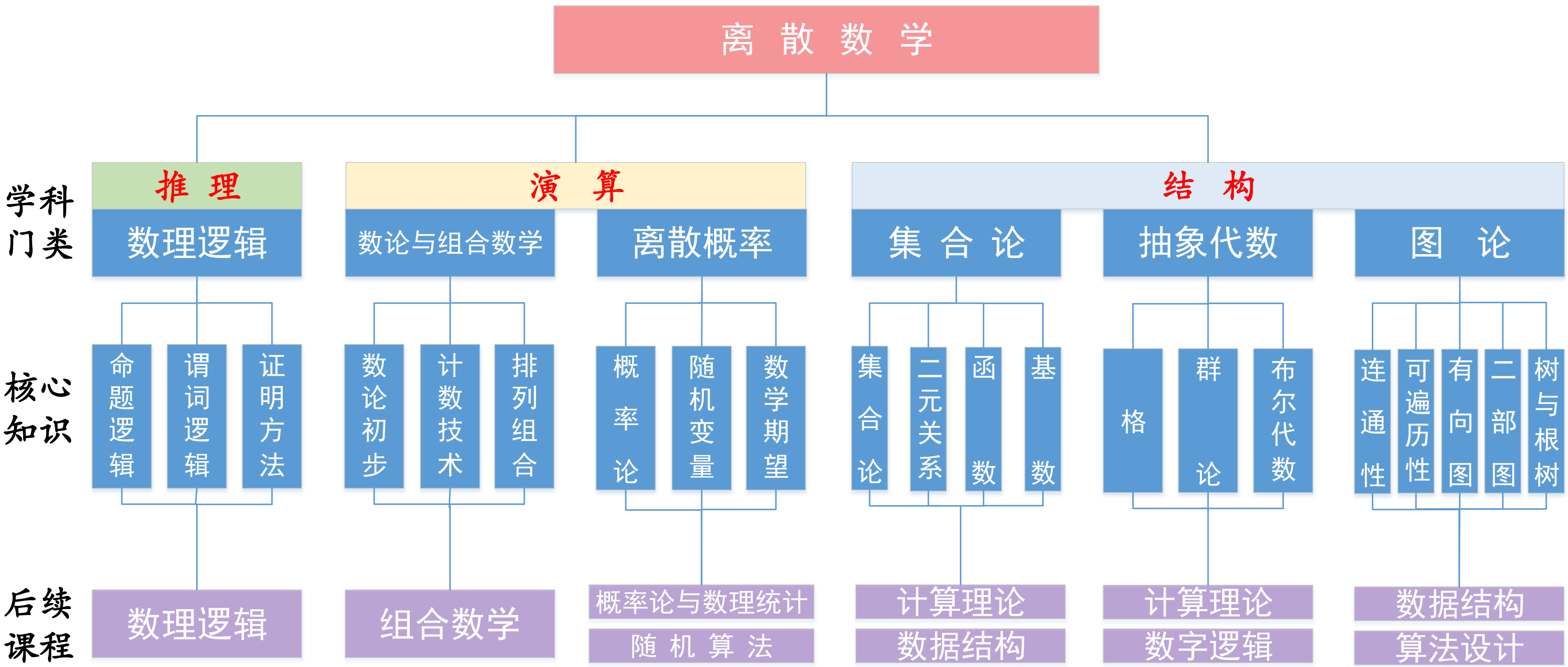
离散数学·习题课
Discrete Mathematics

第三十讲：总复习与核心知识串讲

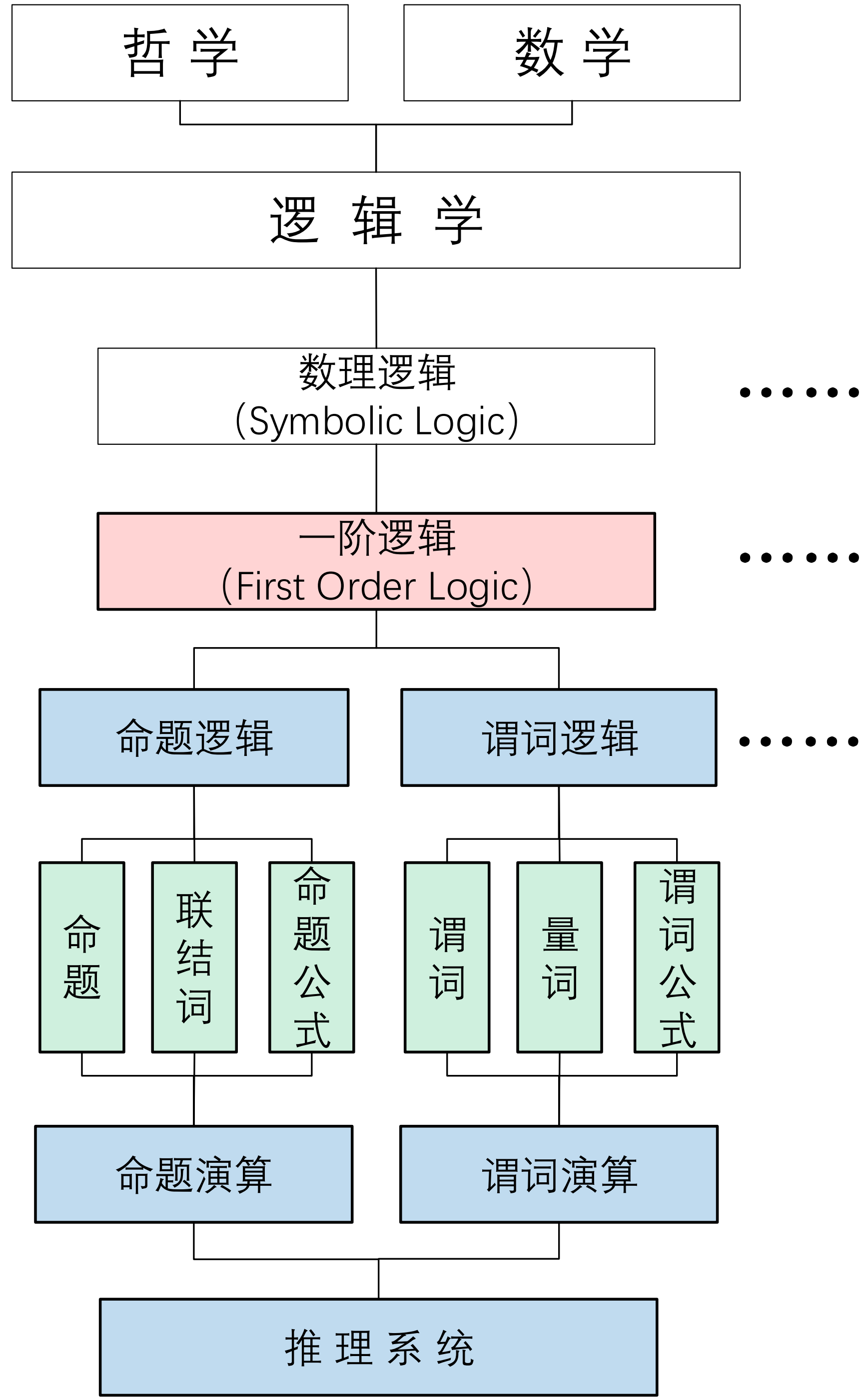
吴 楠
南京大学计算机科学与技术系

2017 年 6 月 22 日

本课程核心内容总体框图



逻辑初步部分总框图


哲 学
数 学
逻 辑 学
数理逻辑
(Symbolic Logic)
一阶逻辑
(First Order Logic)
命题逻辑
谓词逻辑
命题
联结词
命题公式
谓词
量词
谓词公式
命题演算
谓词演算
推 理 系 统

