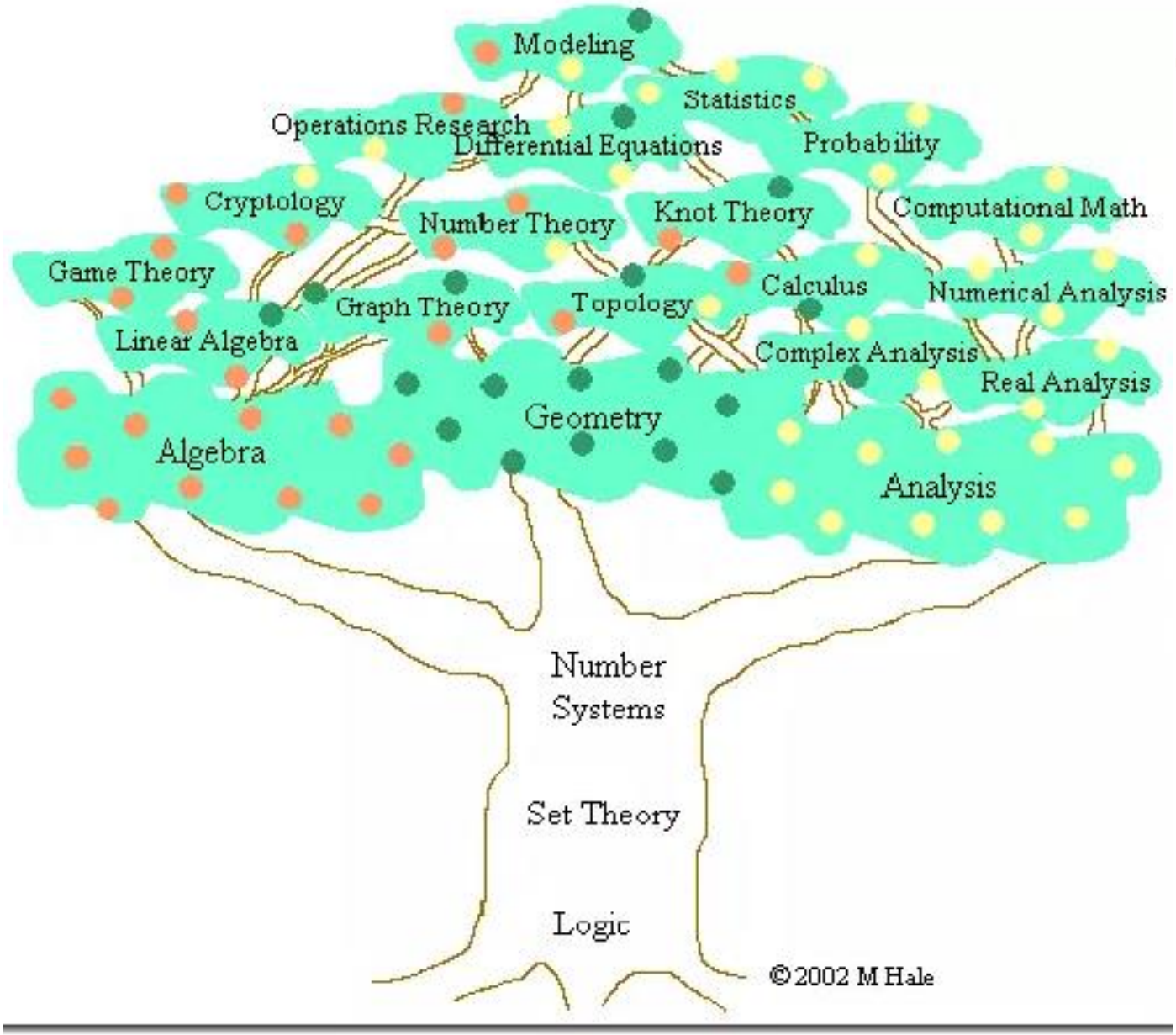
  xu-zw21@mails.tsinghua.edu.cn 18821217679

  助教 陈涵

  ch23@mails.tsinghua.edu.cn 13606869678

为什么要学习离散数学II

- 传统上，数学是以分析为中心的，研究的是连续的对象，以微积分为基础
- 随着计算机科学的出现，以离散对象为研究重点的数学分支蓬勃壮大起来，出现了离散数学
- 理论计算机科学的基础是离散数学
  - **集合论，数理逻辑**：奠定了计算机科学的基础
  - **图论，组合数学**：计算机科学，尤其是理论计算机科学的核心是算法，而**大量的算法建立在图和组合数学**的基础上
  - **代数结构，数论**：代数是无所不在的，在数学中非常重要。在计算机科学中，也是无处不在。


Modeling
Statistics
Operations Research
Differential Equations
Probability
Cryptology
Number Theory
Knot Theory
Computational Math
Game Theory
Calculus
Numerical Analysis
Graph Theory
Topology
Linear Algebra
Complex Analysis
Real Analysis
Geometry
Algebra
Analysis
Number
Systems
Set Theory
Logic
©2002 M Hale

为什么要学习离散数学II

- D.E.Knuth，Discrete Mathematics

  传统数学研究对象过于抽象，需要直接面向计算机应用

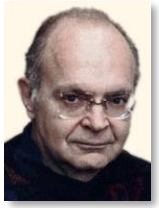
  “Discrete Mathematics”

  “Concrete Mathematics”

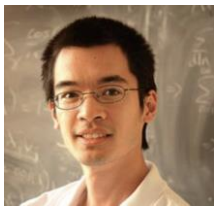
- D. E. Knuth 1974 年图灵奖获得者

  “ The Art of Computer Programming”

学好离散数学，脱颖而出

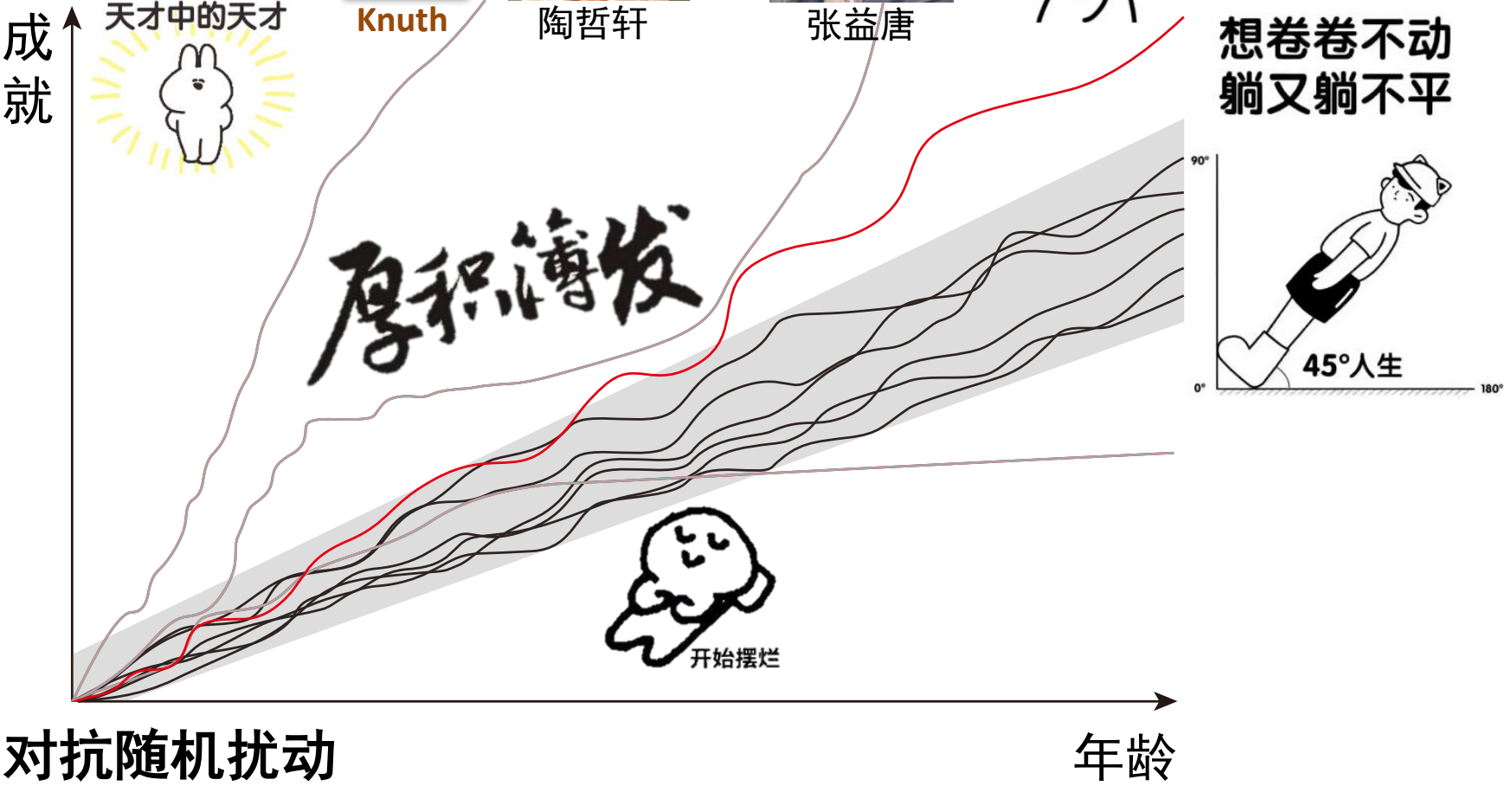


Knuth



陶哲轩

张益唐



对抗随机扰动
避免均值回归

代数结构的定位

建模：为数据和操作它们的算法提供了数学基础

- **数据类型的建模**
  - 复杂数据类型，如列表、树和图，可以使用代数结构（如半群、群和环）来建模。这有助于定义操作这些数据类型的算法。
- 在多个计算机学科中均有应用：形式语言和自动机理论、密码学、并行计算与分布式系统、编译器设计、计算机图形学和视觉处理、算法复杂度和计算模型、软件测试、形式验证

图论部分的定位

计算机求解问题的一般步骤

- **建模（图论）**：将问题抽象成一个适当的数学模型
- **数据结构**：转换成计算机可处理的对象（数据的存储、数据关系的表达、对数据进行的运算处理等）
- **算法**：程序性能优化


离散数学II
你

如何学好离散数学II

- 课件
- 教材

- 歌德说。。。
  - 光有知识是不够的，还应当运用；光有愿望是不够的，还应当行动。

- 连接应用：理解离散数学在软件工程和计算机科学中的应用。

课程基本信息

- 教材
  - 图论与代数结构（第2版）/清华大学计算机系列教材 清华大学出版社，崔勇，张小平 著

    改编自《图论与代数结构》，戴一奇、胡冠章、陈卫 清华大学出版社
- 参考书
  - Kenneth H.Rosen, Discrete Mathematics and Its Applications (Fifth Edition)
  - 《离散数学及其应用》第8版
  - Douglas West, Introduction to Graph Theory (Second Edition), Pearson Education.
  - 《数据结构与算法分析—C语言描述》, Mart Allen Weiss 著，机械工业出版社

