离散（2）CheatSheet

整理：顾一马；司路阳

- **邻集**： 外邻集 $N^+(v)$：直接后继，内邻集 $N^-(v)$：直接前驱
- **度**：图的最大度 $\Delta(G)$，最小度 $\delta(G)$
- 有向/无向图均成立：$\sum_{v\in V}\deg(v)=2|E|$，有向图为$\sum d^+(v_i)=\sum d^-(v_i)$
- 奇数度顶点的个数为偶数
- 非空简单图一定有度数相同的顶点（抽屉原理，取值范围为$1\sim n-1$）
- **基本图**：空图：$|E|=0$，平凡图：$|V|=1$
- **无向图**：简单图：无重边，无自环 多重图：有重边，无自环 伪图：有重边，有自环
  - k-正则图：每个顶点的度数为 k 的无向简单图，边数 $m=\frac{n\cdot k}{2}$ 圈图：C_n
- **二分图（偶图）**： 完全二分图：$K_{m,n}$ 判定：不包含奇数长度的圈
- $R(p,q)$：满足$R(p,q)$ 个人中，或者有 p 个人相互认识，或者有 q 个人相互不认识

a\b	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1
2	1	2	3	4	5	6	7	8	9	10
3	1	3	6	9	14	18	23	28	32	
4	1	4	9	18	25					

同构 $G_1\cong G_2$

- **必要不充分条件**：1. 顶点数、边数相同 2. 度数列相同（不考虑顺序）3. 对应顶点的关联集及邻域元素个数相同 4. 存在同构的导出子图
- **充要条件**：1. 顶点之间存在双射使得对应边能双射 2. $\overline{G_1}\cong\overline{G_2}$（补图同构，要求简单图） 3. 邻接矩阵可通过行列交换得到
  - 所有对应子图同构
- **自补图**：$G\cong\overline{G}$

矩阵表示

- **邻接矩阵** A： $n\times n$表示两点之间是否有边 A^k 的元素 $a_{ij}^{(k)}$ 表示从顶点 v_i 到 v_j 的长度为 k 的路径数量；行和为出度列和为入度；可拓展$a_{ii}=1$表示自环，$a_{ij}=2$表重

  - 对G中任意三个不同的顶点，存在只包含上面点的初级道路
- **点断集**： 顶点子集 $S\subseteq V$，移除 S 及其关联边后，图 $G-S$ 联通分量增加，但是删除任何真子集联通分量不增加 **点割集**：移除 S 及其关联边后，图 $G-S$ 不再连通或只有一个孤立点 **点割量**：$\kappa(G)=\min|S|:S\subseteq V,$移除 S 后 $G-S$ 不连通。
- **边断集**：边子集 $E'\subseteq E$，移除 E' 后，图 $G-E'$ 联通分量增加，删真子集不增加 **边割集**：删除若干条边变为非联通 **边断量**：$\lambda(G)=\min|E'|:E'\subseteq E,$移除 E' 后 $G-E'$ 不连通

图的遍历

- **Warshall 算法**：计算传递闭包，判断点对间是否存在路径，基于 $P(G)=A+A^2+\cdots+A^{n-1}$。
- **Floyd-Warshall 算法**：求所有点对间最短路径，时间复杂度 $O(n^3)$ 外层为k 运行为 $p_{ij}^k=p_{ij}^{k-1}\vee(p_{ik}^{k-1}\wedge p_{kj}^{k-1})$

欧拉图与哈密顿图

欧拉路与回路

- **定义**：欧拉路：经过每条边一次且仅一次的迹。欧拉回路：起点和终点相同的欧拉路。
- **判别定理**：
  - **无向图**：
    - 欧拉回路：G 连通，所有顶点度数为偶数。 欧拉道路：G 连通，恰有 0 或 2 个奇度顶点。 若有 k 个奇度顶点，可划分为 $k/2$ 条边不重的迹。
  - **有向图**：
    - 欧拉回路：G 强连通，$\forall v, d^+(v)=d^-(v)$。 欧拉道路：G 单向连通，至多一个顶点 $d^+(v)-d^-(v)=1$，至多一个顶点 $d^-(v)-d^+(v)=1$，其余 $d^+(v)=d^-(v)$。

