第十章　群与环

- 主要内容
  - 群的定义与性质
  - 子群与群的陪集分解
  - 循环群与置换群

第十章：群与环

第一节：群的定义及性质

群简介

- 群在抽象代数中具有基本的重要地位
  - 群是一个特殊的代数系统
  - 是环、域和模的基础
  - 在几何学、代数拓扑学、函数论、泛函分析及其他许多数学分支起作用
  - 群论的重要性还体现在物理学和化学的研究中

群简介

- 群论是法国传奇式人物伽罗瓦提出
  - 用以解决了五次方程问题
  - 提出：把数学运算归类
- 例：全体整数的加法构成一个群

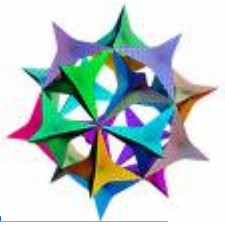
10.1 群的定义及性质

- 半群<G,*>： <G,*>是一个代数系统,*是G上的二元运算,如果*在G上成立结合律
  - $a*(b*c)=(a*b)*c$
- 例：下列代数系统是半群
  - R_+表示正实数集合,$<R_+,+>$,$<R_+,*>$是半群
  - $<M_n(R),+>$, $<M_n(R),\cdot>$是半群, $M_n(R)$是n阶矩阵的全体

10.1 群的定义及性质

- 独异点<G,*>： 有幺元的半群
- 例：下列代数系统是独异点
  - <N,+,0>,<N,*,1>均为独异点
  - <P(S), ∪,Ø>,<P(S), ∩,S>均为独异点
  - <P(S), ⊕, ∅>为独异点
  - <A^A, o>为独异点： o为函数复合
    - 单位元为恒等函数

10.1 群的定义及性质



- 群<G,*>： <G,*>为独异点， 并且
  - 每个元素都有逆元
- 例：
  - <Z,+>是群, 幺元是0, 逆元是相反数
  - $<M_n(R),\bullet>$， $\bullet$为矩阵乘法运算
    - 存在幺元是单位矩阵I_n
    - 不是群, 逆矩阵不一定存在
  - $<S_n(R),\bullet>$ 为群
    - $S_n(R)$=所有可逆矩阵的全体

10.1 群的定义及性质

- $<N_6,+_6>$为群,其中$N_6=\{0,1,2,3,4,5\}$
  - 幺元是0
  - $1+_65=0,2+_64=0,3+_63=0$
- $<P(A),\oplus>$为群
  - $\forall B\in P(A),B\oplus\varnothing=\varnothing\oplus B=B$
  - $B\oplus B=\varnothing$

10.1 群的定义及性质

- 例：四元群，设G={e,a,b,c}运算*表如下

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

- e为单位元
- G中运算是可交换的
- 每个元素都有逆元

回顾

- 半群<G,*>： <G,*>是一个代数系统,*是G上的二元运算,如果*在G上成立结合律
- 独异点<G,*>： 有幺元的半群
- 群<G,*>： <G,*>为独异点，并且每个元素都有逆元

10.1 群的定义及性质

- 群论中一些重要的概念
  - 有限群G：G为有限集
  - 无限群G：G为无限集
  - 群G的阶：G的基数
  - 平凡群：只含单位元的群
  - 交换群(阿贝尔群)：G中的二元运算是可交换的
- 例：
  - $<Z,+>$为无限群
  - $<Z_n,\oplus>$是有限群, 阶数为n
  - $<\{0\},+>$是平凡群

10.1 群的定义及性质

- 群中元素的幂：G为群，a∈G的n次幂
  - $a^0=e$
  - $a^n=a^{n-1}a$, $n>0$
  - $(a)^n=(a^{-1})^m$, $n<0$, $m=-n$
- 例：
  - $<Z_3,\oplus>$中求2^{-3}
    - $2^{-3}=(2^{-1})^3=1^3=1\oplus1\oplus1=0$

10.1 群的定义及性质

- 群的元素的阶(周期): G是群，$a \in G$
  - a的阶：最小的正整数k，$a^k=e$
  - 记作|a|=k: a为k阶元
  - k不存在，则a为无限元
- 例：
  - $<Z_6,\oplus>$中, 2和4是3阶元, 3是2阶元
  - 四元群中, e是1阶元, 其他元素是2阶元

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

10.1 群的定义及性质

- **定理：G是群，G中幂运算满足：**

1) $\forall a \in G, (a^{-1})^{-1} = a$

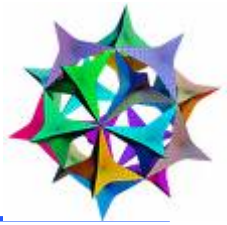
2) $\forall a, b \in G, (ab)^{-1} = b^{-1}a^{-1}$