考核与计分方案

- 纸质小作业： 20%

  每周通过网络学堂提交，小作业统一提交pdf格式文件，手写的可以拍照后用图像软件、Acrobat或者word，转换导出pdf，其他方式写的（比如word、latex）最后也导出pdf。不要提交压缩包，不要提交图片格式文件（jpg等）

- 上机小作业： 25%

  共5次，均为基本算法与核心算法，具体要求助教会在网络学堂上发布。

- 闭卷考试： 50% （代数结构 30%；图论 70%）
- 平时成绩：5%

作业要求

- 请使用作业纸，写清名字与学号
- 作业需手写后拍照并转成pdf文件上传至网络学堂提交。
  - 每次作业只能提交一个pdf文件
- 每周五9:50之前交上周的作业

奖项

- 最佳纸质作业奖
- 最佳编程作业奖

答疑

- 时间：每周四下午2:30-4:30
- 办公室
  - 刘世霞：东主楼10-407
  - 周旻：东配楼11-307
  - 杨维铠：东主楼10-406
  - 肖冬：东主楼10-410
  - 陈涵：东配楼11-320
  - 许智威：东配楼11-320

答疑：课程学习反馈

- 荷塘雨课堂
  - 作业形式

调研反馈：

针对课程学习有什么问题和建议？

谢 谢

作业题

- 习题八：4

  （{O}，×）->（{0}，×）

- 习题八：11

  $(a, b)(c, d) = (ac, cb+d)$

清華大學
Tsinghua University

代数结构

刘世霞
shixia@tsinghua.edu.cn

引言

- 经典代数：初等代数、高等代数和线性代数
  - 代数方程和线性方程组

- 代数结构：近世代数、抽象代数
  - 现代科学技术的数学基础之一
  - 代数系统：由一个集合和定义在这个集合中的一种或若干种运算所构成的系统。
    - 整数集合和普通加法构成一个代数系统

代数结构简介

- 定义：非空集合A和A上k个一元、二元或n元运算$f_1,f_2,.....,f_k$(其中，f_i是n_i 元代数运算，n_i 为正整数，i=1,2,3,...，k)组成的系统称为代数结构（代数系统）
- 代数结构是抽象代数的一个主要内容
- 研究的中心问题：
  - 集合上的抽象运算及运算的性质和结构
- 研究内容
  - 关注数学的体系结构
  - 半群、群、~~环、域、格和布尔代数等~~

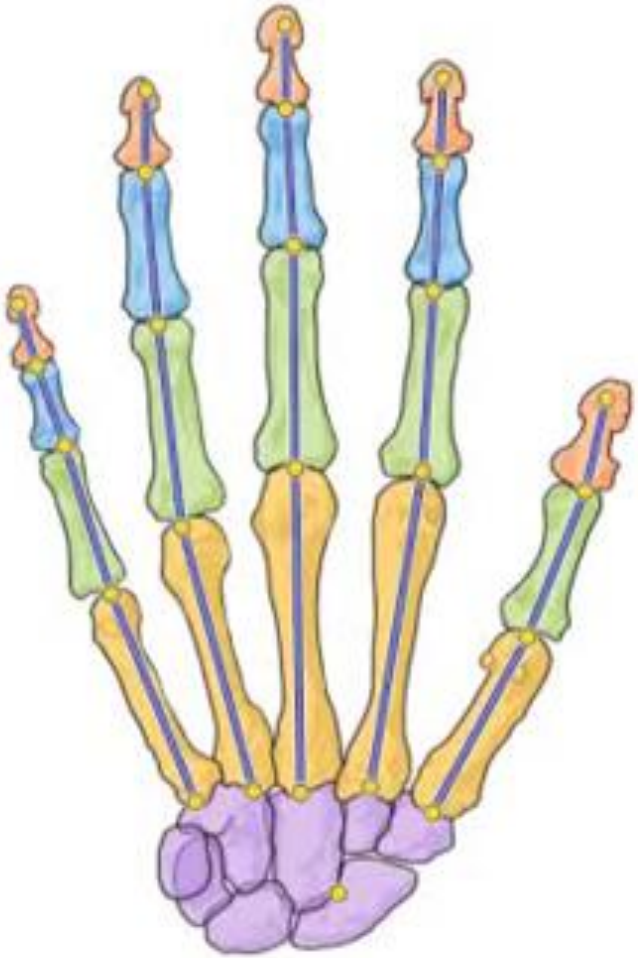
关于代数结构

- 研究意义：研究抽象代数结构的基本特征和基本结构，不仅能深化代数结构的理论研究，也能扩展其应用领域。

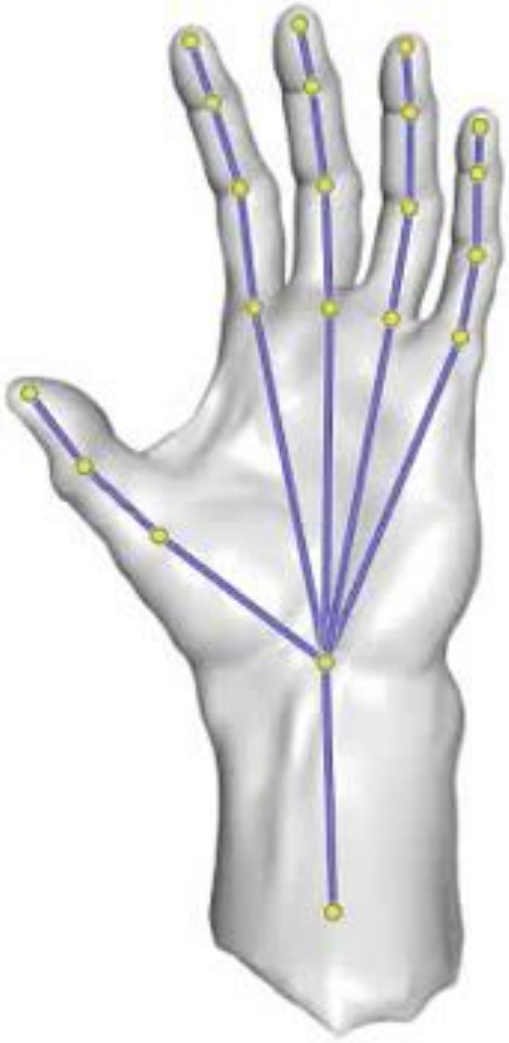
应用：

- 现代数学，如拓扑学、泛函分析等
- 计算机科学：如
  - 半群→自动机、形式语言
  - 群→纠错码的设计
  - 格和布尔代数→计算机硬件设计、通讯系统设计
- 其他：代数方程求解、物理、化学

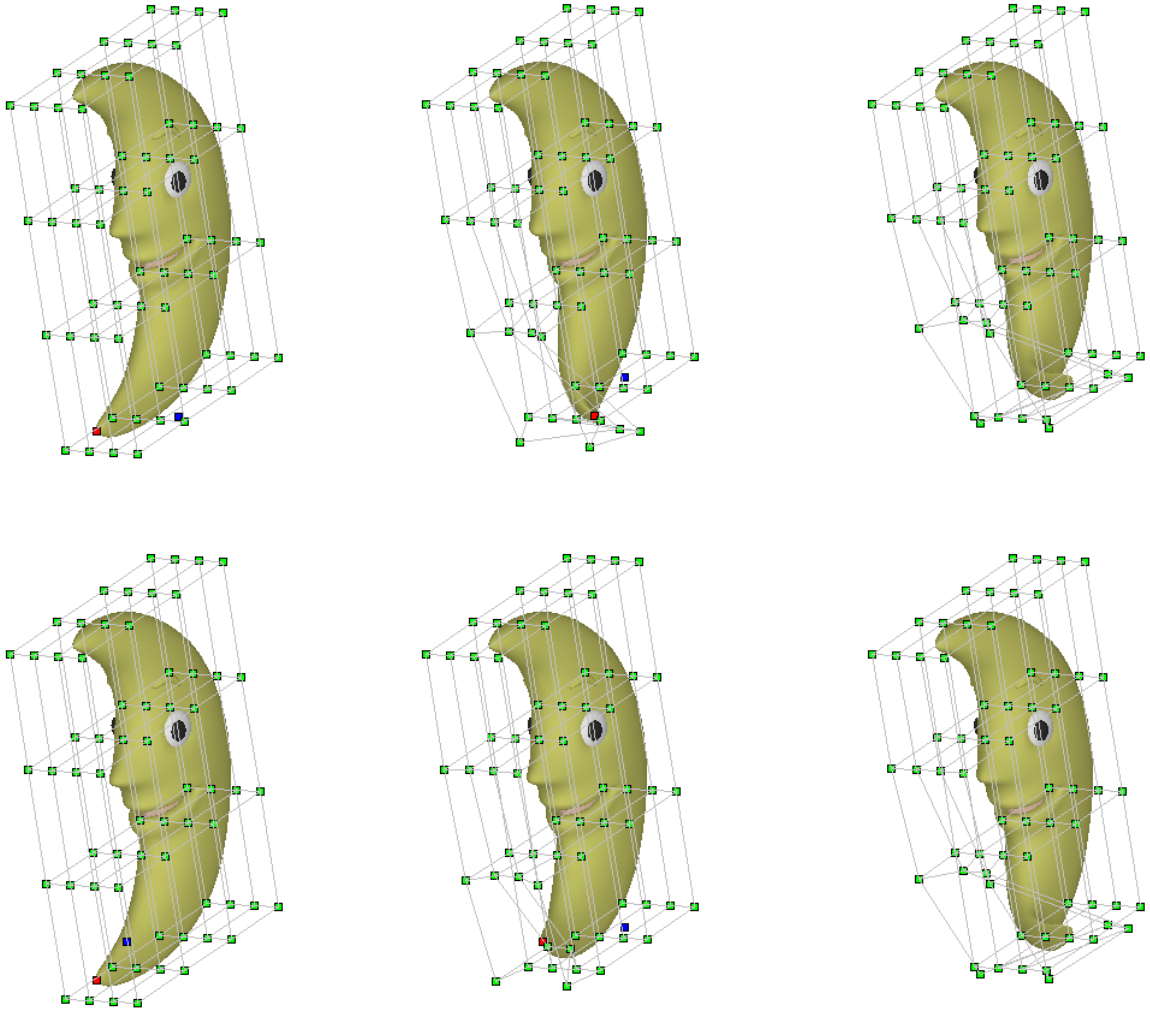
2D Image



3D Surface



交换群性质



群论的出现

- 群论是现代数学非常重要的分支，群论产生的开端非常平凡，但是群论的创立者却充满了传奇。代数方程根式解法的研究有很悠久的历史。大家知道，一个实系数的代数多项式在实数域中只要能分解成一些实系数的一次因式与二次因式的乘积，则利用我们熟知的二次方程

$$ax^2 + bx + c = 0$$

的求根公式

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

- 人们试图对次数更高的方程得到类似的求解公式
- 形如 $ax^3+bx^2+cx+d=0$的三次方程的求根公式直至16世纪才被发现. 它是由意大利数学家费罗(Ferro)和丰塔那(Fontana) 彼此独立得到的.
- 1545年, 卡尔达塔(Cardano)在他的《大术》(Ars Magna)一书中公开发表了丰塔那的方法. 这部书还讲述了费拉里(Ferrari)求解四次方程的方法.

- 但事情的发展似乎突然停了下来.