哈密顿路与回路

- **定义**：哈密顿路径：经过每个顶点一次且仅一次的路径（初级）。哈密顿回路：起点和终点相同的路径。
- **必要条件**：
  - 若有哈密顿回路，则 $\forall S\subset V,\omega(G-S)\le|S|$（$\omega(G-S)$ 为删除 S 后连通分支数）。 若有哈密顿路径，则 $\omega(G-S)\le|S|+1$。
  - 若有 **2 度顶点**，其两条边必在哈密顿回路中。 没有**1度顶点 有割点的图不是H图**
  - 二分图有哈密顿回路，则两部顶点集大小相等。

边

- **权矩阵**：无法直接表示重边，在邻接矩阵上加上权
- **关联矩阵**：$n\times m$，元素为+-1 能表示重边但是不能表示自环；出度为正入度为负

列表表示

- **边列表**：(u,v,w) 三维向量保存每条边的起点、终点、权值 排序提高查询效率
- **邻接表**：
  - 正向表/逆向表（有向图） $(n+1)$维向量A m维向量B $B(A(i))\sim B(A(i+1)-1)$都是v_i的后继\前驱
  - 十字链表（有向图） 十字链表用**四个指针域（tail、head、hlink、tlink）在边结点中同时链接出边表和入边**

概念

- **通路 (Walk)**：顶点和边交替的序列
- **简单通路\回路 (Trail)**：**边**不重复的通路\回路
- **路径 (Path) / 初级通路**：**顶点不重复的通路**
- **回路 (Circuit) / 闭通路**：起点和终点相同的通路
- **圈 (Cycle) / 初级回路**：除起点和终点外，其余**顶点**不重复的回路
- **短程线 (Geodesic)**：u,v 间最短路径，距离记为 $d(u,v)$

连通性

- **有向图连通性**：单向连通、强连通、弱连通（视为无向图、为主要讨论的）
- **割点**：顶点 v 是图 G 的割点 $\iff$ 存在与 v 不同的两个顶点 u,w，使得任何从 u 到 w 的路径 P_{uw} 都经过 v $\iff$ 图 $G-v$ 可以划分为两个顶点集 U 和 W，使得对任意 $u\in U$ 和 $w\in W$，所有路径 P_{uw} 都经过 v
- **割边（桥）**：边 e 是图 G 的割边 $\iff$ e 不属于图 G 的任何回路 iff存在 G 的两个顶点 u,w，使得任何一条从 u 到 w 的路径 P_{uw} 都经过边 e $\iff$ 图 G 可以划分为两个顶点集 U 和 W，使得对任意 $u\in U$ 和 $w\in W$，路径 P_{uw} 都经过 e
- **点连通度** $\kappa(G)$ **与边连通度** $\lambda(G)$：
  - 性质：$\kappa(G)\le\lambda(G)\le\delta(G)(最小度)$（Whitney 不等式）
  - 简单联通图中
- **块**：极大无割点的连通子图。连通图 $G(|V|\ge 3)$ 是块的等价性质：
  - 任意两个顶点同属某一初级回路
  - 任意顶点和任意边同属某一初级回路
  - 任意两条边同属某一初级回路
  - 给定两个点 u,v，和边e存在包含e的初级道路P_{uv}
  - 对G中任意三个不同的顶点，存在只包含两点不含第三点的道路

- **充分条件**（简单图，$n\ge 3$）：
  - **Dirac 定理**：若 $\delta(G)\ge n/2$，则有哈密顿回路。若 $\forall v,d(v)\ge(n-1)/2$，则有哈密顿路径。
  - **Ore 定理**：若任意不相邻顶点 u,v，$d(u)+d(v)\ge n$，则有哈密顿回路。若任意两点 u,v，$d(u)+d(v)\ge n-1$，则有哈密顿路径。
  - **闭包理论**：
    - 闭包 $C(G)$：反复连接度数和 $\ge n$ 的不相邻顶点。G 有哈密顿回路 $\iff$ $C(G)$ 有哈密顿回路。若 $C(G)=K_n$，则 G 有哈密顿回路。