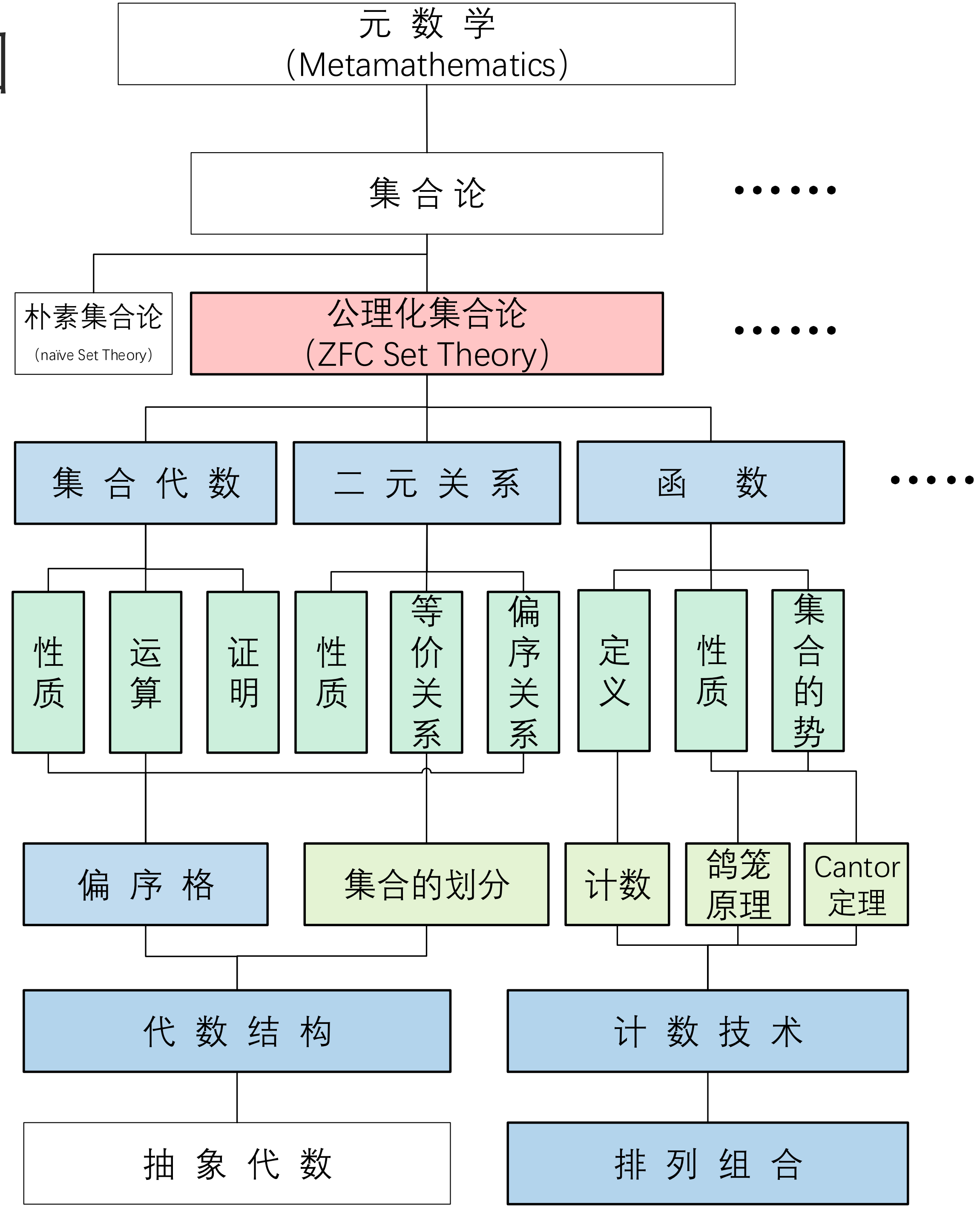
逻辑初步部分内容提要（续）

- 命题逻辑与一阶谓词逻辑初步：
  - 命题为可判断真假的陈述句，真值可变之陈述句为命题变元
  - 命题可通过否定、合取、析取、蕴含、等价等联结词扩展为更复杂的命题，任何命题逻辑公式可化为范式
  - 真值表可用于命题逻辑等值式的证明
  - 谓词描述某对象的某种属性，对象用谓词变元描述
  - 使用量词可更精确地约束谓词的适用范围：∀, ∃
  - 命题逻辑与谓词逻辑的推理规则

证明理论部分内容提要

- 证明理论与常用的证明方法：
  - 证明的本质是保证真实性，数学证明的推理方式是演绎推理，推理出的结果（逻辑推论）称为定理
  - 数学证明的一般形式是在ZFC公理体系下证明$\boldsymbol{A_1} \wedge \boldsymbol{A_2} \wedge \cdots \wedge \boldsymbol{A_k} \rightarrow \boldsymbol{B}$ 永真
  - 常用的证明方法包括：
    - 直接证明法，间接证明法
    - 归谬法（反证法），穷举法
    - 空证明法，平凡证明法
    - 构造性证明法，反例证明法

集合论部分总框图


元 数 学
(Metamathematics)
集 合 论
……
朴素集合论
(naïve Set Theory)
公理化集合论
(ZFC Set Theory)
……
集 合 代 数
二 元 关 系
函 数
……
性质
运算
证明
性质
等价关系
偏序关系
定义
性质
集合的势
偏 序 格
集合的划分
计数
鸽笼原理
Cantor定理
代 数 结 构
计 数 技 术
抽 象 代 数
排 列 组 合

集合论部分内容提要

- 集合代数：
  - 集合三特性：确定性、互异性、无序性
  - 集合的外延原则（集合相等）与概括原则（集合的谓词描述）
  - 集合的构成限制（罗素悖论）
  - 子集、空集与幂集
  - 集合的并（∪）、交（∩）、相对补（−）、绝对补（$\overline{\quad}$）、对称差（⊕）、广义交与广义并等运算
  - 交换律、结合律、分配律、De Morgan律等
  - 集合相等的基本证明方式

集合论部分内容提要（续）

- 二元关系的性质：
  - 自反性：$\forall x(x \in A \rightarrow \langle x,x\rangle \in R)$
  - 反自反性：$\forall x(x \in A \rightarrow \langle x,x\rangle \notin R)$
  - 对称性：$\forall x \forall y(x,y \in A \land \langle x,y\rangle \in R \rightarrow \langle y,x\rangle \in R)$
  - 反对称性：$\forall x \forall y(x,y \in A \land \langle x,y\rangle \in R \land \langle y,x\rangle \in R \rightarrow x = y)$
  - 传 递 性 ： $\forall x \forall y \forall z(x,y,z \in A \land \langle x,y\rangle \in R \land \langle y,z\rangle \in R \rightarrow \langle x,z\rangle \in R)$

集合论部分内容提要（续）

- **等价关系与划分：**
  - 等价关系：非空集合上的关系R，若其是自反的、对称的和传递的，则R为该集合上的一个等价关系
  - 等价类：若R为非空集合上的等价关系，$\forall x \in A, [x]_R = \{y | y \in A \wedge xRy\}$，则称$[x]_R$为$x$为关于$R$的等价类
  - 商集：$A/R = \{[x]_R | x \in A\}$
  - 集合的划分：与集合上的等价关系一一对应

集合论部分内容提要（续）

- 关系的闭包：
  - 自反闭包：$r(R) = R \cup R^0$
  - 对称闭包：$s(R) = R \cup R^{-1}$
  - 传递闭包：$t(R) = R \cup R^2 \cup R^3 \cup \cdots$
  - 等价闭包：$tsr(R) = t\left(s\left(r(R)\right)\right)$
  - 三种闭包的关系矩阵求法：
    - $\boldsymbol{M}_r = \boldsymbol{M} + \boldsymbol{E}$　$\boldsymbol{M}_s = \boldsymbol{M} + \boldsymbol{M}^T$　$\boldsymbol{M}_t = \boldsymbol{M} + \boldsymbol{M}^2 + \boldsymbol{M}^3 + \cdots$
  - 传递闭包的Warshall算法

集合论部分内容提要（续）

- 函数的概念：
  - 设F为二元关系，若$\forall x \in \mathrm{dom}\,F$皆有唯一的$y \in \mathrm{ran}\,F$使得$xFy$成立，则称$F$为函数，记作$y = F(x)$
  - $F = G \Leftrightarrow F \subseteq G \wedge G \subseteq F$
  - 设A, B为集合，f为函数，且$\mathrm{dom}\,f = A, \mathrm{ran}\,f \subseteq B$，称$f$为从$A$到$B$的函数，记作$f: A \to B$
  - 从A到B的全体函数的集合称为“B上A”，记为$B^A = \{f \mid f: A \to B\}$，若$|B| = m, |A| = n$，则$|B^A| = m^n$