虽然有很多数学家作出了努力, 其中包括18世纪中叶伟大的瑞士数学家欧拉(Euler), 但没有一个人能找出五次方程的求根公式.

拉格朗日(Lagrange)在1770年猜测:

这样的求根公式不存在.他预见到一般方程的可解性问题最后将归结到关于诸根的某些排列置换问题。

- Lagrange的洞察力启发了年轻的Abel与Galois，他们在继承了Lagrange留下的宝贵遗产基础上，各自作出了重要的贡献。尤其是，犹如划破黑夜长空的一颗彗星——伽罗华(Galois)的出现，开创了置换群论的研究.
- 1824年, 挪威数学家阿贝尔(Abel)证明了拉格朗日的看法.
- 阿贝尔在高中读书时就阅读了拉格朗日、高斯有关方程式论的著作。开始时，他利用高斯处理二项式方程的具体方法去研究五次方程，曾一度以为能用根式解出五次方程，但很快他发现其中存在的问题。

- 这时，Abel敏感地猜想到一般五次方程不可能用根式求解的结论。
- 接着，Abel成功地证明了一条定理，今天称之为Abel定理。由此定理，Abel就证明了：“高于四次的一般方程不可能有一般形式的根式解”。这是数学史上的一项重要成就。
- 但是虽然没有通用公式，有些特殊的五次方程有求根公式，那么自然会问：如何判定一个给定的五次方程是否有这样的求根公式?
- 对具有根式解的代数方程的特征问题，阿贝尔一直在竭尽全力地研究这个问题. 不幸的是，1829年死神夺去了年仅26岁的他，使他即将完成的光辉事业功亏一篑。

群论的创始者：伽罗华

- 在这一时期, 碰巧还有一位年轻人也在勤奋地钻研这个问题, 而且最终取得了成功, 他就是伽罗华(Galois).
- 可是这位年轻人获得的非凡成果, 在他因决斗去世11年后才开始得到数学界的承认.

伽罗华(Galois)

Galois Theory

Evariste Galois(1811−1832)

- French mathematician, who showed that whether a polynomial was solvable or not was equivalent to whether or not the permutation group of its roots had a certain structure, i.e. whether or not it was a solvable group.

代数方程能用根式求解的充分必要条件是自同构群可解

- Using Galois theory, certain problems in field theory can be reduced to group theory, which is in some sense simpler and better understood.

伽罗华(Galois)

- 伽罗华1811年10月降生于巴黎近郊
- 14岁那年因考试不及格而重上三年级
- 15岁参加声望很高的巴黎高等工科大学的入学考试时，伽罗华失败了，不得不进入较普通的师范学校
- 就是在这所学校，伽罗华写出了他的第一篇关于连分数的数学论文，显示了他的能力
- 他的下两篇关于多项式方程的论文遭到法国科学院的拒绝。更糟的是，两篇论文手稿还莫名其妙地被丢失了
- 1829年7月，他在巴黎高等工科大学的入学考试中再次失败
- 怀着沮丧之情，伽罗华于1830年初又向科学院提交了另一篇论文，这次是为竞选一项数学大奖

伽罗华(Galois)

- 科学院秘书傅立叶（Fourier）将其手稿拿回家去审读，不料在写出评审报告前去世了，此文再也没有找到
- 三失手稿，加之考巴黎高等工科大学两度失败，伽罗华遂对科学界产生排斥情绪，变成了学生激进分子，被学校开除
- 担任私人辅导教师谋生，但他的数学研究工作依然相当活跃。在这一时期写出了最著名的论文“关于方程可根式求解的条件”，并于1831年1月送交科学院
- 到3月，科学院方面仍杳无音讯，于是他写信给院长打听他的文章的下落，结果又石沉大海
- 他放弃了一切希望，参加了国民卫队。在那里和他在数学界一样运气不佳。他刚加入不久，卫队即遭控告阴谋造反而被解散

伽罗华(Galois)

- 在1831年5月10日进行的一次抗议聚宴上，伽罗华手中举着出鞘的刀提议为国王干杯，这一手势被同伙们解释成是要国王的命；第2天他就被捕了，后来被判无罪，并于6月15日获释
- 7月4日，他终于打听到他给科学院的那篇论文的命运：因“无法理解”而遭拒绝
- 审稿人是著名的数学家泊松（Poisson）
- 7月14日因为他在公共场所身着已被解散的国民卫队的制服，又遭逮捕并被判了六个月监禁
- 在获释不久，他陷入了与斯特凡小姐的恋情。这导致了他的早亡。这次恋爱事件不知何故引起了一场决斗

- 1832年5月29日，决斗的前夜，伽罗华写了封很长的信给他的朋友舍瓦利耶（A. Chevalier），其中大致描述了他的数学理论，从而给数学界留下了唯一一份它将蒙受何等损失的提要
- 在第二天的决斗中（离25步远用手枪射击），伽罗华的胃部中弹，24小时后去世，享年不足21岁
- 伽罗华留给世界的最核心的概念是（置换）群，他成了群论的创始人。
- 工作：探寻五次和五次以上方程的一般公式解法
- 方法：他并不急于寻求解高次方程的方法，而是将重心放在判定已知的方程是否有根式解。与拉格朗日相同，也从方程根的置换入手。当他系统地研究了方程根的排列置换性质后，提出了一些确定的准则以判定一个已知方程的解是否能通过根式找到。---群
- 人们认为“他的死使数学的发展被推迟了几十年”

主要内容

- 第七章：代数结构预备知识
- 第八章：群

第七章 代数结构预备知识

7.1 集合与映射

- 设S是任意一个集合，如果元素a属于S，记为$a \in S$，否则记$a \notin S$。
- S中不同元素的个数成为该集合的基数，用$|S|$表示。
- 当集合S确定之后，能对应地得到另一个集合$P(S)$，$P(S)$是S的全部子集的集合。成为S的幂集。
- $P(S)$的基数是$2^{|S|}$。

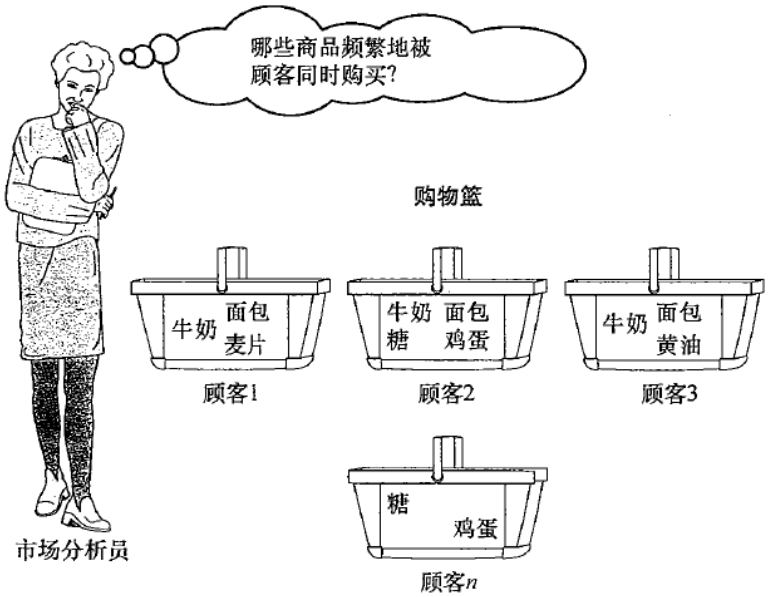
7.1 集合与映射

- $P(S)$中的元素A，是集合S的一个子集，可以刻画为

$$A = \{x \in S | p(x)\}$$

其中p代表某种性质。

- 因此A可以解释为：具有性质p的S的元素的集合
- 应用：频繁模式挖掘



$A \cup B = \{x \mid x \in A \vee x \in B\}$ $\quad -A = E - A = \{x \mid x \notin A\}$

$A \cap B = \{x \mid x \in A \wedge x \in B\}$ $\quad A - B = \{x \mid x \in A \wedge x \notin B\}$

$A \oplus B = (A - B) \cup (B - A) = \{x \mid x \in A \,\overline{\vee}\, x \in B\}$

元素x $\in$ 集合A

$A = B \Leftrightarrow (\forall x)(x \in A \leftrightarrow x \in B)$ $\quad \mathrm{A} = B \Leftrightarrow (A \subseteq B \wedge B \subseteq A)$

$A \neq B \Leftrightarrow (\exists x) \neg (x \in A \leftrightarrow x \in B)$

$A \subseteq \mathrm{B} \Leftrightarrow (\forall x)(x \in A \rightarrow x \in B)$

$A \subset B \Leftrightarrow (A \subseteq B \wedge A \neq B)$

$\emptyset = \{x \mid x \neq x\}$

$E = \{ x \mid x = x \}$

对任意的集合A，$\emptyset \subseteq A$

A和B不相交 $\Leftrightarrow \neg (\exists x)(x \in A \wedge x \in B)$

$\cup A = \{x \mid (\exists z)(z \in A \wedge x \in z)\}$

$\cap A = \{x \mid (\forall z)(z \in A \rightarrow x \in z)\}$

$\cup \emptyset = \emptyset$

$\cap \emptyset$无意义

$P(A) = \{x \mid x \subseteq A\}$

7.1 集合与映射

- 集合运算：

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

- 分配律！

7.1 集合与映射

- 定义7.1.1：设S和T是给定的两个集合，如果有一个规则f，使对任意一个元素$x \in S$，在T中有唯一的元素y与之对应，则称f是S到T的一个映射，记作$f: S \to T$和$y = f(x)$。
- S称为f的定义域，T为f的值域，y称为x的象，x称为y的原象。
- 根据定义：
  - S中每个元素在T中都有象
  - T中的每个元素在S中不一定都有原象
  - 习惯上我们将S中全部元素的象所构成的集合成为f的象，记作$f(S)$。显然$f(S) \subseteq T$。