最短路径问题

- **单源最短路径**：
  - **Dijkstra 算法**：正权图，时间复杂度 $O(n^2)$ 或 $O(m+n\log n)$（使用堆）。 权为1是退化为 BFS
  - **Bellman-Ford 算法**：可处理负权边（无负权回路），时间复杂度 $O(nm)$。在迭代之后$\pi(i)$不变结束。初始化为∞ 更新 $\pi(i)\leftarrow\min[\pi(i),\min_{j\in\Gamma_i^-}(\pi(i)+w_{ji})]$
- **所有顶点对最短路径**：
  - **Floyd-Warshall 算法**：可处理负权边（无负权回路），时间复杂度 $O(n^3)$。

旅行商问题 (TSP)

- **问题**：给定带正权的完全图，求最短哈密顿回路（NPC 问题）。
- **算法**： **精确算法**：分支定界法将边权值从小到大进行排序，选取构成哈密顿回路的边。复杂度 $O(n!)$，右子树的代价总是大于左子树，右子树的最小代价总是大于等于左子树的任何一条路径，是剪枝的依据。
  - **近似算法**：最近邻点法（贪心）：$O(n^2)$。最廉价插入法：近似比 $\frac{|T'|}{|T_{opt}|}<2$。
- T是一个不断扩充的初级回路，最初T是一个自环，找一个与T**最近的节**点j，将j插入T中
- 假设与T中的最近为t，具体插入的前面或后面， 依据插入后回路T长度增量的大小而定 如果$w(j,t)+w(j,t_1)-w(t,t_1)\le w(j,t)+w(j,t_2)-w(t,t_2)$， 则插到j与$t_1$之间；否则在j与$t_2$之间

中国邮路问题 (CPP)

- **问题**：经过每条边至少一次后返回出发点的最短回路。对于欧拉图自然解决，对半欧拉图，欧拉路径+首尾最短路即可。
- **必要条件**：每条边至多重复一次 对于任意一个回路，重复边长度不超过回路一半。
- **无向图**：1. 找出度为奇的点。2. 依据条件1构造邮路，即G的每条边最多重复一次，并保证计算复杂度边之后度都是偶数3. 由条件2对所有回路进行判断，在G的任

意一个回路上，如果重复边的长度之和超过该回路上度的一半，则令回路中的重复边不重复，不重复边变为重复

- **有向图**：
  - 转化为最小费用最大流问题。

关键路径 (PT)

- 拓扑排序：反复寻找入度为0的节点并更新，要求有向图中没有有向回路。时间复杂度为$O(m+n)$
- **计算从起点开始的最长路径** $\pi(v_j)=\max_{v_i\to v_j}(\pi(v_i)+w(v_i,v_j))$寻找所有前驱点集。
- **事件最晚发生时间** $\tau(v_j)=\pi(v_n)-\pi(v_i,v_n)=\min_{v_j\to v_k}(\tau(v_k)-w(v_j,v_k))$，在计算$\pi(v_i,v_n)$从某个点到终点的最长路径，可以将各边方向调转而权值不变
- **允许延误时间**：$t(v_j)=\tau(v_j)-\pi(v_j)$。

树的定义与性质

- **树**：连通的无回路图 **林**：不含回路的图。
- **等价**（$G=(V,E)$，$n=|V|$，$m=|E|$）：G 是树（连通且无回路）$\iff$ 任意两顶点间有唯一路径。$\iff$ 无回路，且 $m=n-1$。$\iff$ 连通，且 $m=n-1$。$\iff$ 连通，每条边是桥。$\iff$ 无回路，任意加边形成唯一含新边的回路。

支撑树 (Spanning Tree)

- **定义**：包含图 G 所有顶点的树；**树枝**：树中的边；**弦**：非树边。**余树**：$\overline{T}=G-T$
- **最小支撑树 (MST)**：
  - 破圈法：每次去掉回路的一条边。避圈法：使用BFS/DFS，拓展未拓展的点（没有边权情况）
  - **Prim 算法**：贪心选择连接已选和未选点集的最短边，复杂度 $O(n^2)$ 或 $O(m\log m)$。
  - **Kruskal 算法**：按边权从小到大选边，避开形成环，直到选 $n-1$ 条边，复杂度 $O(m\log m)$使用并查集。

