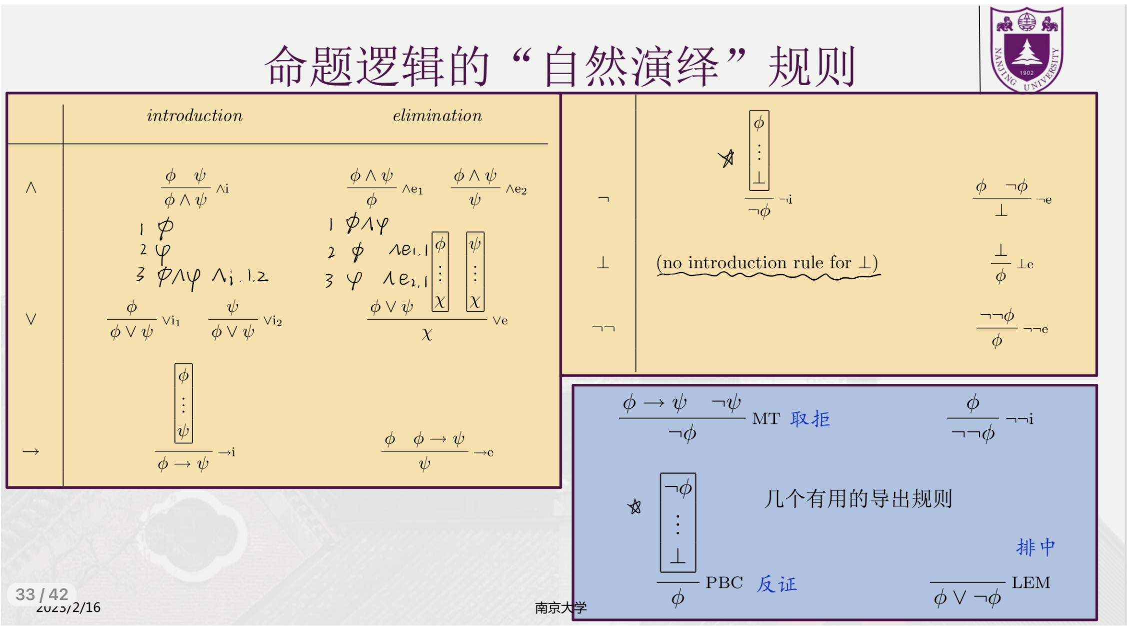
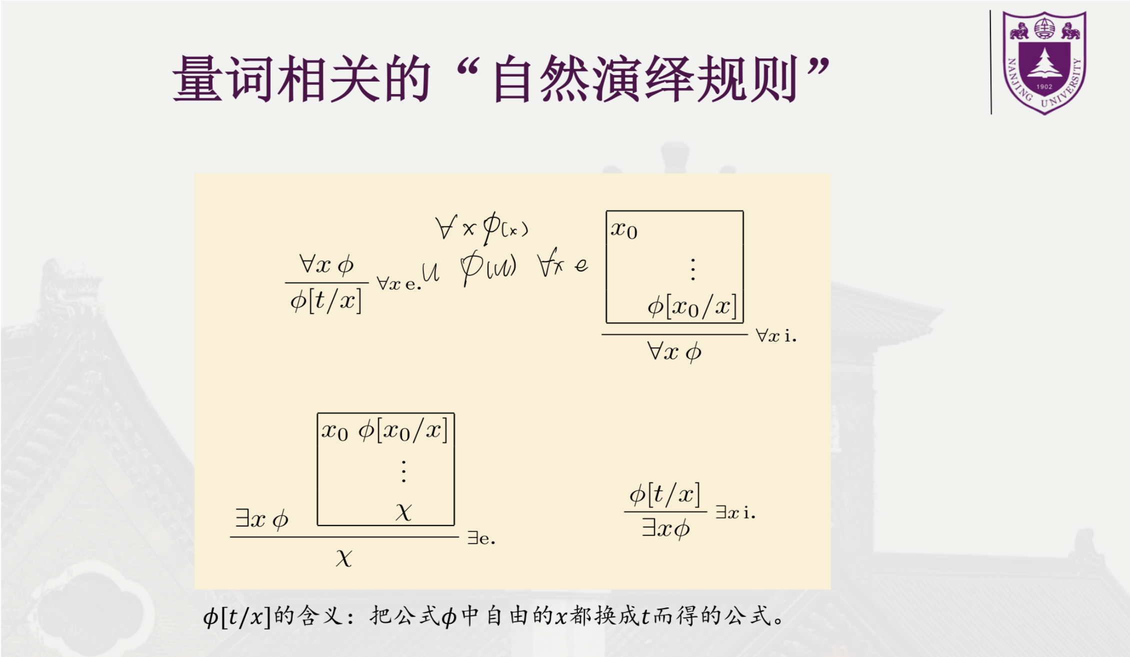
知识点整理