7.1 集合与映射

- 定义7.1.2：两个映射f, g

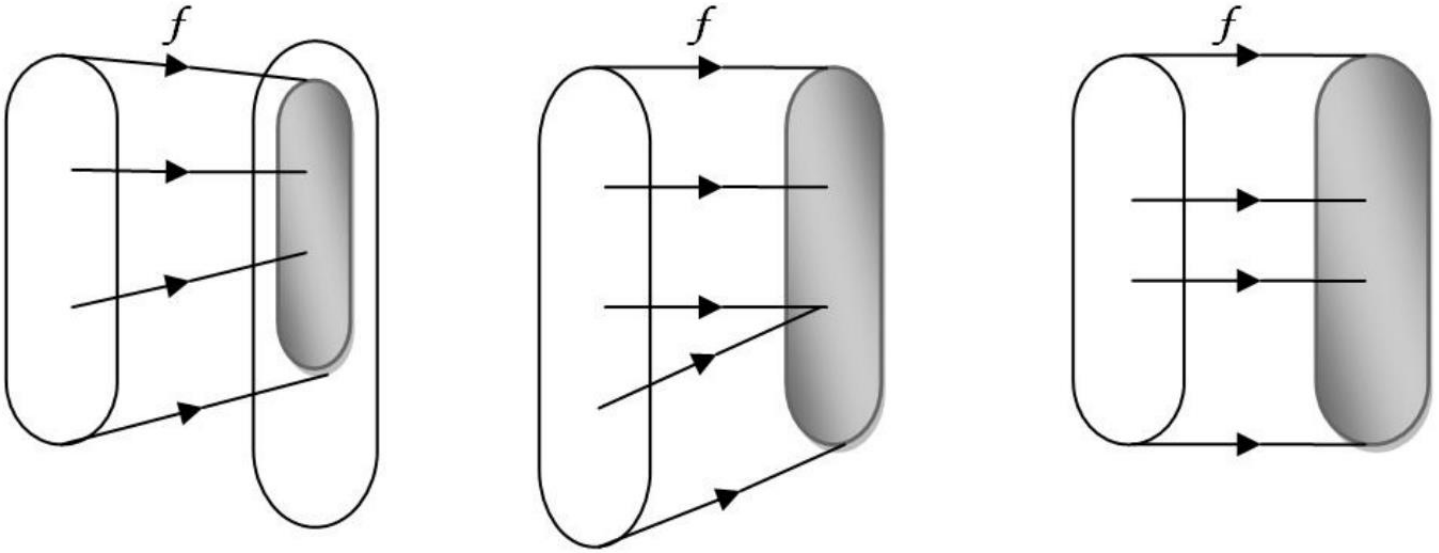
$$f: A_1 \to B_1$$
$$g: A_2 \to B_2$$

当且仅当$A_1 = A_2$，$B_1 = B_2$，且对任意$x \in A$，都有$f(x) = g(x)$，称f和g是相等的映射，记为$f = g$。

7.1 集合与映射

定义7.1.3 设f是A到B的一个映射。

1. 若对任意$a_i \neq a_j$，$a_i, a_j \in A$，都有$f(a_i) \neq f(a_j)$，称f是A到B的单射。
2. 若$f(A) = B$，则称f是A到B的满射。
3. 若f既是单射又是满射，则称它是A到B的双射。



单射　　满射　　双射

多选题 1分

Setting

定义f: $n \to n$, 当2|n时

$n \to n+1$ 当2∤n时

A和B是整数集合，则f是A到B的一个

A 映射

B 单射

C 满射

D 双射

提交

7.1 集合与映射

- 定义7.1.4：设A,B,C是三个集合，有两个映射

$$f:A\to B \quad g:B\to C$$

- 则由f和g可确定一个A到C的映射h，

$$h:\ a\to g(f(a))$$

- 称h为f与g的合成，记作$h=gf$，亦即

$$h(a)=(gf)(a)=g\big(f(a)\big)$$

$$gf(a)=g(f(a))$$

- 映射的合成一般不满足交换律，但是满足结合律。

$$\alpha:A\to B,\beta:\mathrm{B}\to\mathrm{C},\gamma:\mathrm{C}\to\mathrm{D}$$

$$\gamma(\beta(\alpha(a)))=(\gamma\beta)(\alpha(a))=((\gamma\beta)\alpha)(a)$$

$$\gamma(\beta(\alpha(a)))=\gamma((\beta\alpha)(a))=(\gamma(\beta\alpha))(a)$$

$$\gamma(\beta\alpha)=(\gamma\beta)\alpha$$

7.1 集合与映射

- 定理7.1.1：设f是A到B的映射，I_A和I_B分别是A和B中的恒等映射，则 $I_B f = f$，$f I_A = f$
- 证明：
  - $I_B f$和f具有相同的定义域A和相同的值域B，且对于任意的$a \in A$，都有

$$I_B f(a) = I_B(f(a)) = f(a)$$

  - 因此 $I_B f = f$
  - 同理可证：$f I_A = f$

- 定义7.1.2：两个映射f, g

$$f: A_1 \to B_1$$
$$g: A_2 \to B_2$$

当且仅当$A_1 = A_2$，$B_1 = B_2$，且对任意$x \in A$，都有$f(x) = g(x)$，称f和g是相等的映射，记为$f = g$。

7.1 集合与映射

定义7.1.5

- 设两个映射：

$$f: A \to B \quad g: B \to A$$

- 若$gf = I_A$成立，则称f是左可逆映射，g是右可逆映射，并称g是f的左逆映射，f是g的右逆映射。
- 又若$fg = I_B$也成立，则称f和g都是可逆映射。

- 思考：可逆映射是否一定是双射？

设置

可逆映射是否一定是双射?

A 是

B 否

设两个映射：

$$f: A \to B \quad g: B \to A$$

若$gf = I_A$成立，则称f是左可逆映射，g是右可逆映射，并称g是f的左逆映射，f是g的右逆映射。

又若$fg = I_B$也成立，则称f和g都是可逆映射。

提交

7.1 集合与映射

定理7.1.2

- A到B的映射f:

  f是左可逆的充要条件是f为单射

  f是右可逆的充要条件是f为满射

推论：$f:A \to B$是可逆映射，当且仅当f是双射

入要单，出要满

可逆映射是否一定是双射?

7.1 集合与映射

- 必要性：f左可逆⟶f为单射
  - 如何证明f是单射？

    $\forall a_1, a_2 \in A \quad f(a_1) = f(a_2) \Rightarrow a_1 = a_2$
  - 由f左可逆，可知必存在$g: B \to A$，使得

    $$gf = I_A$$

$$a_1 = I_A(a_1) = gf(a_1) = g(f(a_1)) = g(f(a_2)) = gf(a_2) = I_A(a_2) = a_2$$

- 充分性：f为单射⟶f左可逆
  - 如何证明f左可逆？构造g使得 $gf = I_A$
  - 定义$g: B \to A$ 如下：

$$g(b) = \begin{cases} a, \text{若存在} a \in A, \text{使} f(a) = b \\ a_0, \text{若} b \notin f(A) \text{且} a_0 \in A \end{cases}$$

  - 此时，$\forall a \in A \quad gf(a) = g\big(f(a)\big) = g(b) = a$
  - 因此 $gf = I_A$

7.1 集合与映射

定理7.1.3

- 设f是A到B的映射，且

$$gf = I_A, fh = I_B, \qquad \text{则} g = h$$

- 证明：

$$g: B \to A, \quad h: B \to A$$

$$g = gI_B = g(fh) = (gf)h = I_A h = h$$

可逆映射的逆映射是唯一的！

7.1 集合与映射

例： 设$f:A\to B, g:B\to C$都是双射，则gf是A到C的双射

- 证明：
  - 由定理7.1.2的推论，有逆映射$f^{-1}:B\to A, g^{-1}:C\to B$，因此$f^{-1}g^{-1}$是$C$到$A$的映射，并且

$$(gf)(f^{-1}g^{-1})=((gf)f^{-1})g^{-1}=(g(ff^{-1}))g^{-1}=gg^{-1}=I_C$$
$$(f^{-1}g^{-1})(gf)=f^{-1}(g^{-1}(gf))=f^{-1}((gg^{-1})f)=f^{-1}f=I_A$$

  - 因此gf是可逆映射，$f^{-1}g^{-1}$是它的逆。所以gf是双射。
  - 由该例和定理7.1.3可知，$(gf)^{-1}=f^{-1}g^{-1}$

推论： $f:A\to B$是可逆映射，当且仅当f是双射

第七章 代数结构基本知识

7.1 集合与映射

7.2 等价关系

7.3 代数系统的概念

7.4 同构与同态

7.2 等价关系

定义7.2.0

- 设A, B是集合，称集合
$$\{< a, b > | a \in A, b \in B\}$$
- 是A和B的笛卡儿积，记为$A \times B$

- 对于集合A到集合B的任何一个映射f，都可以写出很多二元组(a, b)，其中$a \in A, b \in B$。显然，这是$A \times B$的子集。
- 我们将映射的概念加以推广，即定义域不一定是A本身，就引出二元关系。

7.2 等价关系

定义7.2.1

- 集合A和B的笛卡儿积$A \times B$的任一子集R称为A与B之间的一个二元关系，它的元素是有序对(a,b)，记为aRb，其中$a \in A, b \in B$。当$(a,b) \notin R$时，说a与b没有R关系，记作$a\not Rb$。
- 当$A = B$时，称R为集合A上的二元关系。

多选题 1分

Setting

对于集合A上的二元关系R，要证其为等价关系，需要验证

A 自反性

B 对称性

C 反对称性

D 传递性

Submit

7.2 等价关系

定义7.2.2 设R是集合A上的二元关系，如果

1. 对所有的$a \in A$，都有aRa，即R具有自反性
2. 对所有的$a, b \in A$，若aRb，则bRa，即R具有对称性
3. 对所有的$a, b, c \in A$，若aRb，则bRc，则aRc，即R具有传递性

则称R是A上的等价关系。用符号 $\backsim$ 表示。

7.2 等价关系

- 设R是集合A上的一个等价关系，对任一元素$a \in A$, 可以把所有与a有R关系的元素构成一个集合，称之为A的一个等价类，记作$\bar{a}$，即

$$\bar{a} = \{x \in A | x \sim a\}$$

- 其中，a为该等价类的代表元
- 等价类$\bar{a}$的性质：

1. $a \in \bar{a}$
2. 若b, c $\in \bar{a}$，则 b~c
3. 若b $\in \bar{a}$ 且b~x，则$x \in \bar{a}$

等价类中任两个元素都有等价关系！

任两个有等价关系的元素都在同一等价类中！

7.2 等价关系

定理7.2.1 设~是A上的一个等价关系，对任意元素$a, b \in A$

- 若非　$\overline{b} = \overline{a}$
- 则有　$\overline{b} \cap \overline{a} = \varnothing$

定理7.2.2 设$\overline{a_1}, \overline{a_2}, \cdots, \overline{a_n}$是$A$上由等价关系~确定的全部等价类，那么

$$\bigcup_{i=1}^{n} \overline{a_i} = A \qquad \overline{a_i} \bigcap_{i \neq j} \overline{a_j} = \varnothing$$