集合论部分内容提要（续）

- 函数的性质
  - $f: A \to B$ 是满射的 $\Leftrightarrow \operatorname{ran} f = B$
  - $f: A \to B$ 是单射的 $\Leftrightarrow \forall x_1 \forall x_2 \big(x_1, x_2 \in A \land x_1 \neq x_2 \to f(x_1) \neq f(x_2)\big)$

    $\Leftrightarrow \forall x_1 \forall x_2 (x_1, x_2 \in A \land f(x_1) = f(x_2) \to x_1 = x_2)$
  - $f: A \to B$ 是双射的 $\Leftrightarrow f$ 是单射的且是满射的
- 函数的复合
- 反函数
  - 只有双射函数才可定义反函数

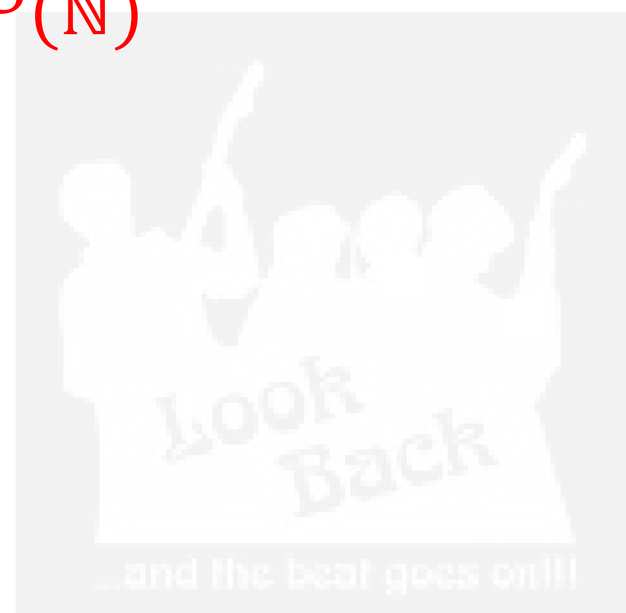
集合的势部分内容提要

等势与优势的概念：

- 设A, B为集合，若存在从A到B的双射函数，则称集合A与集合B等势，记为$A \approx B$。如果A不与B等势，则记做$A \not\approx B$；等势关系是等价关系
  - 双射函数的构造技巧
- 设A, B为集合，若存在从A到B的单射函数，则称集合B优势于集合A，记做$A \preccurlyeq\cdot B$；$A \prec\cdot B \Leftrightarrow A \preccurlyeq\cdot B \wedge A \not\approx B$
- Cantor定理：$\mathbb{N} \prec\cdot \mathbb{R}$，任意集合$A \prec\cdot \mathcal{P}(A)$

集合的势部分内容提要（续）

- 几个重要的等势与优势关系：
  - $\mathbb{N} \approx \mathbb{Z} \approx \mathbb{Q} \approx \mathbb{N} \times \mathbb{N}$
  - $\mathbb{R} \approx [a, b] \approx (c, d) \approx \{0,1\}^{\mathbb{N}} \approx \mathcal{P}(\mathbb{N})$
  - $\{0,1\}^{A} \approx \mathcal{P}(A)$
- 有穷集合的基数：
  - $\mathrm{card}(A) = n \Leftrightarrow A \approx n$
  - $\mathrm{card}(A)$亦可记为$|A|$



集合的势部分内容提要（续）

- 无穷集合的基数：
  - $\mathrm{card}(\mathbb{N}) = \aleph_0$
  - $\mathrm{card}(\mathbb{R}) = \aleph$
  - $\aleph_0 < \aleph$
- 可列集：
  - $\aleph_0$是最小的无穷基数
  - 设集合A，若$\mathrm{card}(A) \le \aleph_0$，则称$A$为可列集

集合的势部分内容提要（续）

- 排列组合
  - 加法原理与乘法原理
  - 排列与组合
  - 环排列
  - 不可区分元素的排列与有重复的组合
- 鸽笼原理

数论初步部分内容提要

- 整数与整数集的性质
  - 质数：性质、求法、互质
  - 算术基本定理：每个大于1的整数皆可分解为有限个质数之积，不考虑顺序的情况下分解唯一
  - 最大公约数：$a, b \in \mathbb{Z}^+, (\exists s, t \in \mathbb{Z})(\gcd(a, b) = sa + tb)$
  - 有理数：$q \in \mathbb{Q} \Leftrightarrow q = \frac{b}{a} \wedge (a, b) = 1$
  - 欧拉函数：$\varphi(n) = |\{m \in \mathbb{Z}^+ | m \leq n \wedge (m, n) = 1\}|$
  - 欧拉定理与费马小定理：$a, n, p \in \mathbb{Z}^+$,
    - $(a, n) = 1 \rightarrow a^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n)$
    - p为质数 $\wedge\, p \nmid a \rightarrow a^{p-1} \equiv 1 (\mathrm{mod}\, p)$

数论初步部分内容提要（续）

- 整数的运算：
  - 整除
  - 模
    - $(a+b) \bmod d = (a \bmod d + b \bmod d) \bmod$
    - $(a \times b) \bmod d = [(a \bmod d)(b \bmod d)] \bmod d$
  - 同余
    - $a \equiv b(\bmod m) \Leftrightarrow (\exists m \in \mathbb{Z}^{+})(m|(a-b))$
  - 中国剩余定理