支撑树计数

- $G=(V,E)$ 的关联矩阵 B。划去顶点 v_k 对应的行，得到 $(n-1)\times m$ 的 B_k为基本关联矩阵$rank(B)=n-1$，任一 k 阶子方阵 B_0，有 $det(B_0)=0,\pm1$
- C 为 G 中的回路 $\Leftrightarrow$ 各列对应线性相关。B_k 任一 $(n-1)$ 子阵行列式非零 $\Leftrightarrow$ 构成支撑树
- **Binet-Cauchy:** $det(AB)=\sum_{i=1}^{\binom{m}{n}}A_iB_i$，不同树数目为 $det(B_kB_k^T)$。不含 e_i：将 e 对应列删去即可，必含 e_i：将 (i,j) 中 v_i,v_j 收缩为一个点。无向图中计数，任意一条边赋一个方向

- **Kuratowski 定理**：
  - 图是平面图 $\iff$ 不含与 K_5 或 $K_{3,3}$ 同胚的子图（反复插入度为2的结点/边收缩）。
- **对偶图** G^*：每个面对应一个顶点，相邻面间公共边对应一条边。
  - 性质：若 G 连通，$(G^*)^*\cong G$。G 的圈对应 G^* 的割集。G有对偶图 $\iff$ G为平面图 轮图是自对偶图

图的着色

- **点着色**：相邻顶点颜色不同，色数 $\gamma(G)$ 为最小颜色数。
  - **性质**：$\gamma(K_n)=n$，$\gamma(C_{2k})=2$，$\gamma(C_{2k+1})=3$。**Welch-Powell 算法**：按度数递减排序，贪心着色。
  - **色多项式** $f(G,t)$：表示用 t 种颜色着色的方法数。$f(K_n,t)=t(t-1)\dots(t-n+1)$。$f(T_n,t)=t(t-1)^{n-1}$（$n$ 阶树）。
    - 递推：$f(G,t)=f(\overline{G}_{ij},t)-f(\mathring{G}_{ij},t)$ $\quad\gamma(G)=\min\{\gamma(\overline{G}_{ij}),\gamma(\mathring{G}_{ij})\}$ 分别为将两个不相邻的顶点连边、将两个点合并
- **边着色**：相邻边颜色不同，边色数 $\gamma'(G)$。将每条边上设为一个顶点，若关联同一个顶点连上边。**域着色**：转换为对偶图
  - **Vizing 定理**：$\Delta(G)\le\gamma'(G)\le\Delta(G)+1$。轮图$\gamma'(K_n)=n$奇数，为偶数时为$n-1$
  - $\gamma(G)=2\Leftrightarrow$ G为二分图 $\Leftrightarrow$ G中没有奇回路
  - G为域2-可着色 $\Leftrightarrow$ G中有欧拉回路
  - **Brooks定理**: 连通图 G 不是完全图 K_n 且不是奇圈，则有 $\gamma(G)\le d_{max}$ (其中 d_{max} 为图 G 的最大度) 对于任意图，总有 $\gamma(G)\le d_{max}+1$

图的匹配

- **匹配**：边无公共顶点的边集。**最大匹配**：边数最多的匹配，极大匹配是不能再连边。**可增广路径**：两端为非饱和点的交错路径。
- **Berge 定理**：匹配 M 是最大匹配 $\iff$ 无关于 M 的可增广路径。
- **匈牙利算法**：用于二分图最大匹配，寻找可增广路径。
- Step1. 任给一初始匹配 M，给饱和点“1”标记
- Step2. 判断 X 中各顶点是否都已拥有非零标记 若是，结束。M 为最大匹配。否则，找一“0”标记点 $x_0,U\leftarrow\{x_0\},V\leftarrow\emptyset$
- Step3. $\Gamma(U)=V$?
  - 3.1. 否！在$\Gamma(U)-V$中找y_i，判断是否标注1
    - 否！找到从 x 到 y 的可增广路 P 令 $M\leftarrow M\oplus P$ 给 x,y 标记“1”，转 step2
    - 是！则有边$(y_i,z)\in M$那么$U\leftarrow U\cup\{z\}$，$V\leftarrow V\cup\{y_i\}$转3