集合A上的等价关系~可确定它的一个划分！

Application Example: Community Detection

- M. E. J. Newman

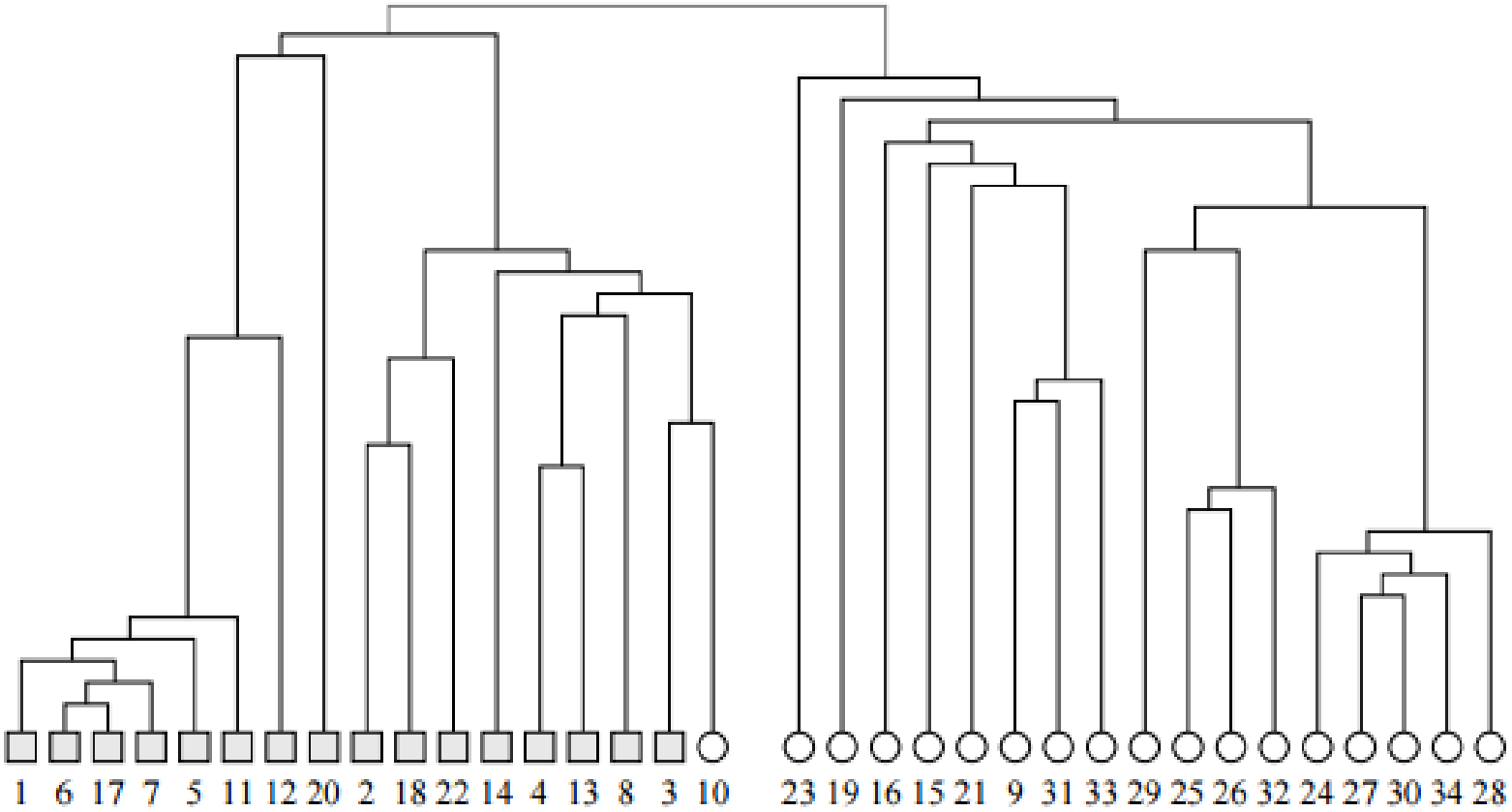
Fast algorithm for detecting community structure in networks

ularity" Q as follows [6]. Let e_{ij} be the fraction of edges in the network that connect vertices in group i to those in group j, and let $a_i = \sum_j e_{ij}$ [19]. Then

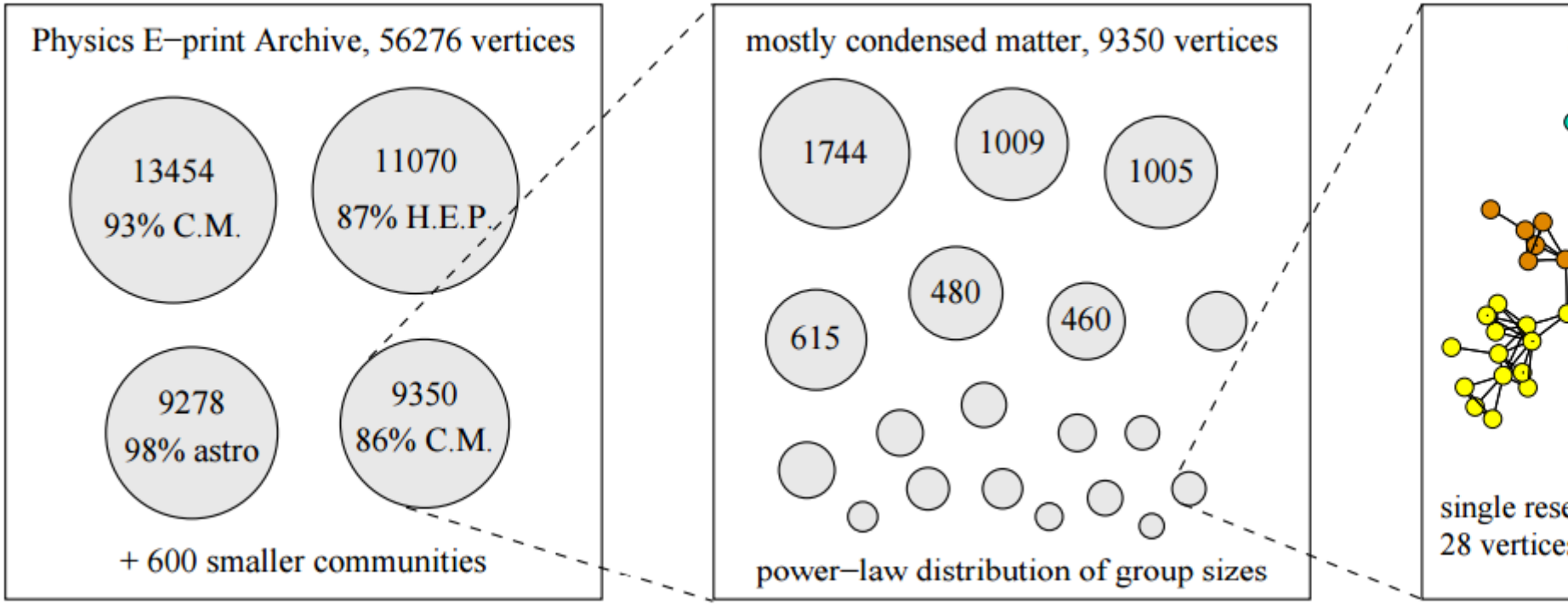
$$Q = \sum_i (e_{ii} - a_i^2) \qquad (1)$$

