离散数学Chapter 5：群、环和域

- 5.1 半群和独异点
  - 一、半群和独异点的基本概念
    - 半群，交换半群
      - 设 S 是一个非空集合，* 是 S 上的一个二元运算，如果* 是可结合的，则称代数系统 <S；* > 是半群。
      - 若在半群 <S；* > 中，运算 * 满足交换律，则 <S；* > 称为交换半群
    - n次幂，指数
      - 设<S；* >是一个半群，则对任意的 x ∈ S 和任意正整数 n，定义 x 的 n次幂为
      - $x^1 = x$，$x^{n+1} = x^n * x$（$n \in Z^+$）
      - 并称 n 为 x 的指数
      - 定理：
        - 设<S；* >是一个有限的半群，则必有 a ∈ S，使得 a 是一个幂等元，即 a * a = a
    - 独异点，交换独异点
      - 若半群<S；*> 中运算 * 有单位元，则称该半群为独异点。
      - 若独异点<S；*>中运算 * 满足交换律，则称该独异点为交换独异点。
      - 注意：
        - 独异点中唯一的单位元常记为 *e*。
        - 设 <S；*> 为有限独异点，则关于运算 *的运算表中没有两行或两列是相同的。
    - 循环独异点,生成元
      - 在独异点<S；*> 中，如果存在元素 $g \in S$，使得 *S* 中的每一元素 *a* 都能写成 g^i（$i \in N$）的形式，则称独异点 <S；*> 为循环独异点，元素 *g* 称为该循环独异点的生成元。
      - 定理：
        - 每一个循环独异点都是可交换的。
        - 设<S；* >是一个有限的独异点，则对每一 a ∈ S，存在正整数 j，使得 a^j 是一个幂等元
        - 设<S；* >是是独异点，且 S 中所有元都可逆，则对任意的 a，b ∈ S
          - (1) $(a^{-1})^{-1} = a$
          - (2) $(a*b)^{-1} = b^{-1} * a^{-1}$
  - 二、子半群和子独异点
    - 子半群,子独异点

- <S；*>是一个半群，若<H；*>是<S；*>的子代数，则称<H；*>是<S；*>的子半群。
- 设<S；*>是一独异点，若<H；*>是<S；*>的子代数，且单位元$e \in H$，则称<H；*>是<S；*>的子独异点。
- 注意：
  - 子半群（子独异点）也是一个半群（独异点）。
  - 半群（独异点）是自身的一个子半群（子独异点）。
  - <{e}；*>也是独异点<S；*>的子独异点
- 定理：
  - 设<S；*>是一个可交换的独异点，则S的所有幂等元的集合形成<S；*>的一个子独异点。

- **三、半群和独异点的同态**
  - **代数系统的同态（单同态、满同态）、同构和积代数的概念以及一些有关的结论可以推广到半群和独异点中**
  - 设h是从代数系统$V_1 =< S_1；* >$到$V_2 =< S_2；\circ >$的满同态，其中运算*和$\circ$都是二元运算。
    - （1）若$V1$是（交换）半群，则$V2$也是（交换）半群。
    - （2）若$V1$是（交换）独异点，则$V2$也是（交换）独异点。
    - **注：**
      - 可以利用此定理判断某些代数系统是半群或独异点。
  - （交换）半群的同态像是（交换）半群，（交换）独异点的同态像是（交换）独异点。
  - 给定代数系统$V1$=<*S*1；*>和$V2$=<*S*2；∘>，其中运算*和∘都是二元运算，则
    - （1）若$V1$，$V2$是（交换）半群，则$V1 \times V2$也是（交换）半群。
    - （2）若$V1$，$V2$是（交换）独异点，则$V1 \times V2$也是（交换）独异点。

- **5.2 群**
  - **一、群的基本概念**
    - **1．群的定义**
      - **群，交换群，阿贝尔群**
        - 设<G；*>是一个代数系统，如果G上的二元运算满足下列条件，则称<*G*；*>是一个群，简记成群G。
          - *（1）运算*是可结合的；*
          - **（2）存在单位元$e \in G$；**
          - **（3）G中所有元素都可逆。**
        - 如果群<G；*>的运算*是可交换的，则称该群为交换群或阿贝尔群。