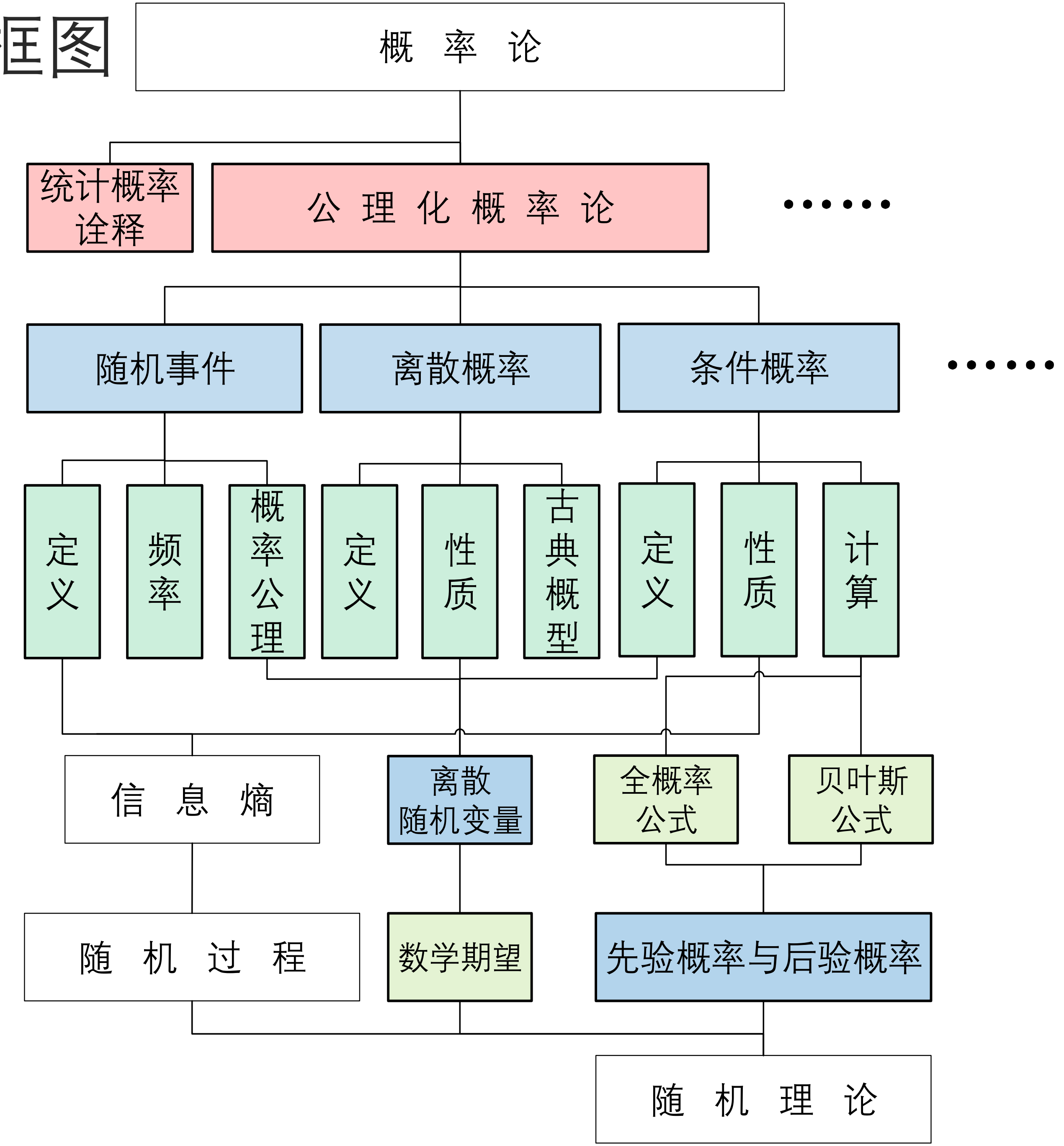
数论初步部分内容提要（续）

- 数学归纳法与递归结构：
  - 数学归纳法
    - 理论：$\boldsymbol{P}(1), \forall x\left(\boldsymbol{P}(x) \rightarrow \boldsymbol{P}(x+1)\right) \Longrightarrow \forall x \boldsymbol{P}(x)$
    - 方法：奠基、归纳基础、归纳步骤、结论
  - 强数学归纳法
    - 理论：$\boldsymbol{P}(1), \forall x\left(\forall y < x, \boldsymbol{P}(y) \rightarrow \boldsymbol{P}(x)\right) \Rightarrow \forall x \boldsymbol{P}(x)$
    - 方法：奠基、归纳基础、归纳步骤、结论

数论初步部分内容提要（续）

- 数学归纳法与递归结构（续）：
  - 递归集合定义
    - 方法：奠基、归纳步骤（产生规则）、排斥规则
  - 结构归纳法
    - 理论：递归集合定义、数学归纳法
    - 方法：奠基（检查基础元素）、归纳步骤（针对产生规则证明新元素也符合谓词）、结论

离散概率部分总框图


概 率 论
统计概率诠释
公 理 化 概 率 论
……
随机事件
离散概率
条件概率
……
定义
频率
概率公理
定义
性质
古典概型
定义
性质
计算
信 息 熵
离散随机变量
全概率公式
贝叶斯公式
随 机 过 程
数学期望
先验概率与后验概率
随 机 理 论

离散概率部分内容提要

- 随机现象与随机试验
- 样本空间与随机事件
  - 基本事件（样本点）、样本空间、复杂事件
- 随机事件与集合代数
- 频率与概率的统计诠释
- 统计诠释概率的性质

离散概率部分内容提要（续）

- 概率的公理化定义
  - 非负性、规范性、可列可加性公理
- 离散概率
  - 样本空间为离散样本空间，概率函数p满足：
    - (1) $\forall \omega \in \Omega, 0 \le p(\omega) \le 1$;
    - (2) $\sum_{\omega \in \Omega} p(\omega) = 1$.
  - 事件A的离散概率规定为$P(A) = \sum_{\omega \in A} p(\omega)$

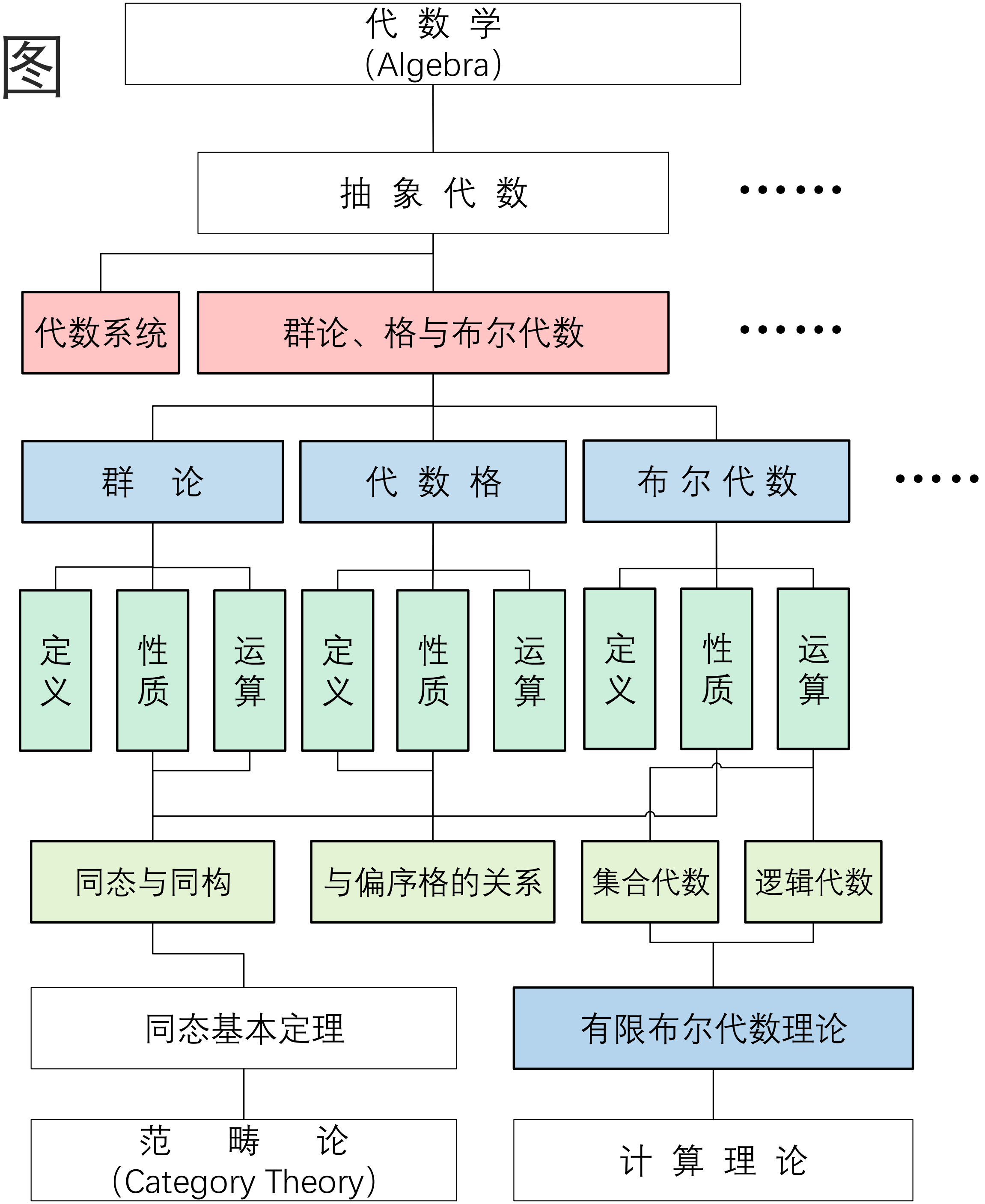
离散概率部分内容提要（续）

- 条件概率
  - $P(A|B)=\dfrac{P(AB)}{P(B)}$
- 贝叶斯公式
  - $P(B_i|A)=\dfrac{P(B_i)P(A|B_i)}{\sum_{j=1}^{n}P(B_j)P(A|B_j)}$
- 先验概率与后验概率
- 独立事件： $P(AB)=P(A)P(B)$

离散概率部分内容提要（续）

- 离散随机变量
- 离散随机变量的概率分布
- 离散随机变量的数学期望
  - 定义在样本空间$\boldsymbol{\Omega}$上的一个随机变量X的数学期望为 $E(X)=\sum_{s\in\boldsymbol{\Omega}}p(X=s)X(s)$
  - 数学期望的线性特征：对于任意离散随机变量$X_i\ (i=1,2,\cdots,n)$及任意$a,b\in\mathbb{R}$，有：$E(X_1+X_2+\cdots+X_n)=E(X_1)+E(X_2)+\cdots+E(X_n)$

代数系统部分总框图


代 数 学
(Algebra)
抽 象 代 数
……
代数系统
群论、格与布尔代数
……
群 论
代 数 格
布 尔 代 数
……
定义
性质
运算
定义
性质
运算
定义
性质
运算
同态与同构
与偏序格的关系
集合代数
逻辑代数
同态基本定理
有限布尔代数理论
范 畴 论
(Category Theory)
计 算 理 论

代数系统部分内容提要

- 二元运算和一元运算的概念：
  - 设S为集合，函数$f: S \times S \to S$称为集合S上的二元运算
  - 设S为集合，函数$f: S \to S$称为集合S上的一元运算