- 外向树、根树：某点入度为0，其余入度为1。$\vec{B}_k$ 将 G 的基本关联矩阵 B_k 中所有1改为0。v_k 为根，根树数 $det(\vec{B}_kB_k^T)$
- 不含 e 的根数：删去 e 列计算 必含 $e=(u,v)$：作差，或 $G'=G-\{e(u,v)t\neq u\}$

回路和割集矩阵

- 全部初级回路构成矩阵，称完全回路矩阵 $C_e:k\times m$，k 为所有回路数。**基本回路矩阵**: 每条余树枝所对应的回路$C_f:(m-n+1)\times m$，$rank(C_f)=m-n+1$
- B 与 C_e 边次序一致时 $BC_e^T=\vec{0}$。**回路矩阵**: $(m-n+1)$ 个互相独立回路构成矩阵 C，$C:(m-n+1)\times m$有$BC^T=\vec{0}$。$C=PC_f$，P 为非奇异方阵
- 任一 $(m-n+1)$ 行列式非零当且仅当列对应余树
- $C_f=(I\ C_{f12})$ $\quad B_k=(B_{11}\ B_{12})$ $\quad C_{f12}=-B_{11}^TB_{12}^{-T}$ $\quad B_{12}$ 对应一棵树
- S 为割集，G 的全部割集组成矩阵，为完全割集矩阵 S_e $\quad S_e:k\times m$，k 为割集数，$rank(S_e)=n-1$
- **基本割集**: S_i 中只有一条树边 e_i 及余树边，与 e_i 方向一致 $\quad S_f$: 基本割集矩阵，只有基本割集，$(n-1)\times m$ 边次序一致 $S_eC_e^T=0$
- $(n-1)$ 个相互独立割集构成割集矩阵 S $\quad SC^T=\vec{0}$ $\quad S=PS_f$ $\quad P$ 可逆，S 次序与 S_f 一致
- $S_f=(S_{f11}\ I)$ $\quad C_f=(I\ C_{f12})$ $\quad S_{f11}=-C_{f12}^T$ 边次序一致
  $S_{f11}:(n-1)\times(m-n+1)$ $\quad C_{f12}:(m-n+1)\times(n-1)$
- $S_{f11}=B_{12}^{-1}B_{11}$，$B_{12}$ 为树，B_{11} 为树余

Huffman 编码

- **目标**：构造带权路径长度 $WPL=\sum w_il_i$ 最小的二元树（w_i 为叶子权，l_i 为路径长度）。
- **Huffman 算法**：每次合并权值最小的两个节点，复杂度 $O(n\log n)$。生成最优前缀码（无码字是另一码字前缀）。

平面图

- **定义**：可画在平面上且边不相交的图。
- **面（域）**：外部面（无限面），内部面（有限面）。 面度 $\deg(R)$：边界边数。$\sum_{R\in F}\deg(R)=2m$（对偶图的握手定理）。
- **欧拉公式**（连通平面图）：$n-m+d=1+k$（n：顶点数，m：边数，d：面数，k：联通支数目）。没有割边情况下$m\le\frac{t(n-2)}{t-2}$（每个域边界数至少为t）
- **推论**：简单平面图（$n\ge3$）：$m\le3n-6$，$d\le2n-4$（极大平面图取等）。
  - 极大平面图有G是联通的，不存在割边，$3d=2m$，每个域的边界数为3（**充要条件**）
  - 无K_3子图：$m\le2n-4$。 最小度 $\delta(G)\le5$。