- 设<G；*>是一个代数系统，如果<G；*>是独异点，且G中所有元素都可逆，则<G；*>是一个群。
  - 注意：
    - 若 <*G*；*> 是群，且 # G >1，则 <*G*；*> 无零元。
    - 若 <*G*；*> 是群，则 <*G*；*> 中唯一的幂等元是单位元 e

- **2．群中元素的幂**
  - 幂
    - 设 <*G*；*> 是群，则对任意的 $x \in G$，定义 x 的幂为
      - $x^0 = e$， $x^{n+1} = x^n * x$， $x^{-n} = (x^{-1})^n$　其中 $n \in \mathbf{N}$。
    - 也满足以下两式
      - $x^m * x^n = x^{m+n}, (x^m)^n = x^{mn}$
      - $x^{-n} = (x^{-1})^n = (x^n)^{-1}$

- **3．群的阶和元素的周期**
  - 阶，有限群，无限群
    - 设 <*G*；*>是群，若 G 是有限集，则称<*G*；*>是有限群，G 中元素的个数称为群<*G*；*>的阶；若 G 是无限集，则称<*G*；*>是无限群。
  - 有限周期，有限阶，周期，阶
    - 设 < G；* >是群，$a \in G$，若存在正整数r，使得 $a^r = e$称元素a具有有限周期或有限阶。使 $a^r = e$成立的最小的正整数r称为 a 的周期或阶。
    - 如果对于任何正整数r，均有 $a^r \neq e$，则称 a 具有无限周期或无限阶。
    - 注意：
      - **群中单位元具有有限周期，且周期是 1。**

- **二、群的基本性质**
  - **1．消去律**
    - 设 <*G*；*> 是群，则对任意的a，$b \in G$，
      - （1）存在唯一的元素$x \in G$，使 a * x = b。
      - （2）存在唯一的元素$y \in G$，使 y * a =b。
      - **注：**定理说明在群中方程 a * x=b 与 y * a = b 有唯一解。
    - 左消去律，右消去律
      - 设<*G*；*> 是群，则运算 * 满足消去律，即对任意的 a，b，$c \in G$
      - （1）若 a * b = a * c，则 b = c；

        左消去律
      - （2）若 b * a = c * a，则 b = c。

        右消去律
      - 设 < G；*> 是群，且对任意的 a，$b \in G$，有 $(a * b)^n = a^n * b^n$，则 < G；*> 是阿贝尔群，反之也成立
  - **2.元素运算后的逆元**

- 设<*G*；*>是一个群，则对任意的a，$b\in G$，有
  - $(a^{-1})^{-1}=a,(a*b)^{-1}=b^{-1}*a^{-1}$
- **3．关于元素的周期**
  - 若群<*G*；*>中元素 a 具有有限周期r，则$a^k=e$当且仅当 $r|k$，即 k 是 r 的整数倍
  - 定理：
    - 群中任一元素与它的逆元具有相同的周期。
      - 说明：群中任意元a的逆元的周期是 a的周期的因子。
      - **注：**定理的证明说明，群中任一元素与它的逆元要么具有有限的周期且相等，要么具有无限周期，不可能出现一个为有限周期而另一个为无限周期。
    - 在有限群中，每个元素均具有有限周期，且周期不超过群的阶。

三、群的同态

- 代数系统的同态（单同态、满同态）、同构和积代数的概念以及一些有关的结论也可以推广到群中。
  - 设 h 是从代数系统 $V_1=<G_1;*>$ 到代数系统$V_2=<G_2;*>$ 的满同态，其中运算 * 和 ∘ 都是二元运算，若 $V1$ 是（交换）群，则 $V2$ 也是（交换）群。
    - **注：**可以利用此定理判断某些代数系统是群。
  - 推论:(交换）群的同态像是（交换）群。
  - 给定代数系统 $V1$ = <*G*1；*> 和 $V2$ = <*G*2；∘>，其中运算 * 和 ∘ 都是二元运算，若 $V1$ 和 $V2$ 是（交换）群，则 $V1\times V2$ 也是（交换）群。

5.3 置换群与循环群

一、置换群

1．置换的概念

- n元置换
  - 设 A ={$a1$，$a2$，…，an} 是一个非空有限集合，A 上的双射函数称为A 的 n 元置换。
  - 一个 n 元置换 f：A→A 常表示成如下形式，这里n个列的次序是任意的。

$$f=\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ f(a_1) & f(a_2) & \dots & f(a_n) \end{pmatrix}$$