3) $\forall a \in G, a^n a^m = a^{n+m}, n, m \in Z$

4) $\forall a \in G, (a^n)^m = a^{nm}, n, m \in Z$

5) 若G为交换群，则 $(ab)^n = a^n b^n$

10.1 群的定义及性质



2）证明：

$(a*b)*(b^{-1}*a^{-1})$

$=a*(b*b^{-1})*a^{-1}$

$=a*e*a^{-1}=e$

$(b^{-1}*a^{-1})*(a*b)$

$=b^{-1}*(a^{-1}*a)*b$

$=b^{-1}*b=e$

所以$(a*b)^{-1}=b^{-1}*a^{-1}$成立

10.1 群的定义及性质

- 定理：设<G,*>是群,则∀a,b,c∈G
  - ① 如a*b=a*c, 则b=c
  - ② 如b*a=c*a, 则b=c

证明：(1)群中的每一个元素都有逆元，因此只要两边同左乘a^{-1},即可得证。

(2)同理可证。

- 注：如果a*b=c*a,未必得到b=c，而只能知道$b=a^{-1}*c*a$，因为*不一定满足交换律

10.1 群的定义及性质

- 例：设G为群，$a,b\in G$，且 $(ab)^2=a^2b^2$

  证明：$ab=ba$

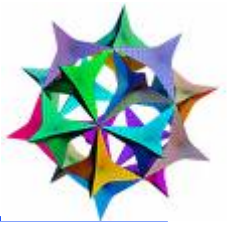
证：$(ab)^2=(ab)(ab)$

$=abab=a^2b^2=aabb$

因为群的运算满足消去律，所以有

$ab=ba$

10.1 群的定义及性质



- 定理：设G为群，a∈G，|a|=r。对整数k
  - ① $a^k=e$ 当且仅当 k是r的整数倍
  - ② $|a^{-1}|=|a|$

证：①充分性：由于k是r的整数倍，必存在整数m使得k=mr, 所以有$a^k= a^{mr}= (a^r)^m= e$。

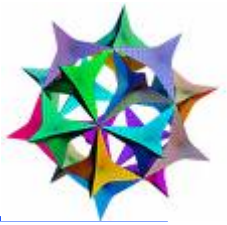
必要性：存在整数m和i，使得k=mr+i, 从而有

$e= a^{mr+i}= a^{mr}\ a^i= a^i$

因为a的阶是r，并且$0\le i\le r-1$

所以i＝0。则k是r的整数倍

10.1 群的定义及性质



- 定理：设G为群，$a \in G$，$|a|=r$。对整数k
  - ① $a^k=e$ 当且仅当 k是n的整数倍
  - ② $|a^{-1}| = |a|$

证：②由于$(a^{-1})^r = (a^r)^{-1} = e^{-1} = e$。可知$a^{-1}$的阶是存在的。

令$|a^{-1}| = t$，根据前面证明有r是t的整数倍。

而a又是a^{-1}的逆元，所以a的阶也是a^{-1}的阶的因子，故有t是r的整数倍。

从而证明了r=t，即$|a^{-1}| = |a|$

10.1 群的定义及性质

- 例：设G为有限群，则G中阶大于2的元素有偶数个

证：由前面定理，对任意$a \in G$

$a^2=e \Leftrightarrow a^{-1}a^2=a^{-1}e \Leftrightarrow a=a^{-1}$

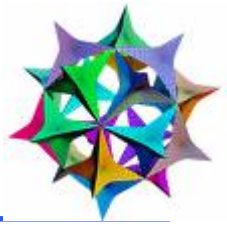
故G中阶大于2的元素a, 必有

$$a \neq a^{-1}$$

由于$|a|=|a^{-1}|$，故G中阶大于2的元素成对出现

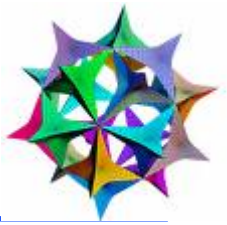
第二节：子群与群的陪集分解

10.2 子群与群的陪集分解



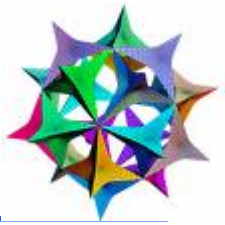
- 子群：设<G,*>是群,H是G的(非空)子集,如果H关于G的运算*构成群,则称H为G的子群，记作H≤G
  - 如果H是G的真子集，则称H是G的真子群，记作H＜G
- 子群说明：<H,*>是子群, 则
  - H对于运算*是封闭的
  - G的幺元e在H内
  - H的每个元素的逆元仍在H内(对逆运算封闭)。至于运算的结合律,由于在G中成立,对于H必然成立
  - 如H构成子群,必然是非空的,至少有幺元e

10.2 子群与群的陪集分解



- 例：
  - $\langle R,+\rangle$是群，$Q\subseteq R$，$\langle Q,+\rangle$是子群。
    - $\langle N,+\rangle$？
  - $\langle N_6,+_6\rangle$是群。$H_1=\{0,2,4\}$，则$\langle H_1,+_6\rangle$是不是子群？
    - $2+_6 2=4\in H_1, 4+_6 4=2\in H_1$
    - 2,4互为逆元
  - $H_2=\{0,1,5\}$，$\langle H_2,+_6\rangle$是不是子群？
    - $1+_6 1=2\notin H_2, 5+_6 5=4\notin H_2$
    - H_2对运算$+_6$不封闭

10.2 子群与群的陪集分解



- 子群的判定定理一：设<G,*>是群，H⊆G,<H,*>是子群的充要条件是以下三条同时成立
  - ① H非空
  - ② 如果a∈H,b∈H,则a*b∈H
  - ③ 若a∈H,则a^{-1}∈H

证明：必要性是显然成立,下证充分性。

由(1)因H非空,取a∈H,由(3)a^{-1}∈H,由(2)因a,a^{-1}∈H则a*a^{-1}∈H,∴e∈H, 从而<H,*>是子群

10.2 子群与群的陪集分解

- 子群的判定定理二：设<G,*>是群，H⊆G,<H,*>是子群的充要条件是以下两条同时成立
  - ① H非空
  - ② ∀a,b∈H, 均有$a*b^{-1}\in H$