http://arxiv.org/pdf/cond-mat/0309508.pdf

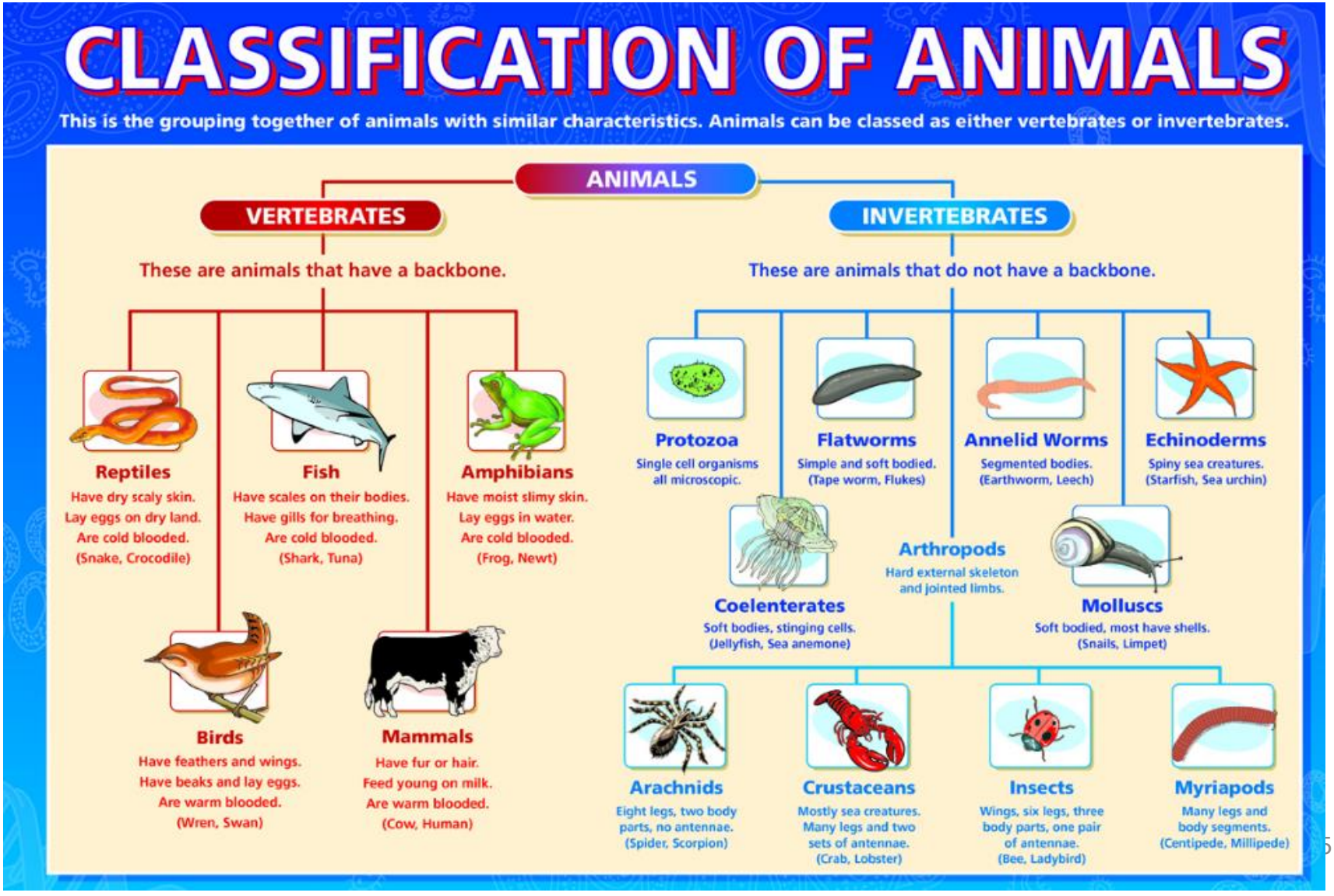
Basic Idea

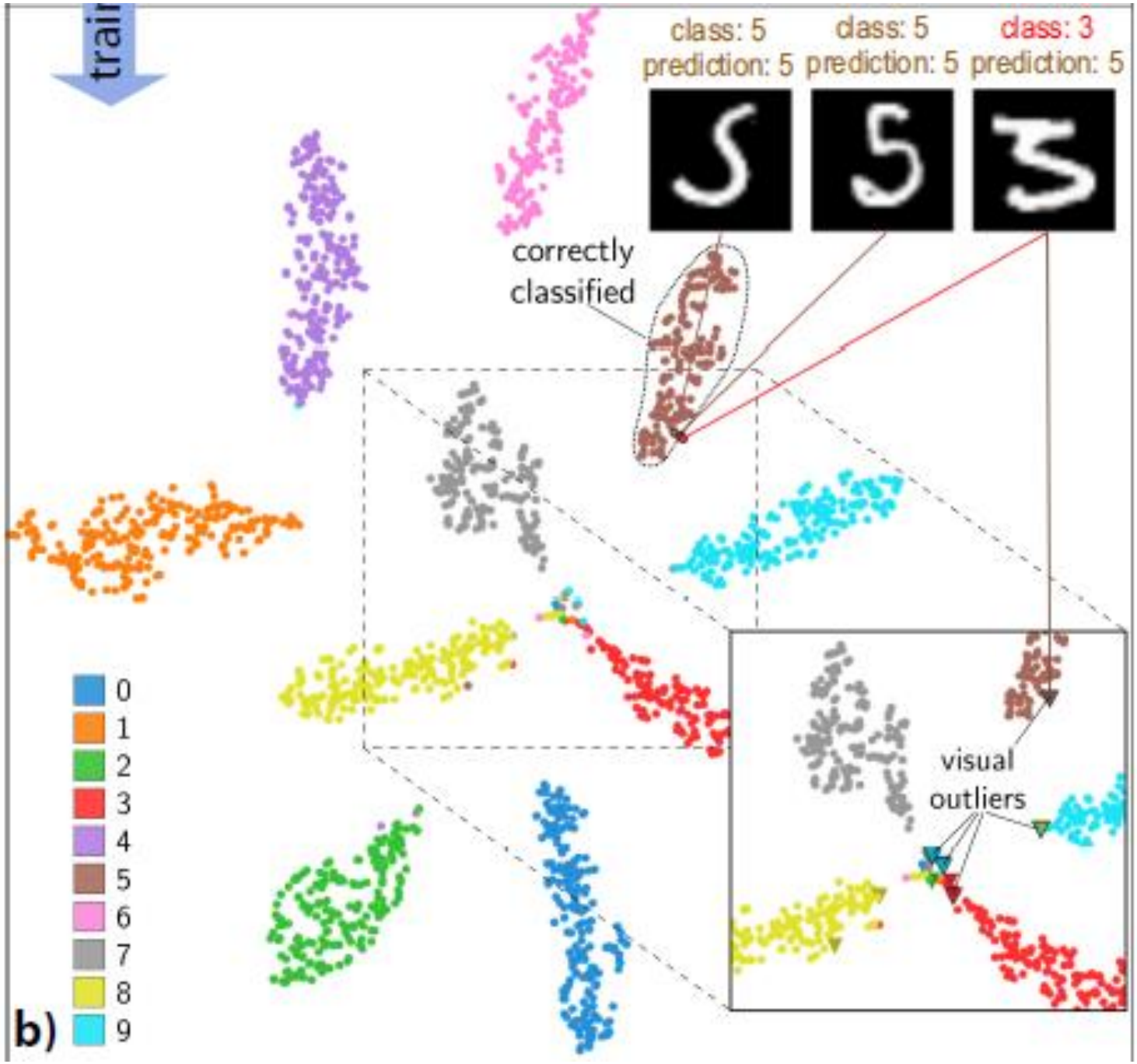

1 6 17 7 5 11 12 20 2 18 22 14 4 13 8 3 10
23 19 16 15 21 9 31 33 29 25 26 32 24 27 30 34 28

Results


Physics E−print Archive, 56276 vertices
13454
93% C.M.
11070
87% H.E.P.
9278
98% astro
9350
86% C.M.
+ 600 smaller communities
mostly condensed matter, 9350 vertices
1744
1009
1005
480
615
460
power−law distribution of group sizes
single rese
28 vertice

Application Example: Classification




class: 5
prediction: 5
class: 5
prediction: 5
class: 3
prediction: 5
correctly
classified
visual
outliers
0
1
2
3
4
5
6
7
8
9
b)

7.2 等价关系

- 把由等价关系~确定的等价类的集合称为等价类族，用$\bar{A}$表示：

$$\bar{A} = \{\bar{a} | a \in A\}$$

- 为表示等价类族是由等价关系~确定的，常使用记号$A/\sim$表示$\bar{A}$，并称之为集合A关于~的商集

商集就是由A上等价关系~确定的等价类的集合

7.2 等价关系

例

- 设$A=\{0,1,2,\ldots\}$是非负整数集合，m是一个正整数，令R是A中的模m同余关系，则

$$\overline{1}=\{1,m+1,2m+1,\ldots\},$$
$$\overline{2}=\{2,m+2,2m+2,\ldots\},$$
$$\ldots$$
$$\overline{m-1}=\{m-1,2m-1,3m-1,\ldots\},$$
$$\overline{0}=\{0,m,2m,\ldots\}$$

- 显然R是等价关系，因此

$$A/R=\{\overline{0},\overline{1},\ldots,\overline{m-1}\}$$

7.2 等价关系

- 商集$A/\sim$确定后，对每一个$a \in A$，它必定属于唯一的等价类，即对应商集中某个确定元$\bar{a}$
- 令映射$\gamma: a \to \bar{a}$为集合A到$A/\sim$的一个映射，称之为A到$A/\sim$的自然映射
- 显然，自然映射为满射
- 思考
  - 集合A上的等价关系$\sim$可以确定A的一个划分
  - 那么，如果给定集合A的一个划分，能否确定一个集合A上的等价关系呢？

7.2 等价关系

定理7.2.3

- 集合A的一个划分可以确定A的一个等价关系！
- 证明：
  - 假定$A = \bigcup A_i, (i = 1,2,\cdots n)$
  - 构造关系R：

$$R = \{(x,y) | \exists A_i, x \in A_i \text{且} y \in A_i\}$$

  - 如果能够证明A上的关系R满足自反性、对称性、传递性，即可说明该关系为等价关系。

第七章 代数结构基本知识

7.1 集合与映射

7.2 等价关系

7.3 代数系统的概念

7.4 同构与同态

7.3 代数系统的概念

定义7.3.1

- 设A是非空集合，A^2到A的一个映射$f: A^2 \to A$称为A的一个二元代数运算，简称二元运算

定义7.3.2

- 设A是非空集合，A^n到A的一个映射$f: A^n \to A$称为A的一个n元代数运算，简称n元运算

7.3 代数系统的概念

定义7.3.3

- 设A是非空集合，$f_1, f_2, \cdots, f_s$分别是A的$k_1, k_2, \cdots k_s$元运算，$k_i (i = 1,2, \cdots s)$是正整数。
- 称集合A和运算$f_1, f_2, \cdots, f_s$所组成的系统为一个代数系统（或一个代数结构），简称为一个代数，用记号$(A, f_1, f_2, \cdots, f_s)$表示。
- 当A是有限集合时，也称该系统是有限代数系统。
- 两要素
  - 集合和代数运算

7.3 代数系统的概念

- 例： $(R, +, \times)$是一个代数系统，其中R为实数集，运算为普通的加法和乘法。
- 例： $(M_n(R), \times)$是一个代数系统，其中$M_n(R)$是全体$n \times n$实矩阵的集合，运算为通常的矩阵乘法。
- 例：设A是一个非空集合，2^A是它的幂集，在2^A中定义二元运算$+$和$\cdot$为

$$B + C = B \cup C, \qquad B \cdot C = B \cap C$$

对于任意$B, C \in 2^A$，$(2^A, +, \cdot)$是一个代数系统

7.3 代数系统的概念

思考：如何判定一个给定的系统是代数系统？

- 集合和代数运算
  - 定义的运算应该满足映射成立条件
  - 所有运算的封闭性

多选题 1分

Setting

下列系统中，是代数系统的有

A $(R, +, \times)$

B $(R - \{0\}, \div)$

C $(R, -)$

D $(N, -)$

Submit

7.3 代数系统的概念

- 例： 给定一个系统，集合$X = \{a, b, c, d\}$，定义二元运算·如下表：

•	a	b	c	d
a	a	b	c	d
b	b	c	b	d
c	c	a	b	c
d	c	a	c	c

7.3 代数系统的概念

- 例： 设$Z_m = \{\bar{0}, \bar{1}, \cdots \overline{m-1}\}$是整数模$m$同余所确定的等价类集合，$Z_m$上的运算+定义如下：

$$\bar{i} + \bar{j} = \overline{(i + j)(\mathrm{mod}\, m)}$$

则$(Z_m, +)$是代数系统！

我们称该运算为模m加法运算。

7.3 代数系统的概念

- 代数系统$(X, \cdot)$中，如果$\forall x_i, x_j \in X$，
- 都有$x_i \cdot x_j = x_j \cdot x_i$成立，
- 则称$(X, \cdot)$对于二元运算·适合交换律。

$(M_n(R), +)$

$(M_n(R), \times)$

结合律

- 代数系统$(X, \cdot)$中，如果$\forall x_i, x_j, x_k \in X$，
- 都有$(x_i \cdot x_j) \cdot x_k = x_i \cdot (x_j \cdot x_k)$成立，
- 则称$(X, \cdot)$对于$\cdot$适合结合律。

$(R, +, \times)$

$(R, -)$

$(R - \{0\}, \div)$

7.3 代数系统的概念

定理7.3.1

- 若$(X, \cdot)$对二元运算·适合结合律，则对于任何正整数m和n，有
  1. $x^m \cdot x^n = x^{m+n}$
  2. $(x^m)^n = x^{m \times n}$

指数律！广义结合律

7.3 代数系统的概念

定理7.3.1

- 证明：

对n进行归纳。当$n=1$时，$x^m \cdot x^n = x^{m+1}$，$(x^m)^1 = x^m$，命题正确；

对所有的$n \le k$，假定$x^m \cdot x^k = x^{m+k}$，$(x^m)^k = x^{mk}$成立，那么当$n = k+1$时，

$$x^m \cdot x^{k+1} = x^m \cdot (x^k \cdot x) = (x^m \cdot x^k) \cdot x = x^{m+k} \cdot x = x^{m+(k+1)}$$

$$(x^m)^{(k+1)} = (x^m)^k \cdot (x^m)^1 = x^{mk} \cdot x^m = x^{mk+m} = x^{m(k+1)}$$

因此定理得证

1. $x^m \cdot x^n = x^{m+n}$
2. $(x^m)^n = x^{m \times n}$

7.3 代数系统的概念

定义7.3.4

- 给定一个代数系统$V=(X,\cdot)$
- 如果$\exists e_L \in X$，使得$\forall x \in X$，都有$e_L \cdot x = x$，则称e_L是X上关于运算$\cdot$的一个左单位元。
- 若e既是左单位元又是右单位元，则称之为单位元。

7.3 代数系统的概念

定理7.3.2

- 若代数系统$V=(X,\cdot)$既有左单位元e_L，又有右单位元e_R，则$e=e_L=e_R$是X的唯一的单位元。
- 证明：
  - 因为e_L是左单位元，故$e_L\cdot e_R=e_R$
  - 又因为e_R是右单位元，故$e_L\cdot e_R=e_L$
  - 所以$e_L=e_R=e$是单位元

代数系统单位元唯一！

7.3 代数系统的概念

- 例：
- $(R, +)$　　单位元是“0”
- $(R, \times)$　　单位元是“1”
- $(R, -)$　　右单位元是“0”

7.3 代数系统的概念

定义7.3.5

- 设$V=(X,\cdot)$是有单位元e的代数系统，对于$x\in X$，
- 若$\exists x'\in X$，使得$x'\cdot x=e$，则称x是左可逆的，并称x'是x的一个左逆元；
- 若$\exists x''\in X$，使得$x\cdot x''=e$，则称x是右可逆的，并称x''是x的一个右逆元；
- 若x既是左可逆的又是右可逆的，则说x是可逆元。

适合结合律的代数系统逆元素唯一！

7.3 代数系统的概念

定理7.3.3 设代数系统$V=(X,\cdot)$具有单位元e，且适合结合律，对于$x\in X$，如果x有左逆元x'，又有右逆元x''，则x有唯一的逆元$x^{-1}=x'=x''$，并且$(x^{-1})^{-1}=x$。