  - 注意：
    - 设 f 是集合 A = {$a1$，$a2$，…，an} 上的一个 n 元置换，则 f($a1$)，f($a2$)，…，f(an) 必为 $a1$，$a2$，…，an 的一个排列。
      - 因为 f 是双射，故 f($a1$)，f($a2$)，…，f(an) 各不相同，但所有f(ai) 都是 A 中的元素，且# A = n，因此结论成立。
    - 集合 A 上不同的 n 元置换的数目为***n*!** 个。

- 恒等函数 I_A 是集合 A上的一个置换，称为A 上的恒等置换。
- 设 f1 和 f2 是 A 上任意两个置换，则f1 和 f2 的复合f1∘f2 也是 A 上的一个置换。其中f1∘f2 表示置换 f1 后再接着置换f2 所产生的一种置换（类似于关系的复合），即
  - $f_1 \circ f_2 = f_2(f_1(x)), \forall x \in A$
- 集合 A 上的任意置换f的逆函数 f^{-1}也是 A 上的置换，称为f的逆置换。

- **2．置换群的概念**
  - n 次对称群,n 次置换群

    置换群对称群
    - 基数为n 的集合 A 上的**所有**置换的集合，对于置换的复合运算∘构成一个群，称为 n 次对称群。
    - 集合A 上的**若干**置换的集合，对于置换的复合运算∘构成的群，称为 n 次置换群。
    - 注意：
      - （1）n 次对称群是一个n 次置换群。对称群与置换群一般不是交换群。
      - （2）置换群是最早研究的一类群，而且它是一类重要的非交换群。更为重要的是，每个有限群都与一个置换群同构（凯莱定理），从而任何有限的抽象群可以转化为一个置换群进行研究。
      - （3）对称群的概念首先是伽罗瓦（ÉvaristeGalois，1811-1832，法国数学家）建立的，他创造这个概念来证明四次以上的一般多项式不能用根号解出。从历史来讲，研究群首先研究的是对称群。

- **二、循环群**
  - **1．循环群的概念**
    - 循环群，生成元，生成
      - 在群<G；*> 中，如果存在元素 g ∈ G，使得每一元素 a ∈ G 都能表示成 g^i（i ∈ **Z**）的形式，则称群 <G；*> 为循环群，称 g 为该循环群的生成元，并称群 <G；*> 由 g 生成。
      - 注意：
        - 每一循环群必是交换群。
        - 若 g 是循环群 < G；*>的生成元，则g^{-1} 也是该群的生成元。
        - 每个元都是生成元的循环群