1. 逻辑和证明

- 命题逻辑
  - 命题变元
  - 逻辑符号：析取，合取，否定，蕴含，双蕴含
    - 优先级 否定>合取>析取>蕴含>双蕴含
  - 自然语言翻译成命题表达式：命题变元+逻辑符号
  - 真值表
  - 语义蕴含
  - 析取范式，合取范式，极小项，极大项
    - 析取范式：有限个简单合取式构成的析取式
    - 合取范式：有限个简单析取式构成的合取式
  - **自然演绎法**
    - 

- 谓词逻辑
  - 约束变元，自由变元
  - 带量词的逻辑公式的取反
  - 前束析取/合取范式 PNF
    - 同析取/合取范式，量词均移动至语句前
  - **带量词的自然演绎法**



- 证明方法
  - 略

2. 集合论

- 集合的基数：不同元素的个数
- 幂集：所有子集的集合
- 集合运算
  - 并，交，补，对称差
  - 广义并/交
  - f(S) ⊆ f(S∪T), f(T) ⊆ f(S∪T) -> f(S)∪f(T) ⊆ f(S∪T)
- 有序对 (a, b)
- 笛卡尔乘积
- 二元关系 R⊆A×B
- 函数 f: A→B
  - 单射，满射，双射
  - 反函数
  - 函数的复合
    - 单射和满射的复合 <==> 双射
- 同余算术
  - 欧几里得算法：辗转相除
  - 裴蜀定理
  - 中国剩余定理
  - 费马小定理：a^p ≡ a (mod p) 其中a不是素数p的倍数
  - 欧拉定理
  - 因式分解：2xy − 1 = (2x)y − 1 = (2y − 1)(2y(x−1) + 2y(x−2) + ... + 2y + 1)
  - d|a − b <==> a≡b(mod d)

- 下证：$15 \mid 3n^5+5n^3+7n \iff 3 \mid 5n^3+7n$ 且 $5 \mid 3n^5+7n$
  $\Updownarrow$
  $3 \mid 3n^5+5n^3+7n$ 且 $5 \mid 3n^5+5n^3+7n$
  $\Updownarrow$
  $3 \mid 5n^3+7n$ 且 $5 \mid 3n^5+7n$
- 集合的基数
  - 等势关系：存在从A到B的双射 A≈B
  - S是无限集 <==> 存在S的真子集S’使得S≈S'
- 有限/无限集和可数/不可数集
  - 有限集：存在自然数n与其等势
  - 可数集：存在自然数集N的某个子集与其等势
- 康托尔对角线法
- 康托尔定理：任何集合与其幂集不等势
- 优势关系：找单射
  - 自反性，传递性，反对称性（用于找两个单射）
- 超穷基数：了解一下就行
  - aleph0：可数集合的基数
  - aleph1：可数序数的集合的基数

3. 归纳与递归

- 数学归纳法
- 强数学归纳法：n=0~k均成立，证明n=k+1成立
- 良序原理：可以用于证明数学归纳法的正确性，也可以用归纳公理证明
- 递归定义
- 结构归纳法：数学归纳法，对递归次数做归纳

4. 基本计数技术

- 排列，组合
- 二项式定理
- 杨辉三角
- 范德蒙恒等式
- 多项式定理
- 带重复元素的排列组合
  - 圆排列：P(n, r)/r
  - 不可区分（重复）物体排列：P(n, n)/∏mi! 其中mi是第i个重复项的重复次数
  - 有重复的组合：隔板法 C(n+r-1, r)
- 容斥原理
- 常系数线性递推
- 第二类斯特林数
- 鸽笼原理