证明：必要性：任取a,b∈H.由于H是G的子群，必有$b^{-1}\in H$，从而$a*b^{-1}\in H$。

充分性：因为H非空，必存在x∈H，根据给定条件得$x*x^{-1}\in H$，即e∈H。设a是H的任一元素，即a∈H,由e,a∈H得$e*a^{-1}\in H$,即$a^{-1}\in H$。任取a,b∈H,由刚才的证明知$b^{-1}\in H$。根据给定条件知$a*(b^{-1})^{-1}\in H$,即a*b∈H根据上一定理可知<H,*>是<G,*>的子群

10.2 子群与群的陪集分解

- 子群的判定定理三： $<G,*>$是群,$H \subseteq G$,如果H是有穷集，$<H,*>$是子群的充要条件是：
  - ① H非空
  - ② $\forall a,b \in H$, 均有$a*b \in H$

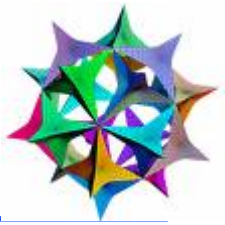
证明：设a是H的任一元素，即$a \in H$，由判定定理一，只需证明$a^{-1} \in H$即可。

若$a=e$，则$a^{-1}= e^{-1} = e \in H$

若$a \neq e$，令$S=\{a,a^2,...\}$，则$S \subseteq H$。由于H是有穷集，必有$a^i= a^j$ $(i<j)$。根据G中的消去律得$a^{j-i}= e$，由$a \neq e$可知$j-i>1$，由此得 $a^{j-i-1} *a =e$和$a*a^{j-i-1} =e$

从而证明了$a^{-1}=a^{j-i-1} \in H$

10.2 子群与群的陪集分解



- 例：设G为群，$a \in G$，令$H=\{a^k \mid k \in Z\}$

即a的所有的幂构成的集合，证明：H是G是子群，称为由a生成的子群，记作<a>

证明：首先由$a \in <a>$知道<a>不为空，任取

$a^m, a^l \in <a>$ ，

则$a^m(a^l)^{-1} = a^m a^{-l} = a^{m-l} \in <a>$

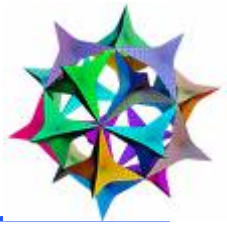
根据判断定理二可知。

例如：整数加群，由2生成的子群是

$<2>=\{2k \mid k \in Z\}=2Z$

群$<Z_6, \oplus>$中，由2生成的子群是？

10.2 子群与群的陪集分解



- 例：设**G**为群，令**C**是与**G**中所有的元素都可交换的元素构成的集合，即

$$C=\left\{a\middle|a\in G\wedge\forall x\in G\left(ax=xa\right)\right\}$$

证明：**C**是**G**的子群，称为**G**的中心

10.2 子群与群的陪集分解

❑ 子群格

若G为群，令$S=\{H|H$是G的子群$\}$是G的所有子群的集合，在S上定义关系R如下：

$$\forall A,B\in S, ARB \Leftrightarrow A\text{是}B\text{的子群}$$

那么<S, R>构成偏序集，称为群G的子群格

10.2 子群与群的陪集分解

- 用图表示子群格

（1）

*	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） $<Z_{12}, \oplus>$

第十章 习题课

- 主要内容
  - 半群、独异点与群的定义
  - 群的基本性质
  - 子群的判别定理

基本要求

- 判断或证明给定集合和运算是否构成半群、独异点和群
- 熟悉群的基本性质
- 能够证明G的子集构成G的子群

练习1

1. 判断下列集合和运算是否构成半群、独异点和群.

(1) a 是正整数，$G = \{a^n \mid n \in \mathbf{Z}\}$, 运算是普通乘法.

(2) $\mathbf{Q}^+$是正有理数集，运算为普通加法.

(3) 一元实系数多项式的集合关于多项式加法.

解

(1) 是半群、独异点和群

(2) 是半群但不是独异点和群

(3) 是半群、独异点和群

方法：根据定义验证，注意运算的封闭性

练习2

2. 设V_1= <Z, +>, V_2 = <Z, ·>,其中Z为整数集合, + 和· 分别代表普通加法和乘法. 判断下述集合S是否构成V_1和V_2的子半群和子独异点.

(1) S= {$2k$ | k∈Z}

(2) S= {$2k$+1 | k∈Z}

(3) S= {–1, 0, 1}

解

(1) S关于V_1构成子半群和子独异点，但是关于V_2仅构成子半群

(2) S关于V_1不构成子半群也不构成子独异点，S关于V_2构成子半群和子独异点

(3) S关于V_1不构成子半群和子独异点，关于V_2构成子半群和子独异点

练习3

3. 设Z_{18}为模18整数加群, 求所有元素的阶.

解:

|0| = 1, |9| = 2, |6| = |12| = 3, |3| = |15| = 6,
|2| = |4| = |8| = |10| = |14| = |16| = 9,
|1| = |5| = |7| = |11| = |13| = |17| =18,

说明:

群中元素的阶可能存在，也可能不存在.

对于有限群，每个元素的阶都存在，而且是群的阶的因子.

对于无限群，单位元的阶存在，是1；而其它元素的阶可能存在，也可能不存在.（可能所有元素的阶都存在，但是群还是无限群）.

练习4

4．证明偶数阶群必含2阶元.

由 $x^2 = e \Leftrightarrow |x| = 1$ 或2.

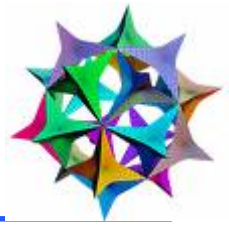
换句话说, 对于G中元素x，如果 $|x| > 2$, 必有$x^{-1} \neq x$.