【例 5.17】群 $<N_5; \oplus_5>$ 是循环群。

因为

$1^0=0,\ 1^1=1,\ 1^2=1\oplus_5 1=2,$

$1^3=1^2\oplus_5 1=2\oplus_5 1=3,$

$1^4=1^3\oplus_5 1=3\oplus_5 1=4,$

所以 1 是其生成元。又

$2^0=0,\ 2^1=2,\ 2^2=4,\ 2^3=1,\ 2^4=3$

$3^0=0,\ 3^1=3,\ 3^2=1,\ 3^3=4,\ 3^4=2$

$4^0=0,\ 4^1=4,\ 4^2=3,\ 4^3=2,\ 4^4=1$

所以 2，3，4 也是其生成元。

注：本例说明

（1）循环群的生成元一般不唯一。

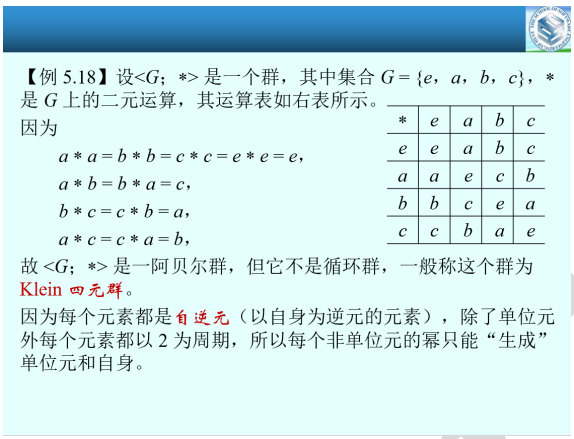
（2）存在循环群，除单位元外，每个元都是生成元。

$\oplus_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

【问题】“除单位元外，每个元都是生成元”的循环群有何特征？

50

- Klein 四元群，自逆元



【例 5.18】设$<G; *>$是一个群，其中集合 $G=\{e, a, b, c\}$，$*$ 是 G 上的二元运算，其运算表如右表所示。

因为

$a*a=b*b=c*c=e*e=e,$

$a*b=b*a=c,$

$b*c=c*b=a,$

$a*c=c*a=b,$

故 $<G; *>$ 是一阿贝尔群，但它不是循环群，一般称这个群为 Klein 四元群。

因为每个元素都是自逆元（以自身为逆元的元素），除了单位元外每个元素都以 2 为周期，所以每个非单位元的幂只能“生成”单位元和自身。

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

- **2．循环群的性质**
  - 在循环群中，生成元的周期可决定群的阶。
  - 设 < G ; * > 是由元素 g 生成的循环群，
    - （1）若 g 的周期为 n，则 < G ； *> 是一个 n 阶的有限循环群；
    - （2）若 g 的周期为无限，则< G ； *> 是一个无限阶的循环群。
    - **注：**循环群的生成元一般不唯一，**但生成元的周期与所生成的循环群的阶是一样的。**
  - 推论：设 <G；*> 是 n 阶循环群，g 是生成元，则 $G=\{g, g^2, \ldots, g^n\}$
  - 推论：设<G；*> 是n阶循环群，g是生成元，则生成元g的周期也是n。
- **5.4 子群及其陪集**
  - **一、子群的定义**
    - 子群，真子群，平凡子群
      - Def_1:设<G；*>是一个群，<H；*>是<G；*>的子代数，若单位元e∈H，且对任意的a∈H，有a^{-1}∈H，则称<H；*>是<G；*>的子群。
      - Def_2:设 <G；*> 是群，H 是 G 的非空子集，若 <H；*> 也是群，则称 <H；*> 是 <G；*> 的子群。
      - 若 H 是 G 的真子集，则称子群 <H；*> 是<G；*> 的真子群。
      - 注意：
        - 群 $<G; *>$ 的任一子群本身也是一个群。
        - 群 <G；*> 的两个子群 <G；*> 与 <{e}；*> 称为 <G；*> 的平凡子群。

        - 交换群的子群也是交换群。
        - n次置换群是n次对称群的子群。
    - 定理：
        - 设<G；*>是一个群，H是G的非空子集，若<H；*>也是群，则<H；*>必是<G；*>的子群。
- **二、子群的判别**
    - 要判断非空子集$H \subseteq G$对运算*能否构成群<G；*>的子群，需要弄清：
        - 封闭性：对任意的a，$b \in H$，是否有$a * b \in H$;
        - 单位元：是否有$e \in H$;
        - 可逆性：对任意的$a \in H$，是否有$a^{-1} \in H$。
    - **子群定义中对单位元e的要求可由封闭性和可逆性推出。**
    - 判别法：
        - 定理 5.17
            - 设<G；*>是群，H是G的非空子集，若
                - （1）对任意的a，b∈H，有a*b∈H，
                - （2）对任意的a∈H，有$a^{-1} \in H$，
            - 则<H；*>是<G；*>的子群。
        - 定理 5.18
            - 设<G；*>是一个群，H是G的一个非空子集，若对任意的a，b∈H，有$a*b^{-1} \in H$，则<H；*>是<G；*>的子群。
        - 定理 5.19
            - 设<G；*>是一有限群，若<H；*>是<G；*>的子代数，则<H；*>是<G；*>的子群。
        - 定理 5.20
            - 设<G；*>是一有限群，若<H；*>是<G；*>的子代数，则<H；*>是<G；*>的子群。
        - 例 5.23
            - 若<G；*>是循环群，则其子群也是循环群。
    - **进一步可以将封闭性和可逆性合并成一个条件。**
- **三、陪集与正规子群**
    - **1．陪集与正规子群的概念**
        - 左陪集，右陪集，代表元。
            - 设<H；*>是<G；*>的子群，g∈G，令
                - g*H={g*h| h∈H}，简记为gH
                - H*g={h*g| h∈H}，简记为Hg
            - 称g*H和H*g分别为由g确定的子群<H；*>在群<G；*>中的左陪集和右陪集。称g为其代表元。