- Burnside 计数定理 $L = 1/|G| \Sigma_{g\in G}|D(g)|$。其中，L 表示总方案数，G 表示所有等价变换组成的集合，D(g) 表示置换后本质未发生改变的方案个数。

5. 离散概率

- 贝叶斯定理

6. 二元关系

- 记号: aRb $R\subseteq A\times B$
- 特殊的二元关系
    - 全域：$A\times B$
    - 恒等：$(x, x), x\in A$
- 定义域，值域，域(定义域∪值域)
- 函数是一种特殊的关系
- 关系的运算
    - $R\upharpoonright S$: R中定义域为S的有序对的集合
    - $R[S]=Ran(R\upharpoonright S)$
    - $R(a)==R[\{a\}]$
    - R^{-1}: 逆运算
    - 关系的复合
- 关系运算的矩阵算法
- 关系的性质
    - 自反性，反自反性
        - R自反<==>$I_A\subseteq R$
    - 对称性，反对称性
        - R对称<==>$R^{-1}=R$
    - 传递性
        - R传递<==>$R^2\subseteq R$
- 关系闭包
    - 自反闭包
        - 定义自己看
        - 计算：$r(R) = R\cup I_A$
    - 对称闭包
        - 计算：$s(R) = R\cup R^{-1}$
    - 传递闭包
        - 计算：对着关系矩阵嗯乘就完事了
            - $t(R) = \cup R^i$
            - $M_{t(R)}=M \vee M^2 \vee ... \vee M^n$
        - Warshall算法 **很重要**
- 等价关系：自反+对称+传递
    - 等价类：任意$x\in A$，$[x]_R = \{y \mid y\in A \wedge xRy\}$
    - 商集：设R是A上的等价关系，则其所有等价类的集合称为商集A/R

- 集合的划分：π⊆P(A)
  - 满足：$\cup A_i$=A；Ai∩Aj=∅ iff i≠j
  - 某等价关系的商集是一个划分
- 偏序关系：自反+反对称+传递 a ≤ b
  - 可比：对x, y 有 x≤y 或 y≤x
  - 全序：任意两个元素可比
  - 覆盖：x < y且不存在x < z < y
  - 哈斯图
  - 上下确界
  - 良序：任一非空子集存在最小元素 必为全序
  - 链与反链
  - Mirsky定理：高度为t的偏序集可划分为t个反链
  - Dilworth定理：宽度为w的偏序集可划分成w个链
- 格
  - 偏序格：对于任意x,y 存在最小上界和最大下界
    - x v y 最小上界
    - x ^ y 最大下界
  - 格的基本关系式
    - a≤c，b≤d => a v b ≤ c v d, a ^ b ≤ c ^ d
  - 格的性质
    - a≤b <=> a^b = a <=> a v b = b
    - 结合律，交换律，**吸收律** => 幂等律
  - 对偶命题
  - 代数格：设L是一个集合，^和v是L上的二元运算，且满足结合律，交换律，吸收律，则称(L, ^, v)是代数格
    - 等同于偏序格
  - 格同态，格同构
  - 分配格，有补格
    - 分配格：满足分配律
    - 有界格：有全下界0和全上界1
    - 有补格：任一元素存在补元
  - 布尔代数：有补的分配格

7. 代数系统和半群

- 代数系统
  - 定义：<S, * >对*运算封闭
  - 单位元：e*x = x*e = x
    - 代数系统不一定有单位元
    - 左幺和右幺
      - 不一定存在或唯一
      - 同时存在必相等且唯一
  - 逆元：$x * x^{-1} = e$