  - 3.2. 是！搜索完毕没找到，x 无法扩大匹配，给 x 标记“2”，转 step2
- **完美匹配**：$|M|=|X|=|Y|$，$|M|=|X|$为完全匹配，存在完全匹配 $\iff$ 对于X的任意子集A有$|\Gamma(A)|\ge|A|$
- **Hall 定理**：存在完美匹配 $\iff\forall x\in X\ d(x)\ge k\quad\forall y\in Y\ d(y)\le k$
- X到Y的最大匹配为$|X|-\delta(G)$其中$\delta(G)=\max\delta(A),A\subset X,\delta(A)=|A|-|\Gamma(A)|$
- **Kőnig 定理**：二分图中，最大匹配边数（相当于邻接矩阵中不在同行同列的非零元最多个数） = 邻接矩阵最小点覆盖数（用最少的行或列盖住非零元）

网络流

- **网络**：有向图 $N=(V,E,c,s,t)$，c 为边容量，s 为源点，t 为汇点。
- **可行流** f：满足容量限制：$0\le f_{ij}\le c_{ij}$ 流量守恒：除 s,t 外，流入 = 流出。
- **流量值** $|f|$：源点流出的总净流量
- **割** $(S,\bar{S})$：$s\in S,t\in\bar{S}$，容量 $C(S,\bar{S})=\sum_{u\in S,v\in\bar{S}}c(u,v)$。
- **最大流最小割定理**：最大流值 = 最小割容量：$\max|f|=\min C(S,\bar{S})$
- **增流路径**为s到t的（无向）初级路径**所有边均为向前边**中总有$f_{ij}\le c_{ij}$令$\delta=\min(c_{ij}-f_{ij})$为增流 初始化流为 0。在残余网络中找增流路径，增加流量，直至无增流路径。
- 如果有向后边边，那么在向前边中$\delta_1=\min(c_{ij}-f_{ij})$，在向后边中$\delta_2=\min f_{ji}$，增流为$\delta=\min(\delta_1,\delta_2)$，若向前边+1向后边要-1
- **Ford-Fulkerson 算法**：对于流量非饱和边计算δ，标号为$\delta(v_j)=\min\{\delta(v_i),\delta\}$
- **Edmonds-Karp 算法**：按照先标号先检查的顺序进行，Ford-Fulkerson 的 BFS 实现，复杂度 $O(nm^2)$。

代数系统与性质

- $gf=I_A$：f为左可逆映射，g是f的的一个左逆映射。f左可逆 $\iff$ f为单射，f右可逆 $\iff$ f满射，f可逆 $\iff$ f为双射
- **等价关系**R，要求自反、传递、对称。商集为$\overline{A}=\{\bar{a}|a\in A\}$记为$A/R$，$a\to\bar{a}$称为$A\to A/\sim$的自然映射
- **代数定义**：$f:A^n\to A$为n元运算，**非空集合** S 和一个或多个**封闭**运算 f，记为$\langle S,f\rangle$。
- **单位元**：e 满足 $e*a=a*e=a$，$e_L\cdot x=x$ 有左单位元和右单位元则相等且唯一
  - **逆元**：$x'\cdot x=e$，x'为x的左逆。若存在左逆 x' 和右逆 x''，且满足**结合律**，则 $x'=x''$，唯一，并且$(x^{-1})^{-1}=x$ **零元**：$z*a=a*z=z$
- **消去律**：对于非零元a左消去：$a*b=a*c\implies b=c$ 右消去：$b*a=c*a\implies b=c$

- **同类型**：所有运算同为k_i元运算 **同态映射**：映射 $h:\langle X,*\rangle \to \langle Y,\cdot\rangle$，满足 $h(x*y)=h(x)\cdot h(y)$。f为单射，称f为单一同态，f为满射，称为满同态，$X\sim Y$，称Y为X的同态象。**同构映射**：双射的同态$f:X\to Y$，称为$X\cong Y$
  - **性质**（满同态）：保持运算性质（交换律、结合律），$h(e)$ 是 S' 的单位元，$h(x^{-1})$ 是 $h(x)$ 的逆元。
- **子代数**：子集 $R\subseteq S$ 在运算 $*$ 下封闭，构成 $\langle R,*\rangle$ **自同态、自同构** 为$X\to X$的映射