- 二元运算与一元运算的算符及表示法：
  - 算符：$\circ$, $*$, $\cdot$, Δ, $\diamond$ 等
  - 表示法：表达式或者运算表

代数系统部分内容提要（续）

二元运算的性质与特异元素：

- 交换律：$\forall x,y \in S, x \circ y = y \circ x$
- 结合律：$\forall x,y,z \in S, (x \circ y) \circ z = x \circ (y \circ z)$
- 幂等律：$\forall x \in S, x \circ x = x$
- 消去律：$\forall x,y \in S, x \circ y = x \circ z \wedge x \neq \theta \Rightarrow y = z$（左消去律）

  $y \circ x = z \circ x \wedge x \neq \theta \Rightarrow y = z$（右消去律）
- 分配律：$\forall x,y,z \in S, x \circ (y * z) = (x \circ y) * (x \circ z), (y * z) \circ x = (y \circ x) * (z \circ x)$
- 吸收律：$\circ$与$*$可交换，$\forall x,y \in S, x \circ (x * y) = x * (x \circ y) = x$
- 单位元e：$\forall x \in S, x \circ e = e \circ x = x$
- 零元θ：$\forall x \in S, x \circ \theta = \theta \circ x = \theta$
- 幂等元x：$\forall x \in S, x \circ x = x$
- 可逆元x及其逆元素x^{-1}：$x \circ x^{-1} = x^{-1} \circ x = e$

代数系统部分内容提要（续）

- 二元运算中的重要定理：
  - 单位元如果存在则唯一
  - 零元如果存在则唯一
  - 如果$|S| > 1$，则单位元不等于零元
  - 对于可结合的二元运算，可逆元素x只有唯一的逆元x^{-1}

代数系统部分内容提要（续）

- 代数系统的相关概念：
  - 非空集合S与在S上封闭的k个一元或二元运算$f_1, f_2, \cdots, f_k$组成的系统称为代数系统，记为$\langle S, f_1, f_2, \cdots, f_k \rangle$
  - 设$V = \langle S, f_1, f_2, \cdots, f_k \rangle$是代数系统，$B \subseteq S$，若运算$f_1, f_2, \cdots, f_k$对$B$均封闭，且$B$和$S$含有相同的代数常数，则称$\langle S, f_1, f_2, \cdots, f_k \rangle$为代数$V$的子代数

代数系统部分内容提要（续）

- 代数系统的同构与同态：
  - 设$V_1 = \langle A,\circ \rangle$，$V_2 = \langle B,* \rangle$是同类型的代数系统，若存在**双射函数**$f: V_1 \rightarrow V_2$使得$\forall x, y \in A, f(x \circ y) = f(x) * f(y)$，则称$f$是$V_1$到$V_2$的同构映射，简称$V_1$与$V_2$同构（isomorphism）
  - 设$V_1 = \langle A,\circ \rangle$，$V_2 = \langle B,* \rangle$是同类型的代数系统，若存在函数$f: V_1 \rightarrow V_2$使得$\forall x, y \in A, f(x \circ y) = f(x) * f(y)$，则称$f$是$V_1$到$V_2$的同态映射，简称$V_1$与$V_2$同态（homomorphism）；特别地，若上述映射f是满射，则称V_1与V_2满同态（epimorphism）

格与布尔代数部分内容提要

- 格的概念：
  - 偏序关系与哈斯图
  - 格的偏序定义：设$\langle S, \preccurlyeq \rangle$为偏序集，若$\forall x, y \in S$，$\{x, y\}$均有上确界和下确界，则$S$关于偏序$\preccurlyeq$构成格（即偏序格）
  - 格的代数定义：代数系统$\langle S, *, \circ \rangle$对于$*$和$\circ$适合交换律、结合律、吸收律，则该系统构成格（即代数格）

格与布尔代数部分内容提要

- 偏序格与代数格的对应关系：

$$\langle L, \preccurlyeq \rangle$$

$$\Downarrow$$

$$\langle L, \wedge, \vee \rangle$$

$$\Downarrow \quad \Downarrow$$

$$\langle L, *, \circ \rangle$$

格与布尔代数部分内容提要（续）

- 格中元素的性质：
  - 对偶原理：若命题f对所有格为真，则其对偶命题f^*亦对所有格为真
  - 上下界：设L是格，$\forall a,b \in L, \boldsymbol{a \preccurlyeq b \Leftrightarrow a \wedge b = a \Leftrightarrow a \vee b = b}$（对应于代数格$\boldsymbol{a * b = a, a \circ b = b}$）
  - 保号性：设L是格，$\forall a,b,c,d \in L, a \preccurlyeq b$且$c \preccurlyeq d \Rightarrow a \wedge c \preccurlyeq b \wedge d, a \vee c \preccurlyeq b \vee d$

格与布尔代数部分内容提要（续）

- 子格：
  - 设$\langle L, \wedge, \vee \rangle$是格，$S \subseteq L$，$S \neq \emptyset$，若$\langle S, \wedge, \vee \rangle$也构成格，则称$S$是$L$的子格
- 格同态映射φ：
  - 设L_1和L_2是格，$\varphi: L_1 \to L_2$，若$a, b \in L_1$满足：$\varphi(a \wedge b) = \varphi(a) \wedge \varphi(b)$，$\varphi(a \vee b) = \varphi(a) \vee \varphi(b)$

格与布尔代数部分内容提要（续）

- 格同态映射的保序性：
  - $x \preccurlyeq y \Rightarrow \varphi(x) \preccurlyeq \varphi(y)$
- 双射φ成为格同构映射之充要条件：
  - $x \preccurlyeq y \Leftrightarrow \varphi(x) \preccurlyeq \varphi(y)$
- 分配格
  - 设$\langle L, \wedge, \vee \rangle$是格，若$\wedge$与$\vee$相互满足分配律，则称$L$为分配格

格与布尔代数部分内容提要（续）

- 分配格第一判定定理
  - L是分配格当且仅当L中不含有与钻石格和五角格同构的子格
  - 推论1：小于五元格的格皆为分配格
  - 推论2：任何链均为分配格
- 分配格第二判定定理
  - L是分配格当且仅当$(\forall a,b,c \in L)$ $(a \wedge b = a \wedge c$且$a \vee b = a \vee c) \Rightarrow b = c$

格与布尔代数部分内容提要（续）

- 有界格
  - 同一律：有界格$\langle L, \wedge, \vee, \mathbf{0}, \mathbf{1}\rangle$，则$\forall a \in L$，有：$a \wedge 0 = 0$，$a \vee 0 = a$，$a \wedge 1 = a$，$a \vee 1 = 1$
- 有界格中的补元
  - 有界格$\langle L, \wedge, \vee, \mathbf{0}, \mathbf{1}\rangle$中元素$a, b$互为补元$\Leftrightarrow$ $a \wedge b = \mathbf{0}$且$a \vee b = \mathbf{1}$
  - 若有界分配格中某元素存在补元，则其补元唯一
  - 有补格：格中每个元素均存在补元

格与布尔代数部分内容提要（续）

- 布尔代数
  - 布尔代数是有补分配格
  - 布尔代数$\langle B,*,\circ,',\mathbf{0},\mathbf{1}\rangle$是代数系统，二元运算$*,\circ$满足：交换律、分配律、单位元律、补元律
- 布尔代数的性质
  - 双重否定：$(a')'=a$
  - De Morgen：$(a\wedge b)'=a'\vee b'$，$(a\vee b)'=a'\wedge b'$

格与布尔代数部分内容提要（续）

- 有限布尔代数的结构
  - 任何有限布尔代数同构于某一幂集格
  - 任何有限布尔代数同构于其原子集合的幂集代数
  - 任何有限布尔代数的基数为$2^n(n \in \mathbb{N})$，n是该布尔代数中的原子数目
  - 有限布尔代数中的元素由其原子唯一确定
  - 任何等势的有限布尔代数均同构

群论部分内容提要（续）

半群与幺半群：

- 设$V = \langle S,\circ\rangle$是代数系统，$\circ$是二元运算，如果$\circ$可结合，则称$V$为半群
- 设$V = \langle S,\circ\rangle$是半群，若$e \in S$是关于$\circ$的单位元，则称$V$为幺半群（Monoid），或可记为$\langle S,\circ,e\rangle$
- 半群的子代数称为子半群，幺半群的子代数称为子幺半群，子幺半群还要求幺元（单位元）在S的子集中