    - 零元
- 半群：具有结合性的代数系统
    - 单元半群：+=单位元
    - 子半群，子单元半群
    - 同态与同构
    - 商半群

8. 群论

- 群
    - 定义：幺半群+对任意元素存在逆元
    - 逆元唯一：对半群，逆元若存在必定唯一
    - 性质：
        - $(a^{-1})^{-1} = a$
        - $(ab)^{-1} = b^{-1}a^{-1}$
        - ab = ac -> b = c 左消去律
        - ba = ca -> b = c 右消去律
    - 元素的阶：$|a| = \min \{k \in Z^+ | a^k = e\}$
        - k不存在则a为无限阶元
        - 性质
            - 有限群中无无限阶元
            - 元素及其逆元同阶
            - 有限群中阶>2的元素有偶数个
            - 偶数群中阶为2的元素有奇数个($a = a^{-1}$)
    - 群的阶：
        - G为有穷集且|G| = n 称G为n阶群
        - G为无穷集 称G为无限群
        - 满足交换律则称G为阿贝尔群
    - 群方程
        - 定理：半群G中方程ax = b与ya = b均有唯一解，则G为群
        - 两种等价定义
            - 半群G中方程ax = b与ya = b均有唯一解，则G为群
            - 半群G中存在左单位元且对所有元素存在左逆元，则G为群
- 子群
    - 定义：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H是G的子群
        - 记为$H \leq G$
    - 判定定理
        - G是群，H是G的非空子集。H是G的子群 <==> 对于任意$a, b \in H$, $ab \in H$且对于任意$a \in H$, $a^{-1} \in H$
        - H是G的非空子集，H是G的子群 <==> 对于任意$a, b \in H$, $ab^{-1} \in H$
        - H是G的**非空有限**子集，H是G的子群 <==> 对于任意$a, b \in H$, $ab \in H$
    - 生成子群

    - 设$a\in G$，构造$H = \{a^k \mid k\in Z\}$，则称H为a生成的子群<a>
    - 证明：判定定理2
  - 元素的阶
    - 对a^n定义
      - $n\geq 0$
      - $n<0$, $a^n = (a^{-n})^{-1}$
    - |a|略
    - 性质：对G的有限阶元素a, b
      - $a^k = e$ <===> |a| 整除 k
      - $|a| = |a^{-1}|$
      - $|ab| = |ba|$
      - $|b^{-1}ab| = |a|$
  - 群的中心
    - 构造$C = \{a \mid a\in G$且对于任意$x\in G, ax = xa\}$，称C为G的中心
  - 左右陪集
    - 定义：设$a\in G$，H是G的一个子群，$aH = \{ah \mid h\in H\}$，则aH称为H的一个左陪集
      - 相应可定义右陪集
      - 对于任意的$h\in H$，$ah\in H$ <===> $a\in H$
    - 划分：设H是G的子群，则H的所有左陪集构成G的划分
      - 对于任意元素$a, b\in G$, $aH = bH$或者$aH\cap bH$ = 空\
      - 定理：
        - $eH = H$
        - $\cup(aH \mid a\in G) = G$
        - 对于任意$a, b\in G$, $aH = bH$ 或 $aH\cap bH$ = 空集
        - $\{aH \mid a\in G\}$ 为G的划分
  - 拉格朗日定理
    - 对G的划分$\{aH \mid a\in G\}$，$|G| = k|H|$，k称为H在G中的指数，记为[G:H]
    - 设G为有限群，$H\leq G$，则$|G| = |H| \cdot [G:H]$
    - 推论
      - 设G为有限群，a属于G，则|a|为|G|的因子
      - 设G为p阶群，若p为质数，则存在$a\in G$使得<a> = G
      - $x^{|G|} = e$
      - 欧拉定理
- 循环群
  - 定义：设G为循环群指：存在$a\in G$，使得G = <a>，其中$\langle a\rangle = \{ a^n \mid n\in Z \}$，a称为G的生成元
  - 有限循环群：|a| = n
  - 无限循环群：a^0为幺
  - 若a是无限循环群的生成元，则a^{-1}也是该无限循环群的生成元
  - 无限循环群有且仅有2个生成元
  - 设G = <a> 且 |a| = n，则对于任意r < n，$G = \langle a^r\rangle$ <===> gcd(n, r) = 1

- n阶循环群G的生成元的个数恰好=不大于n且与n互质的正整数的个数，即Euler函数φ(n)，其生成元集为{i | 0<i≤n ^ gcd(i, n) = 1}
- 设G = <a>为循环群
  - G的子群为循环群
  - 若|a| = ∞，则G的子群除{e}外皆为无限循环群
- 群的直积
  - Cm×Cn ≅ Cmn iff m与n互质，其中Ck表示k阶循环群
- 置换群