- 证明：

  因为$x'\cdot x=e, x\cdot x''=e$, 所以

  $$x'=x'\cdot e=x'\cdot(x\cdot x'')=(x'\cdot x)\cdot x''=e\cdot x''=x''$$

  假定x有两个逆元a，b，则$x\cdot a=e, b\cdot x=e$, 于是

  $$b=b\cdot e=b\cdot(x\cdot a)=(b\cdot x)\cdot a=e\cdot a=a$$

  因此x^{-1}唯一，又由于$x^{-1}\in X$且有唯一逆元x，又有$x^{-1}\cdot(x^{-1})^{-1}=(x^{-1})^{-1}\cdot x^{-1}=e$，因此$(x^{-1})^{-1}=x$

7.3 代数系统的概念

- 定义：代数系统$V=(X,\cdot)$上的二元运算$\cdot$，如果对$\forall a,b,c\in X$

$$ab=ac \quad \Rightarrow \quad b=c$$
$$ba=ca \quad \Rightarrow \quad b=c$$

运算$\cdot$满足消去律！

代数系统的概念-小结

- 基本概念：
  - 二元运算、n元运算
  - 代数系统定义
  - 代数系统的判定
- 代数系统的运算
  - 结合律、交换律、指数律、消去律
- 代数系统的单位元
- 代数系统中的逆元素

第七章 代数结构基本知识

7.1 集合与映射

7.2 等价关系

7.3 代数系统的概念

7.4 同构与同态

7.4 同构与同态

- 有些代数系统，它们除了元素的名称和运算符号不同以外，在结构上是没有差别的
- 例：

$(\{a,b\}, \bullet)$

$\bullet$	a	b
a	a	b
b	b	a

$(\{0,1\}, \times)$

$\times$	0	1
0	0	1
1	1	0

7.4 同构与同态

定义7.4.1

- 设$V_1 = (X, o_1, o_2, \cdots, o_r)$和$V_2 = (Y, \overline{o_1}, \overline{o_2}, \cdots, \overline{o_r})$是两个代数系统，若$o_i$和$\overline{o_i}$都是$k_i$元运算，且$k_i (i = 1,2, \cdots, r)$是正整数
- 则说代数系统V_1和V_2是同类型的。

7.4 同构与同态

定义7.4.2

- 设$(X, \cdot)$和$(Y, *)$是两个同类型的代数系统，$f: X \to Y$是一个双射。
- 如果$\forall a, b \in X$，恒有$f(a \cdot b) = f(a) * f(b)$
- 则称f是$(X, \cdot)$到$(Y, *)$的一个同构映射，并称$(X, \cdot)$与$(Y, *)$同构，用$X \cong Y$表示。

7.4 同构与同态

例

- $(Z_4, +)$是一个代数系统，其中$Z_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$是整数模4同余所确定的等价类集合，$Z_4$上的运算+定义如下：$\bar{i} + \bar{j} = \overline{(i + j)(\mathrm{mod}\, 4)}$
- 其运算表是：

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

7.4 同构与同态

- 另外设$Y=\{a,b,c,d\}$，并定义Y上的运算如下：

·	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

- $(Y,\cdot)$与$(Z_4,+)$是同类型的代数系统。现定义$f:Z_4\to Y$如下：$f:\ \bar{0}\to a,\bar{1}\to b,\bar{2}\to c,\bar{3}\to d$，可以判断f是同构映射，因此$Z_4\cong Y$

7.4 同构与同态

定义7.4.3

- 设$(X, \cdot)$和$(Y, *)$是两个同类型的代数系统，$f: X \to Y$是一个映射。
- 如果$\forall a, b \in X$，恒有$f(a \cdot b) = f(a) * f(b)$
- 则称f是$(X, \cdot)$到$(Y, *)$的一个同态映射，简称同态。

7.4 同构与同态

例

- 一个代数系统$V_1 = (Z, +, \times)$，其中Z是整数集合，$+$ 和 $\times$分别是一般的加法和乘法运算；另一个代数系统$V_2 = (Z_m, +_m, \times_m)$中，$Z_m = \{\bar{0}, \bar{1}, \cdots, \overline{m-1}\}$，其中$+_m$和 $\times_m$ 分别是模m的加法和乘法运算，即

$$\bar{x}_1 +_m \bar{x}_2 = \overline{x_1 + x_2}$$

$$\bar{x}_1 \times_m \bar{x}_2 = \overline{x_1 \times x_2}$$

- 定义映射$f: Z \to Z_m$，即$f(i) = \bar{i}$，则f是V_1到V_2的一个同态

7.4 同构与同态

问题：

- 如果给定一个映射$f: X \to Y$是从代数系统$(X, \cdot)$到$(Y, *)$的一个同态，则必定有$f(X) \subseteq Y$
- 那么，$f(X)$和运算$*$是否能够构成一个代数系统？

- 定义7.4.4 设$(X, \cdot)$是一个代数系统，R是X的一个非空子集，如果R在运算$\cdot$下是封闭的，则称$(R, \cdot)$是$(X, \cdot)$的一个子代数系统或子代数。

7.4 同构与同态

定理7.4.1

- 设映射$f: X \to Y$是从代数系统$(X, \cdot)$到$(Y, *)$的一个同态，则$(f(x), *)$是$(Y, *)$的一个子代数，并称它是在f作用下$(X, \cdot)$的同态象。
- $f(x)$是非空的，证明$f(X)$ 对于运算$*$的封闭性：
  - 由于f是X到Y的映射，故$f(X) \subseteq Y$。设任意元$y_1, y_2 \in f(X)$，则一定存在$x_1, x_2 \in X$, 使$f(x_1) = y_1, f(x_2) = y_2$
  - 因为$(X, \cdot)$是代数系统，则$x_1 \cdot x_2 = x_3 \in X$。因此$y_1 * y_2 = f(x_1) * f(x_2) = f(x_1 \cdot x_2) = f(x_3) \in Y$
  - 即$f(X)$对于运算$*$是封闭的，定理得证

7.4 同构与同态

定义7.4.5

- 设映射$f: X \to Y$是从代数系统$(X, \cdot)$到$(Y, *)$的一个同态，如果：
  1. f是单射，则称f为单一同态
  2. f是满射，则称f是满同态，用$X \sim Y$表示，并称Y是X的一个同态象。

7.4 同构与同态

定理7.4.2

- 给定代数系统$(X, \cdot)$到$(Y, *)$，其中$\cdot$和$*$都是二元运算。
- 设$f: X \to Y$是$(X, \cdot)$到$(Y, *)$的满同态，则
  - 如果$\cdot$是可交换的或可结合的运算，则$*$也是可交换的或可结合的运算。
  - 若$(X, \cdot)$中运算$\cdot$具有单位元e，则$(Y, *)$中运算$*$具有单位元$f(e)$。
  - 对运算$\cdot$，如果每一个元素$x \in X$都有逆元x^{-1}，则对运算$*$，每一个元素$f(x) \in Y$都具有逆元$f(x^{-1})$。

7.4 同构与同态

定理7.4.2 证明

- 代数系统$(X, \cdot)$和$(Y, *)$
  - 因为$f: X \to Y$是满同态，所以能把Y中的每个元写成$f(x)$的形式。如果运算$\cdot$是可交换的或可结合的，则容易证明运算$*$也是可交换的和可结合的。

    证明过程很简单，可以参加教材。
  - 对运算$\cdot$来说，设e是单位元，$e \in X$, 则对任意$f(x) \in Y$，有 $f(x) * f(e) = f(x \cdot e) = f(x)$

    $f(e) * f(x) = f(e \cdot x) = f(x)$

    因此运算$*$ 具有单位元$f(e)$

7.4 同构与同态

定理7.4.2 证明(接上页)

- 代数系统$(X, \cdot)$和$(Y, *)$
  - 同理，设x是X中的任意元，x^{-1}是x关于运算·的逆元，显然$x^{-1} \in X$，对任意$f(x) \in Y$，有

$$f(x) * f(x^{-1}) = f(x \cdot x^{-1}) = f(e)$$

$$f(x^{-1}) * f(x) = f(x^{-1} \cdot x) = f(e)$$

因此$f(x^{-1})$是$f(x)$的逆元

代数系统所适合的一些运算性质，如结合律、交换律、单位元、可逆元等，在满同态映射所构造的任何代数系统（满同态象和同构象）中都能完整地保持下来

7.4 同构与同态

定义7.4.6

- 代数系统$(X, \cdot)$上的同态映射

$$f: X \to X$$

- 称为自同态，若f是同构映射，则称之为自同构。

同构与同态-小结

- 基本概念：
  - 同类型代数系统
  - 同构、同态
  - 子代数系统
  - 单一同态、满同态
  - 自同态、自同构
- 满同态基本性质

第八章 群

8.1 半群

8.2 群、群的基本性质

8.3 循环群 群的同构

8.4 变换群和置换群 Cayley定理

8.5 陪集和群的陪集分解 Lagrange定理

8.6 正规子群与商群

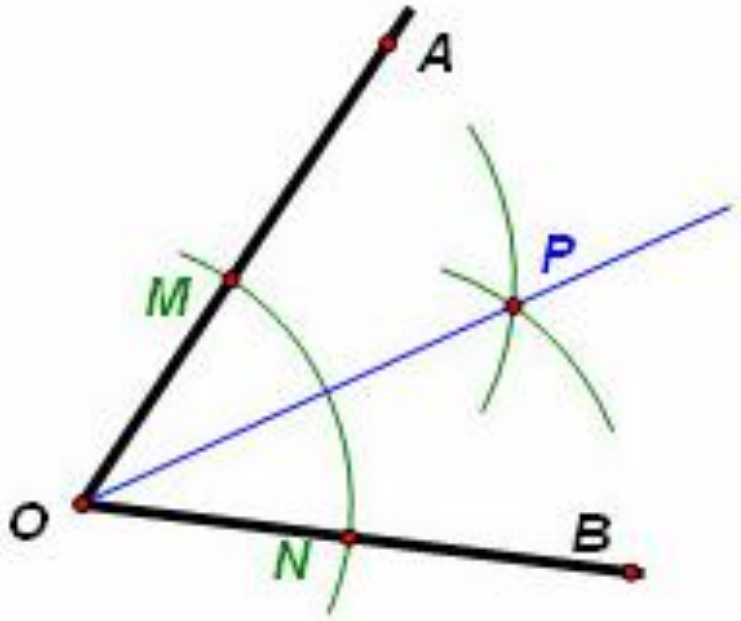
8.7 群的同态、同态基本定理

8.8 群的直积

研究起源

- **群论**的研究起源于19世纪，它是由于方程论的需要，首先作为置换群的理论发展起来的。
- 随后，发现在大多数问题中，重要的不是构成群的置换本身，而应该是集合在代数运算下的性质，因而提出了群的概念。

尺规作图：任意角二等分



尺规作图问题

- 在历史上，限用圆规直尺的古希腊四大几何作图难题（将任意角三等分、倍立方、化圆为方、作正n边形）一直引起无数数学家和数学爱好者的浓厚兴趣，2000多年来，曾有无数人将自己的聪明才智倾注在这些难题上，但未得到丝毫结果，其原因就是缺乏一些新的工具
- 直到伽罗华引入了置换群，创立了抽象代数学，这些难题是否可解才得到圆满可解
- 本课程学习的知识还无法完全解决这个问题，需要学习域，域的扩张的知识