由于 $|x| = |x^{-1}|$，阶大于2的元素成对出现，共有偶数个.

那么剩下的 1 阶和 2 阶元总共应该是偶数个.

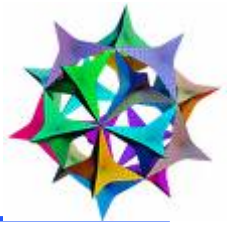
1 阶元只有 1 个，就是单位元，从而证明了G中必有 2 阶元.

作业



- 2
- 3
- 4
- 10
- 22
- 23

回顾



- 半群<G,*>： <G,*>是一个代数系统,*是G上的二元运算,如果*在G上成立结合律
- 独异点<G,*>： 有幺元的半群
- 群<G,*>： <G,*>为独异点，并且每个元素都有逆元
- 元素的阶(周期): G是群，$a \in G$，使得$a^k=e$的最小正整数k

10.2 子群与群的陪集分解

- **陪集：** **<H,*>是<G,*>的子群，a∈G，集合{a}H（或H{a}），称为由a所确定的H在G中的左陪集（右陪集）**
  - 记作aH（或Ha）
  - 元素a称为陪集aH（或Ha）的代表元素

10.2 子群与群的陪集分解

- 例：设G＝{e,a,b,c}是四元群，H＝{e,a}是G的子群，那么H的所有右陪集是：

  He={e,a}=H

  Ha={a,e}=H

  Hb={b,c}

  Hc={c,b}

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

不同的右陪集只有两个，即H和{b,c}

10.2 子群与群的陪集分解

- 定理：设**H**是群**G**的子群，则
  - ① **He=H**
  - ② ∀**a**∈**G**有**a**∈**Ha**

10.2 子群与群的陪集分解

- 定理：设<H,*>是群<G,*>的子群，则

  $a\in Hb$当且仅当$ab^{-1}\in H$当且仅当$Ha=Hb$

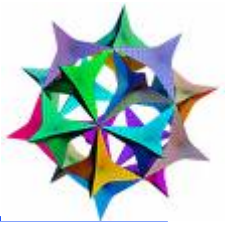
证明：(1) $a\in Hb$当且仅当$ab^{-1}\in H$

$a\in Hb$

$\Leftrightarrow \exists h\in H$，使$a=hb$，即$ab^{-1}=h$

$\Leftrightarrow ab^{-1}\in H$

10.2 子群与群的陪集分解



- 定理：设<H,*>是群<G,*>的子群，则

  $a\in Hb$当且仅当$ab^{-1}\in H$当且仅当$Ha=Hb$

证明：(2) $a\in Hb$当且仅当$Ha=Hb$

充分性: 若$Ha=Hb$，$a\in Ha \Rightarrow a\in Hb$

必要性: $a\in Hb \Rightarrow h\in H$使得$a=hb$，即$h^{-1}a=b$

任取$h_1a\in Ha$，则有$h_1a=h_1(hb)=(h_1h)b\in Hb$

从而得到$Ha\subseteq Hb$

任取$h_1b\in Hb$，则有

$h_1b=h_1(h^{-1}a)=(h_1h^{-1})a\in Ha$

从而得到$Hb\subseteq Ha$

10.2 子群与群的陪集分解

- 定理：设H是群G的子群，在G上定义二元关系～：$\forall a,b\in G,\ a\sim b\Leftrightarrow ab^{-1}\in H$

  ～是G上的等价关系，且$[a]_{\sim}=Ha$

证明：(1)～是G上等价关系

自反性：任取$a\in G$，由$aa^{-1}=e\in H\Leftrightarrow a\sim a$

对称性：任取$a,b\in G$，则$a\sim b\Rightarrow ab^{-1}\in H$

$\Rightarrow (ab^{-1})^{-1}\in H\Rightarrow ba^{-1}\in H\Rightarrow b\sim a$

传递性：任取$a,b,c\in G$，则$a\sim b$且$b\sim c\Rightarrow ab^{-1}\in H$且

$bc^{-1}\in H\Rightarrow (ab^{-1})(bc^{-1})\in H\Rightarrow ac^{-1}\in H$

$\Rightarrow a\sim c$

10.2 子群与群的陪集分解

- 定理：设H是群G的子群，在G上定义二元关系～：$\forall a,b\in G,\ a\sim b\Leftrightarrow ab^{-1}\in H$

  ～是G上的等价关系，且$[a]_{\sim}=Ha$

证明：(2) $[a]_{\sim}=Ha$

任取$b\in G$，则有$b\in[a]_{\sim}\Leftrightarrow a\sim b\Leftrightarrow ab^{-1}\in H$

根据前面定理有

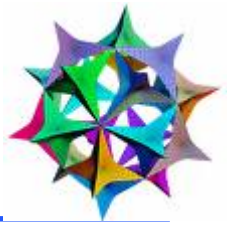
$ab^{-1}\in H\Leftrightarrow Ha=Hb\Leftrightarrow a\in Hb\Leftrightarrow b\in Ha$

故$b\in[a]_{\sim}\Leftrightarrow b\in Ha$，所以$[a]_{\sim}=Ha$

10.2 子群与群的陪集分解

- 推论：设**H**是群**G**的子群
  - **Ha**和**Hb**是任意二个右陪集，有**Ha=Hb**或**Ha∩Hb=Ø**
  - **∪{Ha| a∈G}=G**
- 定理：设**H**是群**G**的子群，则**∀a∈G**，**H≈Ha**

