离散数学

1.重言式的基本概念/重言式的基本定义：设A为任一命题公式。若A在它的各种赋值下取值均为真，则称A是重言式或永真式。

2.主析取范式的基本概念：由n个命题变项构成的析取范式中所有的简单合取式都是极小项，则称该析取范式为主析取范式。

3.主合取范式的基本概念：由n个命题变项构成的合取范式中所有的简单析取式都是极大项，则称该合取范式为主合取范式。

4.集合之间映射的定义：设X,Y是两个集合，f是X到Y的一个关系。如果对任一x∈X，都有唯一的y∈Y，使得<x,y>∈f，则称关系f为函数\映射，

记作f：X——>Y，称f是X到Y的函数\映射

5.两个有限集合建立普通映射时：设|X|=m，|Y|=n，则从X到Y可定义 n^m 个不同的函数。

6.两个有限集合之间可以建立单射时，集合之间元素个数之间的关系：设|X|=m，|Y|=n（可知m≤n），则从X到Y可定义A^m_n（上标m，下标n）个单射

7.一个有n个元素集合可以建立自身到自身单射的数目：设|X|=n，|Y|=n，则从X到Y可定义 n! 个单射

8.群G的元素个数是其子群元素个数的倍数，例如20个元素个数的群不会有7个元素个数的子群等等

9.有限群G的子群H左右陪集个数的关系(相等)

10.一个群中的元素a的阶数m给定，则a^k 的阶数是？ m/(m,k) p191-192

下列名词的基本概念

1.等价关系：集合上的二元关系R同时具有自反性，对称性和传递性，则称R是A上的等价关系。

2.永真式：同重言式

3.置换：一个有限集合的一个一一变换称为一个置换。（一个集合到自身之间的一一映射称为变换）

4.群：一个代数系统G称为一个群，满足下列条件：

（1）结合律成立，即对任意的a，b，c∈G有（$a\circ b$）$\circ c=a\circ$（$b\circ c$）。

（2）存在单位元e：即对任意的a∈G，有$e\circ a=a\circ e=a$。

（3）对G中任意元a，存在a^{-1}属于G，使$a\circ a^{-1}=a^{-1}\circ a=e$，元a称为可逆的，$a^{-1}$叫做a的一个可逆元。

5.互素：若（$a_1, a_2, \ldots, a_n$）=1（即最大公因数为1），则称$a_1, a_2, \ldots, a_n$互素

6.哈斯图：
图中的每个结点表示集合A中的一个元素，结点的位置按它们在偏序中的次序从底向上排列。即对任意a，b属于A，若a<b(a≤b∧a≠b)，则a排在b的下边。如果a<b，且不存在c∈A满足a<c<b，则在a和b之间连一条线。这样画出的图叫哈斯图。