8.1 半群

定义8.1.1

- 设S是非空集合，$\cdot$是S上的一个二元运算，如果$\cdot$满足结合律，则代数系统 $(S,\cdot)$ 称为半群(semigroup)。
- 换句话说，如果对于任意的$a,b,c \in S$，若$(a \cdot b) \cdot c = a \cdot (b \cdot c)$成立，则称$(S,\cdot)$为半群。

封结

8.1 半群

- 例： $(R, +)$

  $\forall a, b, c \in R \qquad (a + b) + c = a + (b + c)$

半群！

- 例： $(R, -)$

  $\forall a, b, c \in R \qquad (a - b) - c \neq a - (b - c)$

8.1 半群

- 例： $(M_n(R),\times)$

  其中$M_n(R)$是全体$n \times n$实矩阵的集合

  $\forall A,B,C \in M_n(R) \qquad (A \times B) \times C = A \times (B \times C)$

  半群！

- 例：$(Z_m,\cdot)$

  设$Z_m = \{\overline{0},\overline{1},\cdots,\overline{m-1}\}$是模$m$同余的等价类集合，$\cdot$是$Z_m$上的模$m$加法运算

  半群！

8.1 半群

定义8.1.2

- 若半群$(M,\cdot)$中有单位元e存在，则称$(M,\cdot)$是一个含幺半群或简称幺群。
- 幺群有时会用三元组$(M,\cdot,e)$表示，方便起见，简称M为幺群，并常用ab表示$a\cdot b$，称为a与b的乘积。

- 例：$(R,+)$

$$\forall a,b,c\in R \qquad (a+b)+c=a+(b+c)$$

$$\forall a\in R \qquad a+0=0+a=a$$

半群！　　幺群！　　**封结幺**

8.1 半群

- 例： $(M_n(R),\times)$

  其中$M_n(R)$是全体$n \times n$实矩阵的集合

  $\forall A,B,C \in M_n(R) \qquad (A \times B) \times C = A \times (B \times C)$

  半群！　　幺群！

- 例：$(Z_m,\cdot)$

  设$Z_m = \{\overline{0},\overline{1},\cdots,\overline{m-1}\}$是模$m$同余的等价类集合，$\cdot$是$Z_m$上的模$m$加法运算

  半群！　　幺群！

8.1 半群

定义8.1.3

- 设$(M,\cdot,e)$是一个幺群，若$\cdot$适合交换律，则称M是交换幺群。

- 例：$(R,+)$

$$\forall a,b,c \in R \qquad (a+b)+c=a+(b+c)$$

$$\forall a \in R \qquad a+0=0+a=a$$

半群！　　幺群！　　交换幺群！

8.1 半群

- 例： $(M_n(R),\times)$

  其中$M_n(R)$是全体$n \times n$实矩阵的集合

  $\forall A,B,C \in M_n(R) \qquad (A \times B) \times C = A \times (B \times C)$

  半群！　　幺群！

- 例：$(Z_m,\cdot)$

  设$Z_m = \{\overline{0},\overline{1},\cdots,\overline{m-1}\}$是模$m$同余的等价类集合，$\cdot$是$Z_m$上的模$m$加法运算

  半群！　　幺群！　　交换幺群！

多选题 1分

设置

$(Z_m,\cdot)$ 设$Z_m=\{\overline{0},\overline{1},\cdots,\overline{m-1}\}$是模$m$同余的等价类集合，$\cdot$是$Z_m$上的模$m$加法运算

A 半群

B 幺群

C 交换幺群

D 都不是

提交

8.1 半群

- **定理8.1.1**：如果二元运算·适合结合律，那么也适合广义结合律。
  - 根据定理显见

$$a^n a^m = a^{n+m} \qquad (a^m)^n = a^{mn}$$

其中定义$a^0 = e$，即M中的单位元。

  - 如果a是M中的一个可逆元，那么一定有$a^{-1} \in M$，于是$a^{-1}a^{-1}\cdots a^{-1}$(n个)可以表示成

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

因此上式中的m, n在整数范围内取值都是成立的。

若a可逆，则a^n也可逆

8.1 半群

- **定义8.1.4**：设$(M,\cdot,e)$是一个幺群，若存在一个元素$g \in M$，使得任意的$a \in M$，a都可以写成g的方幂形式，即$a = g^m$（m是非负整数），则称$(M,\cdot,e)$是一个循环幺群，并且称g是M的一个生成元。

- 例：　$(R,+)$

$$\forall a,b,c \in R \qquad (a+b)+c = a+(b+c)$$

$$\forall a \in R \qquad a+0 = 0+a = a$$

半群！　幺群！交换幺群！循环幺群？　×

- 例：　$(N,+)$

循环幺群？　　√

8.1 半群

- 例：$(Z_m,\cdot)$　　设$Z_m=\{\overline{0},\overline{1},\cdots,\overline{m-1}\}$是模$m$同余的等价类集合，$\cdot$是$Z_m$上的模$m$加法运算

半群！　么群！　交换群！循环么群！

- $<P(B),\oplus>$，其中$\oplus$为集合对称差运算

半群、么群、交换么群

- $<Z_m,.>$，其中$Z_m=\{\overline{0},\overline{1},\cdots,\overline{m-1}\}$，.为模$m$加法

半群、么群、交换么群，循环么群

8.1 半群

定理8.1.2 循环幺群是可交换幺群

- 证明：

  设g是循环幺群中的一个生成元，则对任意$a, b \in M$，有$a = g^m, b = g^n, (m, n \geq 0)$

  由于二元运算适合结合律，因此

  $$ab = g^m g^n = g^{m+n} = g^n g^m = ba$$

  所以循环幺群是可交换的。

8.1 半群

定义8.1.5

- 设$(S,\cdot)$是一个半群，$T \subseteq S$，在运算$\cdot$的作用下如果T是封闭的，则称$(T,\cdot)$是$(S,\cdot)$的子半群。

定义8.1.6

- 设$(M,\cdot,e)$是一个幺群，$T \subseteq M$，在运算$\cdot$的作用下如果T是封闭的，且$e \in T$，则称$(T,\cdot,e)$是$(M,\cdot,e)$的子幺群。

8.1 半群

- 定义8.1.7：设$(A,\cdot)$、$(B,*)$是两个半群。$f:A\to B$是A到B的映射，$\forall a,b\in A$,若$f(a\cdot b)=f(a)*f(b)$成立，则称f是从半群A到半群B的同态映射，简称同态。若f分别是单射、满射和双射时，分称f是单同态、满同态和同构。

- **例**：$(R,+,0)$和$(C^*,\cdot,1)$是两个幺群。其中R是实数集，C^*是非0复数集合，令$f:\theta\to e^{i\theta}$，则对任意的$a,b\in R$有

$$f(a+b)=e^{i(a+b)}=e^{(ia+ib)}=e^{ia}\cdot e^{ib}=f(a)\cdot f(b)$$

- 因此f是R到C^*的同态。

8.1 半群

定理8.1.3

- 设f是从代数系统$(A,\cdot)$到$(B,*)$的满同态，S是A的非空子集。$f(S)$表示S中的元素在f下的象的集合，即$f(S)=\{f(a)|a\in S\}$
- 那么
  1. 若$(S,\cdot)$是半群，则$(f(S),*)$也是半群。
  2. 若$(S,\cdot)$是幺群，则$(f(S),*)$也是幺群。

8.1 半群

定理8.1.3 证明 **封**

- $f(S)$是非空的
- 首先证明$f(S)$对运算$*$是封闭的。
- 任取$a', b', c' \in f(S)$,有$a, b, c \in S$,使得$f(a) = a', f(b) = b', f(c) = c'$
- f是同态，因此$a' * b' = f(a) * f(b) = f(a \cdot b)$
- 因S是半群，满足封闭性，所以$a \cdot b \in S, f(a \cdot b) \in f(S)$
- 即$a' * b' \in f(S)$，所以$f(S)$对于运算$*$是封闭的

8.1 半群

定理8.1.3 证明（cont.）

封结幺

- 再证明$*$在$f(S)$上适合结合律

$$a'*(b'*c')=f(a)*(f(b)*f(c))=f(a)*f(b\cdot c)=f(a\cdot(b\cdot c))$$
$$(a'*b')*c'=(f(a)*f(b))*f(c)=f(a\cdot b)*f(c)=f((a\cdot b)\cdot c)$$

- 上两式相等，所以$*$在$f(S)$上适合结合律
- 因此，$(f(S),*)$是半群
- 第二部分（若$(S,\cdot)$是幺群，则$(f(S),*)$也是幺群）
- 只需证明$e'=f(e)$是$f(S)$的单位元即可

8.1 半群

推论

- 设f是从半群$(A,\cdot)$到代数系统$(B,*)$的满同态，$(S,\cdot)$是$(A,\cdot)$的子半群。
- 则有
  1. $(B,*)$是半群。
  2. $(f(S),*)$是$(B,*)$的子半群。

半群、幺群、子半群的同态象，仍然是半群、幺群、子半群！

常用代数系统的比较

- 小结

封

封结

封结幺

封结幺逆

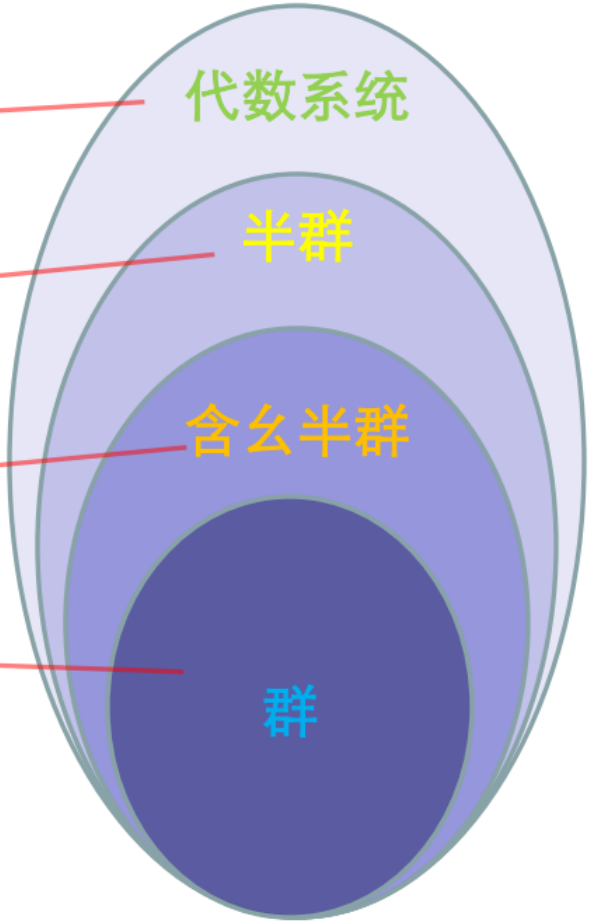
凤姐咬你

非空集合+代数运算

非空集合+代数运算+结合律

非空集合+代数运算+结合律+单位元

非空集合+代数运算+结合律+单位元+逆元



谢谢

shixia@tsinghua.edu.cn