- 群同构
  - 定义：G1 ≅ G2 iff 存在双射f：G1->G2
    - 群同构关系是等价关系
  - 一些特殊的同构例子
    - 任意两个三阶群同构
    - 两个且仅有两个的不同构四阶群：四元循环群和Klein四元群
  - 同态
    - G为无限循环群，则G ≅ <Z, +>
    - G为无限循环群，则G ≅ $<Z_n, +_n>$
    - 推论：循环群均为阿贝尔群
- 正规子群
  - 定义：G的子群H是G的正规子群 iff 对于任意a∈G，Ha = aH
  - Ha = aH iff 对于任意h_i∈H，a∈G，存在h_j∈H，$h_i a = a h_j$
  - N是G的正规子群 iff 对于任意g∈G，n∈N，gng^{-1}∈N
    - 变形：N是G的正规子群 iff 对于任意g∈G，gNg^{-1}∈N
  - 商群

9. 图论

- 定义 G = (V, E)，其中V是非空顶点集，E是边集
  - 简单图：每条边有2个端点，且不同边端点集不同（没有环或者多重边）
  - 无向图，有向图
- 握手定理：Σd(v) = 2m 顶点度数之和=边数*2
  - 推论：无向图中奇数度顶点必为偶数个
- 有向图：
  - φ(e) = (u, v) u邻接到v
  - 出度，入度 出度和=入度和
- 特殊的简单图
  - 完全图 Kn
  - 圈图 Cn
  - 轮图 Wn
  - 立方体图 Qn
  - 正则图：所有顶点度数相同的简单图
- 子图，真子图
- 图的表示

- 关联矩阵：假设G是无向图，$M(G) = [m_{ij}]$为G的关联矩阵，其中m_{ij}满足 =1(ej关联vi) =0(否则)
- 邻接矩阵：G是有向图，A(G)
  - 简单无向图的邻接矩阵是对称矩阵
  - 也可表示多重边，此时不为布尔矩阵
  - 运算
    - 逆图（转置矩阵）A^T
    - $A \times A^T = B = [bij]$ bij表示结点i和结点j均有边指向的那些结点的个数
    - $A^T \times A = C = [cij]$ cij表示同时有边指向i和j的结点个数
    - $A \times A$：长度为2的通路
- 图的运算
- 图同构
- 图的连通性
  - 通路：同构图的不变量
  - 连通：任意两个不同顶点之间存在通路
  - 连通分支：极大连通子图 p(G)
  - 割点：$p(G - v) > p(G)$
    - v是割点 <=> 存在 V - {v}的分划{V1, V2}，使得对任意u∈V1, w∈V2，uw通路均包含v <=> 存在顶点u，w≠v，使得任意的uw通路均包含v
  - $p(G) \le p(G - e) \le p(G) + 1$
  - 割边（桥） $p(G - e) > p(G)$
    - e是割边 iff e不在G的任一简单回路上 iff 存在V的分划{V1, V2}，使得对任意u∈V1, w∈V2，uw通路均包含e iff 存在顶点u，w≠v，使得任意的uw通路均包含e
  - （点）连通度：使连通图G成为不连通图需要删去的最少顶点数k(G)
    - 约定非连通图$k(G) = 0$，$k(Kn) = n - 1$
  - 边连通度λ(G)，同上
  - $k(G) \le \lambda(G) \le \delta(G)$（最小顶点度）
  - 定理：设G是简单图，$|G| = n \ge 3$且$\delta(G) \ge n-2$，则$k(G) = \delta(G)$
  - Whitney定理：图G($|G| \ge 3$)是2-连通图 iff G中任意两点被至少2条除端点外顶点不相交的路径所连接

欧拉图和哈密尔顿图

- 欧拉通路和欧拉回路
  - 欧拉通路：包含图中每条边的简单通路
  - 欧拉回路：……简单回路
  - 有欧拉回路的图称为**欧拉图**，没有欧拉回路但有欧拉通路的图称为**半欧拉图**
  - 连通图G是欧拉图 iff G中每个顶点的度数为偶数 iff G中所有的边包含在若干个相互没有公共边的简单回路中
  - G是半欧拉图 iff G恰有两个奇数度点
  - 若G是弱连通的有向图，G中存在有向欧拉回路 iff G中任一顶点的入度等于出度 iff G中所有边包含在若干个相互没有公共边的有向简单回路中
- Fleury算法