10.2 子群与群的陪集分解

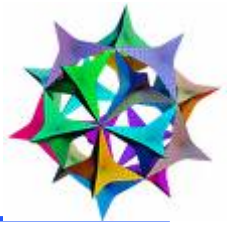


- 性质总结
  - 右陪集的个数和左陪集的个数是相等的
  - 子群的左（右）陪集的基数=子群的阶数
  - 子群的左（右）陪集要么相等，要么相交为空
  - 子群的左（右）陪集集合形成**G**的一个划分

10.2 子群与群的陪集分解

- 正规子群(不变子群)：设<H,*>是群<G,*>的子群，对任意元素a∈G，如果aH=Ha，则称<H,*>为正规子群
  - 任何群都有正规子群
    - G和{e}
  - 阿贝尔群的所有子群都是正规子群

10.2 子群与群的陪集分解



- 陪集数：给定群G及其子群H, 令 $S=\{Ha|a\in G\}$ 和 $T=\{aH|a\in G\}$
  - 定义函数f: $S\to T$
    - $f(Ha)=a^{-1}H, \forall a\in G$
  - f是双射
  - 结论：$|S|=|T|$
  - $[G:H]=|S|$：H在G中的指数

10.2 子群与群的陪集分解

- **拉格朗日定理：** 设G是有限群，H是G的子群

$$|G|=|H|\cdot[G:H]$$

证明：设$[G:H]=r$，$a_1,\ldots,a_r$为H的r个右陪集的代表元，由前面的定理则有

$$G=Ha_1 \cup \ldots \cup Ha_r$$

由前面定理，有$Ha_i \setminus Ha_j=\varnothing,\ i\neq j$

故$|G|=|Ha_1|+\ldots+|Ha_r|$

由于$|Ha_i|=|H|$，则易得$|G|=|H|\cdot r$

故 $|G|=|H|\cdot[G:H]$

10.2 子群与群的陪集分解

- 推论：设G是n阶群，则∀a∈G，|a|是n的因子，且$a^n=e$

证明：∀a∈G, <a>是G的由a生成的子群。由拉格朗日定理，<a>的阶是n的因子。

设|a|=r，则

$<a>=\{e,a,a^2,\ldots,a^{r-1}\}$

故|<a>|=|a|，所以|a|是n的因子

由前面定理知：$a^n=e$

第三节：循环群与置换群

10.3 循环群与置换群

- 循环群：存在$a \in G$，$G=\langle a \rangle$
  - a为G的生成元
- 循环群分类：
  - n阶循环群：a是n阶元
    - $G=\{e,a,a^2,\ldots,a^{n-1}\}$
  - 无限循环群：a是无限元
    - $G=\{e,a,a^{-1},a^2,a^{-2}\ldots,a^{n-1},a^{-(n-1)},\ldots\}$

10.3 循环群与置换群

- 例：$<N_4, +_4>$是循环群，运算表为：

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

幺元为0，1或3是生成元

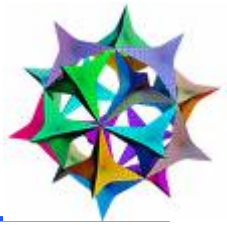
$1^4 = 1 +_4 1 +_4 1 +_4 1 = 0$,周期为4

$1^3 = 1 +_4 1 +_4 1 = 3$

$1^2 = 1 +_4 1 = 2$

$1^1 = 1$

10.3 循环群与置换群



- 定理：循环群必然是交换群
- 反之成立吗？
- 例：四阶群不是循环群, 但是它是交换群

$*$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

10.3 循环群与置换群

- **定理：** 设$G=\langle a\rangle$是循环群，则
  1. 若G是无限循环群，则G只有两个生成元，即a和a^{-1}
  2. 若G是n阶循环群，则G含有h(n)(欧拉函数)个生成元，对于任意小于等于n且与n互素的正整数r，a^r是G的生成元

10.3 循环群与置换群

- **定理：** 设$G=\langle a\rangle$是循环群，则

  ① 若G是无限循环群，则G只有两个生成元，即a和a^{-1}

证明： 显然$\langle a^{-1}\rangle \subseteq G$。为证明$G \subseteq \langle a^{-1}\rangle$，只需证明对任意$a^k \in G$，$a^k$都可以表示成$a^{-1}$的幂。由元素幂的性质有 $a^k=(a^{-1})^{-k}$

从而得到$G=\langle a^{-1}\rangle$，a^{-1}是G的生成元

10.3 循环群与置换群

- 定理：设$G=<a>$是循环群，则
  - ① 若G是无限循环群，则G只有两个生成元，即a和a^{-1}

证明(继续)：再证明G只有a和a^{-1}这两个生成元。假设b也是G的生成元，则$G=<b>$，由$a\in G$可知存在整数t使得$a=b^t$。又由$b\in G=<a>$知存在整数m使得$b=a^m$。