- 正规子群，陪集
  - 设<H；*>是群<G；*>的子群，如果对任意的g∈G，都有gH=Hg，则称<H；*>是群<G；*>的正规子群。此时的左陪集和右陪集简称为陪集。

- **2．正规子群的判别法**
  - 补充定义
    - 设<G；*>是群，H是G的非空子集，g∈G，定义
      - $g*H*g^{-1}=\{g*h*g^{-1}|h\in H\}$，简记为$gHg^{-1}$
    - 一般地，若A，B是G的非空子集，定义
      - $A*B=\{a*b|a\in A，b\in B\}$，简记为$AB$
  - （**判别法**）群<G；*>的子群<H；*>为正规子群的充分必要条件是对任意的g∈G，都有$gHg^{-1}=H$。
  - 群<G；*>的子群<H；*>为正规子群的充分必要条件是对任意的g∈G，都有gHg^{-1}⊆H。
  - 判断H是否是G的正规子群归结为：**对任意的g∈G及任意的h∈H，计算元素$g*h*g^{-1}$是否在H中。**

- **3．陪集分划**
  - 定理5.23
    - 设<H；*>是群<G；*>的子群，若g∈H，则有gH=Hg=H。
  - 定理5.24
    - 设<H；*>是群<G；*>的子群，a，b∈G，则有
      - （1）aH=bH或aH∩bH=Φ。
      - （2）Ha=Hb或Ha∩Hb=Φ。
  - 定理5.25
    - 设<H；*>是群<G；*>的子群，a，b∈G，则有
      - （1）aH=bH当且仅当b∈aH。
      - （2）Ha=Hb当且仅当b∈Ha。
  - 定理5.26
    - 设<H；*>是群<G；*>的子群，则
      - （1）<H；*>的所有相异的左陪集组成G的一个分划。
      - （2）<H；*>的所有相异的右陪集组成G的一个分划。
  - **注意：**
    - 定理中的分划称为群<G；*>中与<H；*>相关的左（右）陪集分划或左（右）陪集分解。
      - 可以看作是由G上某一等价关系R所导致的等价分划：
        - a R b ⇔ a和b在<H；*>的相同的左（右）陪集中
      - 当<H；*>是<G；*>的正规子群时，这种分划简单地称为<G；*>中与<H；*>相关的陪集分划或陪集分解。

- 定理给出了构造左（右）陪集分划的一个方法：
  - （1）H本身是一个，令G′= G–H；
  - （2）若G′= Φ，则结束，否则任取g∈G′，求得gH是一个；
  - （3）令G′= G′–gH，转（2）。
- 可类似地构造H的所有右陪集。

- **四、拉格朗日定理**
  - 定理5.27
    - 设<H；*>是群<G；*>的子群，g∈G，则#(gH) = #(Hg) = # H。即H的任意左（右）陪集与H 具有相同的基数。
  - 定理5.28
    - 设<H；*>是群<G；*>的子群，则的所有相异左陪集的个数和所有相异右陪集的个数相同。
  - 指数：
    - 群<G；*>中子群<H；*>的所有相异的左（右）陪集的个数称为<H；*>在<G；*>中的指数。
  - lagrange theorem（拉格朗日定理）：
    - 设<G；*>是一个有限群，且子群<H；*>在<G；*>中的指数为d，则# G = d·(# H)。
  - 推论：
    - 推论5.7
      - 素数阶群只有平凡子群。

        只有1和它本身
    - 推论5.8
      - 有限群<G；*> 中，任意元的周期必可整除群的阶。
    - 推论5.9
      - 素数阶群必为循环群，且每个非单位元的元都是生成元。
    - 注意：
      - 根据推论5.9，易写出任意素数阶群中二元运算的运算表。
        - 如：

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

        - Lagrange 定理只指出有限群 若有子群，则# H可整除# G，但不保证“若n能整除# G，就必有阶为n的子群”。
        - Lagrange 定理的逆定理对循环群成立。
    - 定理5.30

        - 设<G；*>是n阶循环群，若正整数d能整除n，则存在且仅存在一个阶为d的子群（也是循环群）。
    - 推论5.10
        - 若<G；*>是无限循环群，则<G；*>的子群除<{e}；*>外都是无限循环群，且有无穷多个。
- ***5.5 环和域**

以上内容整理于 幕布文档