群论部分内容提要（续）

- ## 群的定义与概念：
  - 群是特殊的半群和幺半群
  - 设$\langle G,\circ\rangle$是代数系统，$\circ$为二元运算。若$\circ$是可结合的，存在幺元$e\in G$，且对G中任意元素x都存在逆元$x^{-1}\in G$，则称G为群，或记作$\langle G,\circ,e,^{-1}\rangle$
  - 若群G为有穷集，则称为有限群，否则成无限群，群G的基数称为群的阶。只含幺元（阶为1）的群称为平凡群。
  - 若群G中的二元运算可交换，称G为交换群（阿贝尔群）

群论部分内容提要（续）

- 群的基本性质：
  - 幂运算规则：设G为群，则
    - $\forall a \in G, (a^{-1})^{-1} = a \quad \forall a, b \in G, (ab)^{-1} = b^{-1}a^{-1}$
    - $\forall a \in G, a^n a^m = a^{n+m}, n, m \in \mathbb{Z}$
    - $\forall a \in G, (a^n)^m = a^{nm}, n, m \in \mathbb{Z}$
    - $(a_1 a_2 \cdots a_r)^{-1} = a_r^{-1} a_{r-1}^{-1} \cdots a_2^{-1} a_1^{-1}$
  - 设G为群，则G适合消去律：$\forall a, b, c \in G$有$ab = ac \Rightarrow b = c$（左消去律）和$ba = ca \Rightarrow b = c$（右消去律）

群论部分内容提要（续）

- 群中元素的阶：

设G为群，$a \in G$，使得等式：

$$a^k = e$$

成立的最小正整数k称为a的阶（或周期），记为$|a| = k$。称a为k阶元；若不存在这样的正整数k，则称为a为无限阶元

群论部分内容提要（续）

- 元素的阶的性质：
  - 设G为群，$a \in G, k \in \mathbb{Z}, |a| = r$：
    - $\boldsymbol{a^k = e \Leftrightarrow r|k}$
    - $\boldsymbol{|a^{-1}| = |a|}$

群论部分内容提要（续）

- 子群的概念：

子群是群的子代数。其定义为：设G是群，H是G的非空子集，如果H关于G中的运算构成群，则称H是G的子群，记为：$H \leq G$；真子群$H < G \Leftrightarrow H \leq G \wedge H \subset G$。子群的交仍是子群，子群的并一般不构成子群

群论部分内容提要（续）

- 子群的判定定理（一）：

设G为群，H是G的非空子集。H是G的子群

当且仅当：

$$(1)\ \forall a, b \in H \Rightarrow ab \in H$$

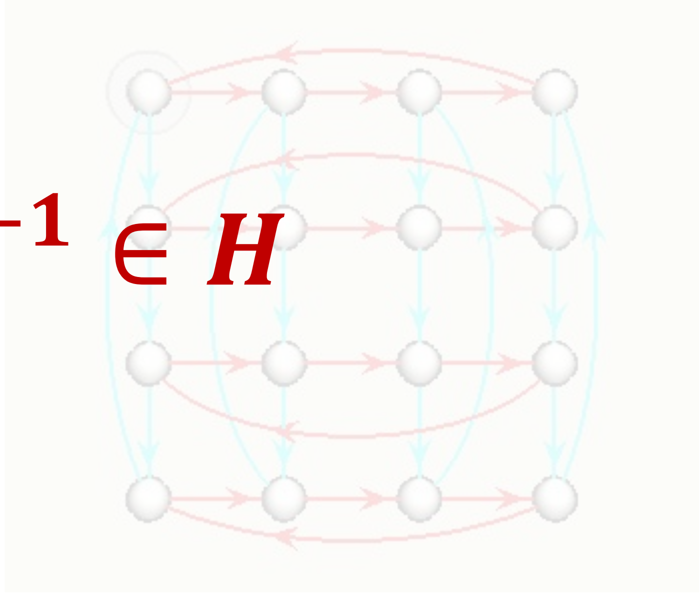
$$(2)\ \forall a \in H \Rightarrow a^{-1} \in H$$

子群的判定定理（二）：

设G为群，H是G的非空子集。H是G的子群

当且仅当：

$$\forall a, b \in H \Rightarrow ab^{-1} \in H$$



群论部分内容提要（续）

- 子群的判定定理（三）：

设G为群，H是G的非空子集。如果H是有穷集，则H是G的子群当且仅当：

$$\forall a,b \in H \Rightarrow ab \in H$$

群论部分内容提要（续）

- 群中元素的生成子群：

设G为群，$a \in G$，令：

$$\boldsymbol{H} = \{\boldsymbol{a}^{\boldsymbol{k}} | \boldsymbol{k} \in \mathbb{Z}\}$$

则$H \leq G$，并称其为由a生成的子群，记为$\langle a \rangle$，

a称为$\langle a \rangle$的生成元，

群论部分内容提要（续）

- 子群的陪集：

设G为群，$H \leq G, a \in G$，令：

$$\boldsymbol{Ha = \{ha | h \in H\}}$$

称Ha是子群H在G中的右陪集。称a为Ha的代表元素。$\forall a \in G, H \approx Ha$

群论部分内容提要（续）

- 子群的陪集构成群集的划分：
  - 设G为群，$H \leq G$，则：

(1) $\forall a, b \in G, Ha = Hb \vee Ha \cap Hb = \emptyset$

(2) $\cup \{Ha | a \in G\} = G$

- Lagrange定理：设$\langle G, * \rangle$为有限群，$\langle H, * \rangle < \langle G, * \rangle$，则 $|G| = |H| \cdot [G : H]$

群论部分内容提要（续）

- 群的同态与同构：
  - 设G_1和G_2是群，$\varphi: G_1 \to G_2$，若$\forall a, b \in G_1$有$\varphi(ab) = \varphi(a)\varphi(b)$，则称$\varphi$是$G_1$到$G_2$的同态映射，简称同态
  - 若φ为满同态，则G_2是G_1的同态像，φ为双射$\Leftrightarrow$同构
- 同态对子群性质的保持：
  - φ是G_1到G_2的同态，$H \leq G_1 \Rightarrow \varphi(H) \leq G_2$

群论部分内容提要（续）

- 循环群：
  - $\langle G,*\rangle$为循环群指：$(\exists \boldsymbol{a} \in \boldsymbol{G})(\boldsymbol{G} = \langle \boldsymbol{a} \rangle)$， $\langle \boldsymbol{a} \rangle = \{\boldsymbol{a}^{\boldsymbol{n}} | \boldsymbol{n} \in \mathbb{Z}\}$， a称为G之生成元
  - n阶循环群G的生成元的个数为Euler函数$\varphi(n)$
  - 对于n的每个因子d， n阶循环群都有一个d阶子群
  - $\langle G,*\rangle$为无限循环群，则$\langle \boldsymbol{G},* \rangle \cong \langle \mathbb{Z},+\rangle$
  - $\langle G,*\rangle$为有限循环群，则$\langle \boldsymbol{G},* \rangle \cong \langle \mathbb{Z}_{\boldsymbol{n}},\oplus_{\boldsymbol{n}}\rangle$