从而得到$a=b^t=(a^m)^t=a^{mt}$

由G中消去律得$a^{mt-1}=e$，因为G是无限群，必有$mt-1=0$。从而证明了$m=t=1$或$m=t=-1$，即$b=a$或$b=a^{-1}$

10.3 循环群与置换群

- 定理：设$G=<a>$是循环群，则

  ②若G是n阶循环群，则G含有h(n)(欧拉函数)个生成元，对于任意小于等于n且与n互素的正整数r，a^r是G的生成元

证明：对$r<n(n>1)$, a^r是G的生成元⇔n与r互素

充分性：设r与n互素，且$r\le n$，那么存在整数u和v使得

$$ur+vn=1$$

因此由元素幂的性质和拉格朗日定理的推论有

$$a= a^{ur+vn}=(a^r)^u(a^n)^v= (a^r)^u$$

所以对任意$a^k\in G$，$a^k=(a^r)^{uk}\in<a^r>$,即$G \subseteq <a^r>$

另一方面，显然有$<a^r> \subseteq G$ 。所以a^r是G的生成元

10.3 循环群与置换群

- 定理：设G＝<a>是循环群，则

  ②若G是n阶循环群，则G含有h(n)(欧拉函数)个生成元，对于任意小于等于n且与n互素的正整数r，a^r是G的生成元

证明：

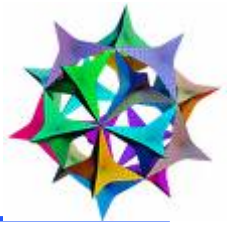
必要性: a^r是G的生成元 ⇒ n与r互素

a^r是G的生成元，则$|a^r|=n$。令r与n的最大公约数为d则存在正整数t使得r＝dt。因此有

$$(a^r)^{n/d}=(a^{dt})^{n/d}=(a^n)^t=e$$

根据n阶群的性质知$|a^r|$是n/d的因子，即n整除n/d。从而证明了d＝1

10.3 循环群与置换群



- 例：$G=<Z_9,\oplus>$
  - 小于或者等于9且与9互素的数：1，2，4，5，7，8
  - G的生成元是1，2，4，5，7，8
- 例：$G=3Z=\{3z|z\in Z\}$，G是无限循环群

  生成元为：3，-3

10.3 循环群与置换群

- **定理：** 下列性质成立
  - ① 设$G=\langle a\rangle$是循环群，则G的子群也是循环群
  - ② 若$G=\langle a\rangle$是无限循环群，则G的子群除{e}以外都是无限循环群
  - ③ 若$G=\langle a\rangle$是n阶循环群，则对n的每个正因子d，G恰好含有一个d阶子群($\langle a^{n/d}\rangle$)

10.3 循环群与置换群

- **置换**：设S={1,2,...,n}，S上的双射σ为S上的n元置换

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

- 例：S={1,2,3,4,5}

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}$$

10.3 循环群与置换群

- **置换乘积：** 设S={1,2,...,n}， σ和τ是S上n元置换， σ和τ的复合σοτ也是置换，称为σ和τ的乘积
- 例：S={1,2,3,4,5}

$$\sigma=\begin{pmatrix}1&2&3&4&5\\2&3&4&1&5\end{pmatrix}\qquad \tau=\begin{pmatrix}1&2&3&4&5\\3&2&1&4&5\end{pmatrix}$$

$$\sigma\circ\tau=\begin{pmatrix}1&2&3&4&5\\2&1&4&3&5\end{pmatrix}$$

10.3 循环群与置换群

- **n元对称群：** $<S_n, \circ>$, S_n为所有的n元置换
  - 任何$\sigma, \tau \in S_n$, $\sigma\circ\tau \in S_n$
  - 恒等置换为单位元
  - 任何$\sigma \in S_n$, $\sigma^{-1} \in S_n$
- **n元置换群：** S_n的子群

10.3 循环群与置换群

- **k阶轮换σ**：σ是S={1,2,…,n}S上n元置换
  - $\sigma(i_1)=i_2,\ \sigma(i_2)=i_3,\ldots,\ \sigma(i_{k-1})=i_k,\ \sigma(i_k)=i_1$
  - $\sigma(i_j)=i_j$，其他i_j
  - 对换：2阶轮换
- **轮换分解**：σ是S={1,2,…,n}S上n元置换

  第一步：找到一个有限序列$i_1,\ldots,i_k$，$k\geq 1$，使得

  $\sigma(i_1)=i_2,\ \sigma(i_2)=i_3,\ldots,\ \sigma(i_{k-1})=i_k,\ \sigma(i_k)=i_1$

  令$\sigma_1=(i_1\ i_2\ \ldots i_k)$，σ′作用于$S-\{i_1,\ldots,i_k\}$，

  则$\sigma=\sigma_1\circ\sigma'$

  第二步：继续分解σ′，可以得到

  $\sigma=\sigma_1\circ\sigma_2\ \ldots\ \circ\sigma_t$

10.3 循环群与置换群

- 例：设S={1,2,…,8}，

$$\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8\\5&3&6&4&2&1&8&7\end{pmatrix}$$

- $\sigma=(1\ 5\ 2\ 3\ 6)(4)(7\ 8)$

10.3 循环群与置换群

- **k阶轮换→对换：** σ是S={1,2,...,n}S上n元置换

  $(i_1\ i_2 \ldots i_k)=(i_1\ i_2)(i_1\ i_3)\ldots(i_1,i_k)$

- 例：设S={1,2,...,8}，

$$\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8\\5&3&6&4&2&1&8&7\end{pmatrix}$$

- σ=(1 5 2 3 6)(4)(7 8)

  =(1 5)(1 2)(1 3)(1 6)(4)(7 8)

第十章 习题课

- 主要内容
  - 半群、独异点与群的定义
  - 群的基本性质
  - 子群的判别定理
  - 陪集的定义及其性质
  - 拉格朗日定理及其应用
  - 循环群的生成元和子群
  - 置换群

基本要求

- 判断或证明给定集合和运算是否构成半群、独异点和群
- 熟悉群的基本性质
- 能够证明G的子集构成G的子群
- 熟悉陪集的定义和性质
- 熟悉拉格朗日定理及其推论，学习简单应用
- 会求循环群的生成元及其子群
- 熟悉n元置换的表示方法、乘法以及n元置换群

练习1

1. 判断下列集合和运算是否构成半群、独异点和群.

(1) a 是正整数，$G = \{a^n \mid n \in \mathbf{Z}\}$, 运算是普通乘法.