7.同余：设a,b∈Z，m是一个正整数，如果用m分别去除a和b，所得余数相同，则称a和b关于模m同余。

8.域：
一个至少有两个元素的整环R叫做一个域，且R的每一个不等于零的元素有一个逆元。

9.划分：
若把一个集合A分成若干个叫做分块的非空子集，如果A中每个元素属于且仅属于一个分块，那么这些分块的全体构成的集合叫做A的一个划分。

计算+证明

1.给定正整数m，计算模m的全部等价类，给出模m的标准剩余系，和既约剩余系

P136-137（概念）

（编）求模4的全部等价类，标准剩余系，既约剩余系。

等价类：[0]={…,-8,-4,0,4,8,…},

[1]={…,-7,-3,1,5,9,…},

[2]={…,-6,-2,2,6,10,…},

[3]={…,-5,-1,3,7,11,…}

完全剩余系：从四个等价类中分别取出一个数字组成，如{0，1，2，3}或{0，5，6，3}……

标准剩余系：{0，1，2，3}(唯一)从完全剩余系选择除去负数的最小余数的组合

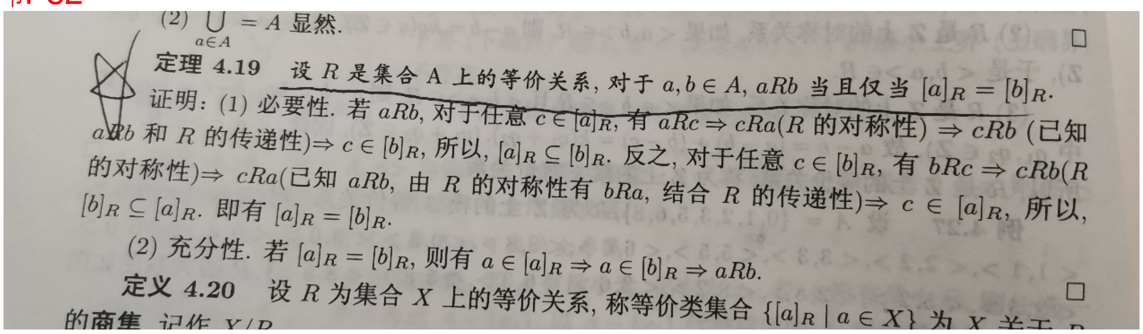
既约剩余系：从完全剩余系中选择出与4互素的数字组成如{1，3}或{5，3}……

既约标准剩余系：{1,3}(唯一)从既约剩余系中选择除去负数的最小余数的组合

2.给定一个集合，计算集合上的已有两个关系的复合关系，复合关系的关系矩阵(例题P67-68)

3.证明：一个集合上的等价关系R给定，元素a,b所在的等价类为[a],[b]，则[a]=[b]的充要条件是a与b有关系

书P82



(2) $\bigcup_{a\in A} = A$ 显然. □

定理 4.19 设 R 是集合 A 上的等价关系, 对于 $a,b\in A$, aRb 当且仅当 $[a]_R=[b]_R$.

证明: (1) 必要性. 若 aRb, 对于任意 $c\in[a]_R$, 有 $aRc\Rightarrow cRa$(R 的对称性) $\Rightarrow cRb$ (已知 aRb 和 R 的传递性)$\Rightarrow c\in[b]_R$, 所以, $[a]_R\subseteq[b]_R$. 反之, 对于任意 $c\in[b]_R$, 有 $bRc\Rightarrow cRb$(R 的对称性)$\Rightarrow cRa$(已知 aRb, 由 R 的对称性有 bRa, 结合 R 的传递性)$\Rightarrow c\in[a]_R$, 所以, $[b]_R\subseteq[a]_R$. 即有 $[a]_R=[b]_R$.

(2) 充分性. 若 $[a]_R=[b]_R$, 则有 $a\in[a]_R\Rightarrow a\in[b]_R\Rightarrow aRb$. □

定义 4.20 设 R 为集合 X 上的等价关系, 称等价类集合 $\{[a]_R\mid a\in X\}$ 为 X 关于 R 的商集, 记作 X/R.

4.群的子群的定义是什么？

假如H对于G的乘法来说组成一个群，群G的一个非空子集H叫做G的一个子群。

任意群G至少有两个子群，它们是单位元组成的一个元素的群和G自身。这两个子群一般称为群的平凡子群。

5.一个群的两个子群的并集不一定是群，交集一定是群，举反例和证明

书P207

$[0]\in H, [4]+[4]=[8]\in H, [4]+[8]=[0]\in H$,

$[8]+[8]=[4]\in H$.

例 7.56 群 G 的两个子群 H 与 K 的交集 $H\cap K$ 也是 G 的一个子群. 定理7.26

证明: 设 G 的单位元为 e, 因为 $e\in H$, $e\in K$, 可知 $e\in \cancel{K}H\cap K$, 从而 $H\cap K\neq\varnothing$. 对于任意的 $a,b\in H\cap K$, 因为 H 和 K 都是子群, 所以 $ab^{-1}\in H$ 和 $ab^{-1}\in K$, 从而 $ab^{-1}\in H\cap K$, 这就证明了 $H\cap K$ 是子群.

例 7.57 举例说明群 G 的两个子群 H 与 K 的并集 $H\cup K$ 可能不是 G 的一个子群. 定理7.27

解: 对于模 12 的剩余类加群 $\mathbf{Z}_{12}$, 不难验证 $H=\{[0],[4],[8]\}$, $K=\{[0],[6]\}$ 是 $\mathbf{Z}_{12}$ 的两个子群, 但是 $H\cup K=\{[0],[4],[6],[8]\}$ 不是 $\mathbf{Z}_{12}$ 的子群, 这是因为 $[4]+[6]=[10]\notin H\cup K$.

一个循环群的子群还是循环群吗? 下面的定理作了说明.