幺半群与半群与群

- **半群**：满足结合律的代数（**封结**） **幺群**：满足结合律且有单位元的**半群**（**封结幺**）满足结合律也满足$a^m a^n=a^{m+n},\quad (a^m)^n=a^{mn}\ m,n\in \mathbf{Z}$
- **交换幺群**：满足交换律的含幺**半群** **循环**：存在生成元 g，$M=\{g^k:k\in\mathbb{N}\}$，循环幺群是可交换幺群
- f为同态$(S,\cdot)$为半（幺）群$(f(S),*)$也是半（幺）群；满同态下$(B,*)$也是半（幺）群；$(f(S),*)$是$(B,*)$的子半群
- **子半群**：$T\subset S$在运算$\cdot$的作用下如果T是封闭的那么称$(T,\cdot)$是$(S,\cdot)$的子半群。若$e\in T$那么称$(T,\cdot)$为$(S,\cdot)$的子幺半群
- **群**：幺半定义基础上，每个元素有逆元(**封结幺逆**) **阿贝尔群**：满足交换律
  - **性质**：满足消去律，若$ab=ba$有$(ab)^n=a^nb^n$，半群中有方程 $a*x=b$ 和 $y*a=b$ 都有解，则为群。 **有限半群满足消去律必为群**，无限半群的反例为$(N^*,\times)$；**有限群**中有$a_iG=G$，无限群的反例为$(\mathbb{Z},+)$。群中没有吸收元
  - **Klein 四元群**：$V_4=\{e,a,a,b,c\}$，每个元素 $x^2=e$，a,b,c任何两个元素的运算为第三个元素，为最小的非循环群
  - 半群有一个**固定的**左单位元，也有左逆元则这个半群是群。半群中任意两个元素a,b，方程$ax=b,ya=b$在半群中都有解，则为群。
  - **群的阶（Order）**： 群的阶指群中元素个数，记作 $|G|$。**元素的阶**：群元素 a 的阶是使得 $a^n=e$ 的最小正整数 n，若 a 的阶为 k，则 $a^m=e\iff k\mid m$。$O\langle a\rangle=O\langle a^{-1}\rangle$元素的阶相等
  - 有限群中，所有元素的阶都有限$r\le|G|$，且整除群阶。所有元素的阶都是有限的群不一定是有限群：$(P(N),\oplus)$；单位元的阶只能为1。
  - **子群**：子代数 $\langle H,*\rangle$ 自身为群。**判定**：$H\subseteq G$ 是子群 $\iff$ **非空**，且$\forall a,b\in H,ab^{-1}\in H$。**子群的交仍然为子群**。$\langle a\rangle$是$G$的子群。
  - 对于群G及其子群H，有$HH=H$；对于群G及其子集H，若$HH=H$不一定有H为G子群，非0有理数上的乘法与全体奇数；存在群是三个真子群的并：Klein四元群，但是不可能为两个真子群的并；不存在无限群只有有限个子群；存在无限群，只有一个/两个元素的阶有限。
  - 群中左逆元也是右逆元，左单位元也是右单位元
  - **推论**：元素的阶是群阶的因子。阶为素数 p 的群是循环群。子群 A,B：$|AB|=\frac{|A||B|}{|A\cap B|}$，其中 $AB=\{ab:a\in A,\ b\in B\}$。
- **正规子群**：$H\lhd G\iff\forall g\in G,\ gH=Hg$；$\le$ 为普通子群符号
  - **等价条件**：$\forall g\in G,\quad gHg^{-1}=H\quad;\quad\forall g\in G,\quad gHg^{-1}\subseteq H\quad;\quad\forall g\in G,\forall h\in H,\ ghg^{-1}\in H$
  - 若 $A\lhd G,\ B\lhd G$，则 $A\cap B\lhd G,\ AB\lhd G$；若 $A\lhd G,\ B\le G$，则 $A\cap B\lhd B,\ AB\le G$
  - **性质**：交换群的子群均为正规。指数为 2 的子群必正规。
- **商群**：若 $H\lhd G$，则 $G/H=\{gH:g\in G\}$ 在运算 $(aH)(bH)=(ab)H$ 下为群。单位元为 H。