(2) $\mathbf{Q}^+$是正有理数集，运算为普通加法.

(3) 一元实系数多项式的集合关于多项式加法.

解

(1) 是半群、独异点和群

(2) 是半群但不是独异点和群

(3) 是半群、独异点和群

方法：根据定义验证，注意运算的封闭性

练习2

2. 设V_1= <Z, +>, V_2 = <Z, ·>,其中Z为整数集合, + 和· 分别代表普通加法和乘法. 判断下述集合S是否构成V_1和V_2的子半群和子独异点.

(1) S= {$2k$ | k∈Z}

(2) S= {$2k$+1 | k∈Z}

(3) S= {–1, 0, 1}

解

(1) S关于V_1构成子半群和子独异点，但是关于V_2仅构成子半群

(2) S关于V_1不构成子半群也不构成子独异点，S关于V_2构成子半群和子独异点

(3) S关于V_1不构成子半群和子独异点，关于V_2构成子半群和子独异点

练习3

3. 设Z_{18}为模18整数加群, 求所有元素的阶.

解:

$|0| = 1,\quad |9| = 2,\quad |6| = |12| = 3,\quad |3| = |15| = 6,$

$|2| = |4| = |8| = |10| = |14| = |16| = 9,$

$|1| = |5| = |7| = |11| = |13| = |17| = 18,$

说明:

群中元素的阶可能存在，也可能不存在.

对于有限群，每个元素的阶都存在，而且是群的阶的因子.

对于无限群，单位元的阶存在，是1；而其它元素的阶可能存在，也可能不存在.（可能所有元素的阶都存在，但是群还是无限群）.

练习4

4．证明偶数阶群必含2阶元.

由 $x^2 = e \Leftrightarrow |x| = 1$ 或2.

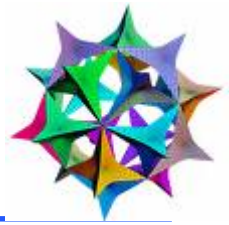
换句话说, 对于G中元素x，如果 $|x| > 2$, 必有$x^{-1} \neq x$.

由于 $|x| = |x^{-1}|$，阶大于2的元素成对出现，共有偶数个.

那么剩下的 1 阶和 2 阶元总共应该是偶数个.

1 阶元只有 1 个，就是单位元，从而证明了G中必有 2 阶元.

有关群性质的证明方法



- 有关群的简单证明题的主要类型
  - 证明群中的元素某些运算结果相等
  - 证明群中的子集相等
  - 证明与元素的阶相关的命题.
  - 证明群的其它性质，如交换性等.
- 常用的证明手段或工具是
  - 算律：结合律、消去律
  - 和特殊元素相关的等式，如单位元、逆元等
  - 幂运算规则
  - 和元素的阶相关的性质. 特别地，a为1阶或2阶元的充分必要条件是$a^{-1}= a$.

证明方法

- 证明群中元素相等的基本方法就是用结合律、消去律、单位元及逆元的惟一性、群的幂运算规则等对等式进行变形和化简.
- 证明子集相等的基本方法就是证明两个子集相互包含
- 证明与元素的阶相关的命题，如证明阶相等，阶整除等. 证明两个元素的阶r 和 s 相等或证明某个元素的阶等于r，基本方法是证明相互整除. 在证明中可以使用结合律、消去律、幂运算规则以及关于元素的阶的性质. 特别地，可能用到a为1阶或2阶元的充分必要条件是$a^{-1} = a$.

练习5

5．设G为群，a是G中的2 阶元，证明G中与a可交换的元素构成G的子群.

证　令$H=\{x \mid x\in G \wedge xa=ax\}$, 下面证明$H$是$G$的子群.
首先e属于H，H是G的非空子集.
任取$x, y \in H$，有

$$(xy^{-1})\,a = x(y^{-1}a) = x(a^{-1}y)^{-1} = x(ay)^{-1}$$
$$= x(ya)^{-1} = xa^{-1}y^{-1} = xay^{-1} = axy^{-1} = a(xy^{-1})$$

因此 xy^{-1}属于H. 由判定定理命题得证.

分析：
证明子群可以用判定定理，特别是判定定理二.
证明的步骤是：
验证 H 非空
任取 $x, y\in H$，证明$xy^{-1}\in H$

练习6

6. (1) 设G为模12加群, 求<3> 在G中所有的左陪集

(2) 设 $X=\{x \mid x\in \mathbf{R}, x\neq 0,1\}$, 在$X$上如下定义6个函数:

$$f_1(x)=x,\quad f_2(x)=1/x,\quad f_3(x)=1-x,$$

$$f_4(x)=1/(1-x),\ f_5(x)=(x-1)/x,\ f_6(x)=x/(x-1),$$

则$G=\{f_1,f_2,f_3,f_4,f_5,f_6\}$关于函数合成运算构成群. 求子群$H=\{f_1,f_2\}$ 的所有的右陪集.

解 (1) <3> = {0, 3, 6, 9}, <3>的不同左陪集有3个，即

$0+\langle 3\rangle=\langle 3\rangle$,

$1+\langle 3\rangle=4+\langle 3\rangle=7+\langle 3\rangle=10+\langle 3\rangle=\{1,4,7,10\}$,

$2+\langle 3\rangle=5+\langle 3\rangle=8+\langle 3\rangle=11+\langle 3\rangle=\{2,5,8,11\}$.

(2) $\{f_1,f_2\}$有3个不同的陪集，它们是：

$$H,\ Hf_3=\{f_3,f_5\},\ Hf_4=\{f_4,f_6\}.$$

练习7

7．设 H_1,H_2分别是群G 的 r, s 阶子群，若$(r,s) = 1$，证明 $H_1\cap H_2 = \{e\}$.