图论部分总框图

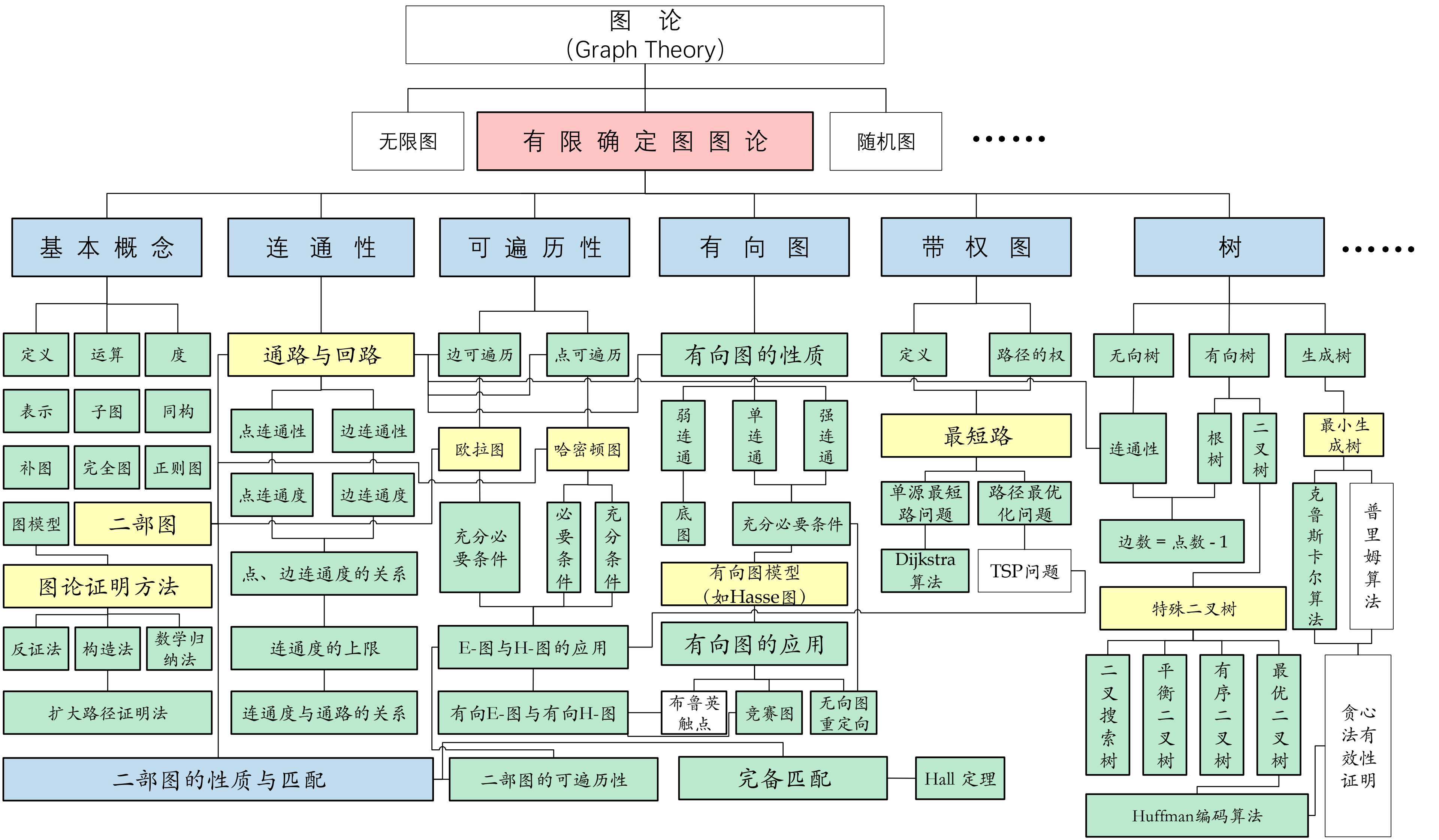


图 论
(Graph Theory)
无限图
有限确定图图论
随机图
……
基本概念
连通性
可遍历性
有向图
带权图
树
……
定义
运算
度
表示
子图
同构
补图
完全图
正则图
图模型
二部图
图论证明方法
反证法
构造法
数学归纳法
扩大路径证明法
通路与回路
点连通性
边连通性
点连通度
边连通度
点、边连通度的关系
连通度的上限
连通度与通路的关系
边可遍历
点可遍历
欧拉图
哈密顿图
充分必要条件
必要条件
充分条件
E-图与H-图的应用
有向E-图与有向H-图
有向图的性质
弱连通
单连通
强连通
底图
充分必要条件
有向图模型
(如Hasse图)
有向图的应用
布鲁英触点
竞赛图
无向图重定向
定义
路径的权
最短路
单源最短路问题
路径最优化问题
Dijkstra算法
TSP问题
无向树
有向树
生成树
连通性
根树
二叉树
最小生成树
边数 = 点数 - 1
特殊二叉树
克鲁斯卡尔算法
普里姆算法
二叉搜索树
平衡二叉树
有序二叉树
最优二叉树
Huffman编码算法
贪心法有效性证明
二部图的性质与匹配
二部图的可遍历性
完备匹配
Hall 定理

图论部分内容提要

- **无向图**：$G = \langle V, E \rangle$：
  - $V \neq \emptyset$为顶点集
  - E是$V\&V$的多重子集，称为边集，元素称无向边
- **有向图**：$G = \langle V, E \rangle$：
  - $V \neq \emptyset$为顶点集
  - E是$V \times V$的多重子集，称为边集，元素称有向边

图论部分内容提要（续）

- 图的记号与特殊的图：
  - n阶图：$|V(G)| = n$的图
  - n阶零图（N_n）：$|E(G)| = \emptyset$且$|V(G)| = n$的图，
    N_1：平凡图
  - 空图：图运算中间结果中$|V(G)| = \emptyset$的图
  - 端点、环、孤立点、相邻、先驱、后继、多重图

图论部分内容提要（续）

- 图的记号与特殊的图（续）：
  - 简单图：既不含平行边也不含环的图
  - 顶点v的度：$d(v)$ =与v 关联的边的条数，一个环的度记为2
  - $\Delta(G) = \max\{d(v)|v \in V(G)\}, \delta(G) = \min\{d(v)|v \in V(G)\}$
  - 悬挂顶点、悬挂边、偶度顶点、奇度顶点

图论部分内容提要（续）

- 与图的基本概念相关的重要定理：
  - 握手定理：无向图$G=\langle V,E\rangle$，$\sum_{i=1}^{|V|} d(v_i)=2|E|$；
  - 任意图中奇数度顶点的个数是偶数
  - 有向图中各顶点入度和与出度和相等，总数为$2|E|$
  - n阶无向简单图的最大度：$\Delta(G)\le n-1$

图论部分内容提要（续）

- 与图的基本概念相关的重要定理（续）：
  - 图同构：$G_1 = \langle V_1, E_1 \rangle, G_2 = \langle V_2, E_2 \rangle$，存在双射函数$f: V_1 \to V_2$，使得$\forall v_i, v_j \in V_1, (v_i, v_j) \in E_1 \Leftrightarrow \left(f(v_i), f(v_j)\right) \in E_2$且两者具有相同重数，则$G_1$与$G_2$同构，记为：$G_1 \cong G_2$
  - 同构的图具有相同的阶、相同的边数、相同的度数列；但反之则不一定

图论部分内容提要（续）

- 与图的基本概念相关的重要定理（续）：
  - 完全图：若n阶无向简单图，若G中每个顶点均与其余$n-1$个顶点相邻，则称G为n阶无向完全图，记作$\boldsymbol{K_n}(n \geq 1)$
  - 正则图：若n阶无向简单图，若$\forall v \in V(G)$，均有$d(v)=k$，则称G为k-正则图

图论部分内容提要（续）

- 子图、母图与生成子图：
  - 子图： $G=\langle V,E\rangle$， $G'=\langle V',E'\rangle$二图，若有$V'\subseteq V$且$E'\subseteq E$，则称G'为G的子图：$G'\subseteq G$
  - 母图： 在上述定义下，G为G'的母图
  - 生成子图：在上述定义下， 若$V'=V$且$E'\subseteq E$，则称G'为G的生成子图

图论部分内容提要（续）

- 补图
  - n阶无向简单图 $G=\langle V,E\rangle$，以V为顶点集，以所有使G成为完全图K_n的添加边组成的集合为边集的图，记作$\bar{G}$

图论部分内容提要（续）

- 图的通路与回路：
  - 通路与回路
  - 简单通路与简单回路：Γ中所有的边各异
  - 初级通路（路径）与初级回路（圈）：Γ中所有顶点与边均各异，则称Γ为初级通路（路径），又若除$v_0 = v_l$，所有的顶点各不相同且所有的边各异，则称Γ为初级回路（圈）
  - 复杂通路与回路：有边重复出现
  - 回路是通路，初级通路（回路）是简单通路，但反之不真

图论部分内容提要（续）

- 关于通路与回路的重要定理：
  - 在n阶图G中，若非同顶点v_i到v_j存在通路，则此二顶点间必存在长度小于或等于$n-1$的通路及路径
  - 在n阶图G中，若存在顶点v_i到自身的回路，则一定存在v_i到自身长度小于或等于n的回路与圈