对换群&置换群

- **定义**：由一个生成元 a 构成：$G=\langle a\rangle=\{a^k:k\in\mathbb{Z}\}$。 循环群必为阿贝尔群。
- **有限循环群**：阶 n，$G=\{e,a,a^2,\dots,a^{n-1}\}$。 生成元：$a^k$ 是生成元 $\iff\gcd(k,n)=1$，共有 $\phi(n)$ 个（ϕ 为欧拉函数）。无限阶循环群的生成元只有两个：a 和 a^{-1}。
- **子群**：循环群的子群仍是循环群。n 阶循环群对每个因子 $d|n$ 有唯一 d 阶子群$\langle a^{\frac{n}{d}}\rangle$，最小正幂为生成元。无限阶循环群的非平凡子群也是无限阶循环群。
- **同构**：无限循环群同构于 $\langle\mathbb{Z},+\rangle$。$n$ 阶循环群同构于 $\langle\mathbb{Z}_n,+_n\rangle$；同阶循环群同构。
- **变换**：$A\to A$的映射称为变换有n^n个（有限），若为满射或单射，则为双射（一一变换）。所有一一变换关于变换的乘法所作成的群叫做A的一一变换群，用$E(A)$表示，$E(A)$ 的子群为变换群
- **置换**：**有限集合**到自身的双射$n!$个。A中的一个一一变换称为一个n元置换，由置换构成的群称为置换群
- **对称群** S_n：n 个元素的**所有**置换在置换乘法下构成的群，阶 $|S_n|=n!$。S_n的子群为n元置换群
- **轮换**：如 $(a_1a_2\dots a_k)$，表示 $a_1\to a_2,\dots,a_k\to a_1$。置换可唯一分解为**不相交**轮换的乘积。**不相交的轮换**（没有公共元素）可交换；Sn中任意一个n元置换，一定可以表示成不相交轮换的乘积的形式，并且表示法是唯一的。$\sigma=(i_1,i_2,\dots,i_k)$的阶为 k。轮换的奇偶性与k无关。
- **轮换的计算**：$\sigma=(i_1,i_2,\dots,i_k)$，$\sigma=(i_1\ i_2)(i_2\ i_3)\cdots(i_{k-2}\ i_{k-1})(i_{k-1}\ i_k)$，$\sigma=(i_1\ i_k)(i_1\ i_{k-1})\cdots(i_1\ i_3)(i_1\ i_2)$
- **逆序数**：置换 σ 的逆序数 $inv(\sigma)$ 为 $\{(i,j)|i<j,\sigma(i)>\sigma(j)\}$ 的个数。奇置换（偶置换）是逆序数为奇（偶）的置换。两个奇置换/偶置换的乘积为偶置换，奇置换和偶置换的乘积为奇置换；置换$\boldsymbol{\sigma}$是偶置换当且仅当σ^{-1}是偶置换/$\tau^{-1}\sigma\tau$为偶置换
- **对换**：长度为 2 的轮换。置换可分解为对换，奇偶性（对换个数奇偶）唯一。
- **交错群** A_n：S_n 中偶置换的子群，阶 $|A_n|=\frac{n!}{2}$。
- **Cayley 定理**：任意群同构于某变换群。设G是n阶有限群，则G与S_n的一个子群同构，有限群 G 与一个置换群同构。

陪集&正规子群与商群

- **陪集**：左陪集：$aH=\{ah:h\in H\}$，右陪集：$Ha=\{ha:h\in H\}$。
  - **性质**： $a\in H\iff aH=H$。无论 a 是否在 H 中，都有 $|aH|=|H|$；左（右）陪集或相等或不相交，构成 G 的划分。指数 $[G:H]$ = 不同陪集数 = $\frac{|G|}{|H|}$。
  - $\forall x\in aH$，都有 $xH=aH$，并叫 a 是 aH 的一个陪集代表；$aH=bH\iff a\in bH$ 或 $b\in aH\iff b^{-1}a\in H$ 或 $a^{-1}b\in H$
- **Lagrange 定理**：有限群 G 中，子群 H 的阶整除 G 的阶：$|G|=[G:H]\cdot|H|$