证 $H_1\cap H_2\leq H_1$，$H_1\cap H_2 \leq H_2$. 由Lagrange定理，$|H_1\cap H_2|$ 整除r，也整除s. 从而 $|H_1\cap H_2|$ 整除 r与s 的最大公因子. 因为$(r,s) = 1$, 从而 $|H_1\cap H_2 | = 1$. 即 $H_1\cap H_2 = \{e\}$.

某些有用的数量结果：设a是群G元素，C为G的中心

$$N(a)=\{ x \mid x\in G, xa=ax \},$$

$|C|$ 是 $|N(a)|$ 和 $|G|$ 的因子，$|a|$ 是 $|N(a)|$ 和 $|G|$ 的因子

$|H| = | xHx^{-1}|$

$|a^n|$ 是 $|a|$ 的因子

$a^2=e \Leftrightarrow a=a^{-1}\Leftrightarrow |a|=1,2$

练习8

8．设 i 为虚数单位，即 $i^2=-1$, 令

$$G=\left\{\pm\begin{pmatrix}1&0\\0&1\end{pmatrix},\ \pm\begin{pmatrix}i&0\\0&-i\end{pmatrix},\ \pm\begin{pmatrix}0&1\\-1&0\end{pmatrix},\ \pm\begin{pmatrix}0&i\\i&0\end{pmatrix}\right\}$$

则G关于矩阵乘法构成群. 找出G的所有子群.

解 令A, B, C, D分别为

$$\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}i&0\\0&-i\end{pmatrix},\begin{pmatrix}0&1\\-1&0\end{pmatrix},\begin{pmatrix}0&i\\i&0\end{pmatrix}$$

G的子群有6个，即

平凡子群：$\langle A\rangle=\{A\}, G$

2 阶子群：$\langle -A\rangle=\{A, -A\}$,

4 阶子群：$\langle B\rangle=\{A,B,-A,-B\}$,

$\langle C\rangle=\{A,C,-A,-C\}$,

$\langle D\rangle=\{A,D,-A,-D\}$,

	A	$-A$	B	$-B$	C	$-C$	D	$-D$
A	A	$-A$	B	$-B$	C	$-C$	D	$-D$
$-A$	$-A$	A	$-B$	B	$-C$	C	$-D$	D
B	B	$-B$	$-A$	A	D	$-D$	$-C$	C
$-B$	$-B$	B	A	$-A$	$-D$	D	C	$-C$
C	C	$-C$	$-D$	D	$-A$	A	B	$-B$
$-C$	$-C$	C	D	$-D$	A	$-A$	$-B$	B
D	D	$-D$	C	$-C$	$-B$	B	$-A$	A
$-D$	$-D$	D	$-C$	C	B	$-B$	A	$-A$

练习9

9．设群G的运算表如表所示，问G是否为循环群？如果是，求出它所有的生成元和子群.

	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	c	d	e	f	a
c	c	d	e	f	a	b
d	d	e	f	a	b	c
e	e	f	a	b	c	d
f	f	a	b	c	d	e

解

易见 a 为单位元.

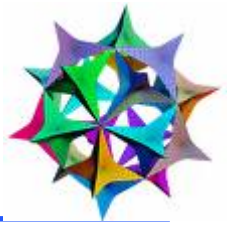
由于$|G|=6$, $|b|=6$, 所以 b 为生成元. $G=\langle b\rangle$为循环群. $|f|=6$, 因而 f 也是生成元

$|c|=3$, $|d|=2$, $|e|=3$, 因此 c,d, e不是生成元.

子群：$\langle a\rangle=\{a\}$, $\langle c\rangle=\{c, e, a\}$,

$\langle d\rangle=\{d, a\}$, G .

练习10



10. 证明Fermat小定理：设 p为素数，则 $p|(n^p-n)$

证：考虑一个圆环上等距离穿有 p个珠子，用 n 种颜色对珠子着色. 考虑围绕中心旋转，则群是

$G=\{\sigma_1, \sigma_2, \dots, \sigma_p\}$

$\sigma_1=(\bullet)(\bullet)\dots(\bullet)$

$\sigma_2=(\bullet\ \bullet\ \dots\ \bullet)$

…

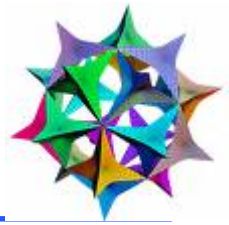
$\sigma_p=(\bullet\ \bullet\ \dots\ \bullet)$

根据Polya定理，不同的着色方案数是

$$M=\frac{1}{p}[n^p+(p-1)n^1]=\frac{1}{p}(n^p-n+pn)$$

于是 $p|(n^p-n)$

作业



- 2
- 4
- 18
- 22
- 24
- 28
- 29

回顾

- 子群：H是G的(非空)子集,且H关于G的运算*构成群
- 子群的判定定理一：设<G,*>是群，H⊆G,<H,*>是子群的充要条件是以下三条同时成立：
  ① H非空
  ② 如果a∈H,b∈H,则a*b∈H
  ③ 若a∈H,则a^{-1}∈H
- 子群的判定定理二：设<G,*>是群，H⊆G, <H,*>是子群的充要条件是以下两条同时成立：
  ① H非空
  ② ∀a,b∈H, 均有$a*b^{-1}$∈H

回顾

- 子群的判定定理三： <G,*>是群,H⊆G,如果H是有穷集，<H,*>是子群的充要条件是：
  ① H非空
  ② ∀a,b∈H, 均有a*b∈H