- 1. 任取v0∈VG，令P0=v0
- 2. 设Pi = v0e1v1e2...eivi，按下列原则从EG - {e1，e2，...，ei}中选择ei+1
    - ei+1与vi相关联
    - 除非别无选择，否则ei+1不应是G-{e1，e2，...，ei}中的割边
- 反复执行第2步，直到无法执行时终止
- 证明
    - v0=vm
        - 反证：推出Vm度数为奇数
    - Pm包括了G中所有的边
        - 反证：

- 哈密尔顿回路/通路
  - 包含G中所有顶点，且各顶点不重复
  - 一些必要条件
    - 若图G中有1顶点度数为1，则无哈密尔顿回路
    - 若有顶点度数>2，则只用两条边
    - 若图中有n个顶点，则哈密尔顿回路恰有n条边
  - 基本必要条件：若图G是哈密尔顿图，则对V的任一非空子集S，都有P(G-S)≤|S|，其中P(G-S)表示图G-S的连通分支数
  - 充分条件：G是无向简单图，|G| = n ≥ 3
    - Dirac定理：δ(G) ≥ n/2
    - Ore定理： 对任意顶点对(u, v)有d(u) + d(v) ≥ n
    - Ore定理的延伸
      - 有限图G是哈密尔顿图 iff 图C(G)是哈密尔顿图
      - 闭合图C(G)：连接G中不相邻的并且其度数之和不小于|G|的点对，直到算法终止
  - 格雷码
  - 竞赛图：底图为完全图的有向图
    - 归纳法可证含哈密尔顿通路

带权图

- Dijkstra算法
- Floyd-Warshall算法
- TSP问题

二部图与匹配

- 完全二部图 Km, n
- 匹配：
  - 极大匹配
  - 最大匹配
  - 完备匹配（单射）
  - 完美匹配（双射） (|V1| = |V2|)
- Hall定理
  - G有V1到V2的完备匹配 iff 对于任一V1的顶点子集A，有|N(A| ≥ |A|

    - 推论：二部图G是k-正则的，则G有完美匹配
    - 推论：二部图G中，若V1每个顶点至少关联t条边，V2每个顶点至多关联t条边，则存在完备匹配

10. 树

基本概念

- 定义：不包含简单回路的连通无向图
- 等价命题
    - T是不包含简单回路的连通图 iff T中任意两点有唯一简单通路 iff T连通，但删除任意一条边后不再连通 iff T中不包含简单回路，但在任意不相邻的顶点对之间加一条边则产生唯一的简单回路
    - 树是边最少的连通图，是边最多的无简单回路的图
- 边和点的数量关系：令边数为m，点数为n
    - $m = n - 1$
    - 连通图边数的下限：$m \geq n - 1$
    - T是树 iff T不含简单回路且m=n-1 iff T连通且m=n-1
- 根树：含根（入度为0）的有向树
- 几种术语
    - m元树，二叉树
    - 完全m元树
    - 平衡
    - 有序
    - 注意不是完全二叉树也能分左右子树
- 有序根树的遍历
    - 前序遍历：根在最前
    - 中序遍历：先访问第一棵子树，再访问根
    - 后序遍历：根在最后

树的应用

- 表达式
    - 波兰表示法（前缀），逆波兰表示法（后缀）
    - 运算方法：
        - 前缀：从右向左，op+右2对象
        - 后缀：从左向右，op+左2对象
- 二叉搜索树
    - u的左子树标号小于u的标号
    - u的右子树标号大于u的标号
- 决策树
- Huffman编码

生成树

- 定义：若图G的生成子图是树，则该子图称为G的生成树

    - 无向图G连通 iff G有生成树
- 构造生成树
    - DFS
    - BFS
- 最小生成树：权值和最小的生成树
    - Prim算法：找点的最小边
    - Kruskal算法：找最小边
        - 引理：更换生成树T和T′的边后仍是生成树