图论部分内容提要（续）

- 无向图的连通性：
  - 顶点之间的连通关系：等价关系
  - 连通图：平凡图或图中任意两顶点均连通
  - 连通分支：顶点集V关于连通关系的商集，$p(G)=|V/\sim|$，其诱导的等价类为导出子图$G[V_i]$，若图G为连通图，则$p(G)=1$，否则$p(G)\geq 2$
  - 短程线：若顶点$u\sim v$，则为其间最短通路，其长度为距离，记为$d(u,v)$；若$u\nsim v$，$d(u,v)=\infty$

图论部分内容提要（续）

- 无向图的连通性（续）：
  - 点割集与割点：对$G=\langle V,E\rangle$，若存在$V'\subset V\wedge V'\neq\emptyset$，使$p(G-V')>p(G)$，且对于任意$V''\subset V'$，$p(G-V'')=p(G)$，则称$V'$是图$G$的点割集，如若$V'$是单点集$V'=\{v\}$，则称$v$为割点
  - 边割集与桥（割边）：平凡图或任意2顶点均连通
  - 连通度：$\kappa(G)=\min\{|V'|\,|V'为G的点割集\}$
    - $\kappa(K_n)=n-1$
    - $k-$连通图：$\kappa(G)\geq k$

图论部分内容提要（续）

- 无向图的连通性（续）：
  - 边连通度：$\lambda(G) = \min\{|E'| \mid E'\text{为}G\text{的边割集}\}$
    - r −边连通图：$\lambda(G) \geq r$
  - 对于任意无向图G，有$\boldsymbol{\kappa(G) \leq \lambda(G) \leq \delta(G)}$
- 扩大路径证明法

图论部分内容提要（续）

- 有向图的连通性：
  - 弱连通图：基图是连通图的有向图
  - 强连通图：对有向图$D = \langle V, E \rangle, \forall v_i, v_j \in V \Rightarrow v_i \leftrightarrow v_j$
  - 单向连通图：对有向图$D = \langle V, E \rangle, \forall v_i, v_j \in V \Rightarrow v_i \rightarrow v_j \vee v_j \rightarrow v_i$

图论部分内容提要（续）

- 有向图的连通性（续）：
  - 强连通图判定定理：对有向图$D=\langle V,E\rangle, V=\{v_1,v_2,\cdots,v_n\}$，$D$是强连通图$\Leftrightarrow$ D中存在经过每个顶点至少一次的回路
  - 单向连通图判定定理：对n阶有向图，D是单向连通图$\Leftrightarrow$ D中存在经过每个顶点至少一次的通路

图论部分内容提要（续）

- 二部图：
  - 无向图$G=\langle V,E\rangle$，若能将V分为不交的V_1和V_2，使得G中每条边的两个端点均分属V_1和V_2，则称G为二部图（bipartite graph），记为$\langle V_1,V_2,E\rangle$
  - 完全二部图：G为简单二部图，V_1中每个顶点均与V_2中所有顶点相邻，记为$K_{|v_1|,|v_2|}$

图论部分内容提要（续）

- 二部图的判定定理：
  - 无向图$G = \langle V, E\rangle$是二部图$\Leftrightarrow$ G中不存在奇数长度的回路
- 欧拉图
  - 含有欧拉回路（经过图中所有边一次且仅一次的回路）的图，平凡图是欧拉图
  - 半欧拉图：含有欧拉通路但不含欧拉回路的图

图论部分内容提要（续）

- 欧拉图的判定定理：
  - 无向图是欧拉图当且仅当其为连通图且不含奇度顶点
  - 无向图是半欧拉图当且仅当其为连通图且恰含2个奇度顶点
  - 有向图是欧拉图当且仅当其为强连通图且每个顶点的入度与出度相等

图论部分内容提要（续）

- 欧拉图的判定定理（续）：
  - 有向图是半欧拉图当且仅当其为单向连通图且恰含2个奇度顶点，其中一个入度比出度大1，另一个出度比入度大1，其余每个顶点的入度与出度相等
  - G是非平凡欧拉图当且仅当G为连通的且为若干不重的圈的并图
- 求欧拉回路的Fleury算法

图论部分内容提要（续）

- 哈密顿图
  - 含有哈密顿回路（经过图中所有顶点一次且仅一次的回路）的图，平凡图是哈密顿图
  - 半哈密顿图：含哈密顿通路但不含欧拉回路的图

图论部分内容提要（续）

- 哈密顿图的性质或定理（充分或必要条件）
  - 哈密顿图成立的简单充分必要条件尚未找到
  - 无向图$G=\langle V,E\rangle$是哈密顿图，则：$\forall V_1(V_1 \subset V \wedge V_1 \neq \emptyset) \Rightarrow p(G-V_1) \leq |V_1|$
  - 无向图$G=\langle V,E\rangle$是半哈密顿图，则：$\forall V_1(V_1 \subset V \wedge V_1 \neq \emptyset) \Rightarrow p(G-V_1) \leq |V_1|+1$

图论部分内容提要（续）

- 哈密顿图的性质或定理（续）
  - 若无向图中含有割点或桥，则其非哈密顿图
  - G是$n(n \geq 3)$阶无向简单图，若对于G中任意不相邻顶点v_i, v_j均有$d(v_i) + d(v_j) \geq n$，则G是$H-$图
  - G是n阶无向简单图，若对于G中任意不相邻顶点v_i, v_j均有$d(v_i) + d(v_j) \geq n-1$，则G中存在哈密顿通路
  - 二阶及以上竞赛图具有哈密顿通路

图论部分内容提要（续）

- 无向树：
  - 连通无回路的无向图
  - 平凡树：即平凡图
  - 森林：$p(G) \geq 2$的无向图且每个分支皆为无向树
  - 树叶：无向树中的悬挂顶点
  - 分支点：无向树中度数大于或等于2的顶点

图论部分内容提要（续）

- 关于无向树的几个等价命题：
  - n阶含m条边的无向图G是无向树
  - G中任意两个顶点之间存在唯一路径
  - G中无（简单）回路且$m = n - 1$
  - G是连通的且$m = n - 1$
  - G是连通的且G中任何边均为桥
  - G中无回路，但在任意两个不同顶点之间加一条新边，所得图中即得到唯一的含新边的圈

图论部分内容提要（续）

- 有关无向树特性的命题：
  - 设T是n阶非平凡无向树，则T中至少含2个树叶
- 生成树：
  - T为无向图G的生成子图且为树，称T为G的生成树
- 有关生成树的几个定理：
  - 无向图G具有生成树当且仅当G是连通图
  - 设G是n阶m条边的无向连通图，则$m \geq n-1$

图论部分内容提要（续）

- 最小生成树：
  - 带权树：无向连通带权图的生成树
  - 树的权：带权树的各边权值之和，记作$W(T)$
  - 最小生成树：无向连通带权图的所有的生成树中权值最小者
- 求最小生成树的Kruskal算法和Prim算法
  - 算法正确性证明——了解梗概

图论部分内容提要（续）

- 有向树：底图为树的有向图称为有向树
- 根 树：若$n(n \geq 2)$阶有向树恰含一个入度为0的顶点，其它顶点入度均为1，则该有向树称为根树，其入度为0的顶点称为根，设根结点为v_0，存在唯一的有向$v_0 v_n$ –通路，但不存在$v_n v_0$ –通路

图论部分内容提要（续）

- 根树的层次表示法
  - 有序：同层中每个顶点排定次序
  - r叉：每个分支点至多有r个儿子
  - r叉正则：每个分支点恰好有r个儿子
  - 完全：每个叶的层数恰等于树高
  - 高度为k完全正则r叉树顶点数：$(r^{k+1}-1)/(r-1)$

图论部分内容提要（续）

- 子树
- 特殊的二叉树
  - 二叉搜索树、AVL树
  - 有序树
  - 最优二叉树、最优二叉编码树（Huffman树）
- Huffman算法（会算法，不要求证明）
- 根树的遍历

期末考试安排与习题课

- 考试时间：2017年7月6日，16:30–18:30
- 考试地点：仙I-206
- 考试范围：除图论外其它内容约占50%，图论部分约占50%
- 考试形式：解答与证明
- 总评成绩构成：平时成绩（30%，含一次课堂测验成绩占总成绩10%）、期中考试成绩（20%）、期末考试成绩（50%）
- 不安排线下答疑，在任何时间进行网上答疑：QQ群、微信、电子邮件等均可实时回复，也可预约助教进行当面答疑
- 习题课：本周六（6月24日）18:30–20:30，系楼229

未在教务处成功选课的同学请不要参加期末考试