6.2变换群

复习: 集合S上的变换是双射函数f: $S \to S$

假设S上的所有变换的集合为S', 则变换的二元运算(复合运算)"$\circ$"构成了一个代数系统$< S', \circ >$, 此代数系统为群

原因:

(1) 复合运算可结合;

(2) "$\circ$"存在单位元, 即恒等变换 $f(x)=x$, $x \in S$

(3) $<S', \circ>$中的每个变换必存在逆元素, 即逆变换

所以, $<S', \circ>$是群, 若$S'' \subset S'$, $<S'', \circ >$也可以构成群

定义6.11 集合S上的若干个变换与复合运算若构成一个群, 称为**变换群**.

变换群的性质

定理6.10 任一群均与一个变换群同构.

证 设<G, $*$>是一个群, 从G中取一元素a, 则存在一个变换

$$f_a: x \to x*a\ ,\ x \in G$$

这样, G中每个元素均有一个变换与之对应, 这些变换$f_a, f_b, f_c, \cdots$构成一个变换的集合G'.

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

变换群的性质

存在一个双射函数$g: G \to G'$使得: $g(a*b) = g(a) \circ g(b)$

(1) 令函数g为: $g(a) = f_a$, 因此G'中每个元素 f_a,均有G中元素a与之对应, 故g为满射. 如果$a \neq b$, 则由消去律可知

$$x*a \neq x*b \ , x \in G$$

故有$f_a \neq f_b$, 因此 $g: G \to G'$是一个双射函数.

(2) 由于$g(a*b) = f_{a*b}$ $\quad$ $g(a) \circ g(b) = f_a \circ f_b$

而 $\quad$ $f_{a*b}(x) = x*a*b = (x*a)*b = f_b(f_a(x)) = f_a \circ f_b(x)$

所以有$g(a*b) = g(a) \circ g(b)$ 因此, $\langle G, * \rangle$与$\langle G', \circ \rangle$同构. 由定理6.9可知$\langle G', \circ \rangle$也是一个群,且它是一个变换群.

Note: 对群的研究可以归结为对变换群的研究;
任一抽象群均可在变换群中找到它的一个实例.

6.3 对称群与置换群

定义6.12 设 $S=\{1, 2, \ldots, n\}$, S上的任何双射函数$\sigma: S \to S$ 称为S上的n元置换.

例如 $S=\{1, 2, 3, 4, 5\}$, 下述为5元置换

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

定义6.13 设σ, τ是n元置换, σ和τ的复合$\sigma \circ \tau$ 也是n元置换, 称为σ与τ 的乘积, 记作$\sigma\,\tau$.

例如

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

定义

定理6.11 所有的 n元置换构成的集合S_n关于置换乘积构成群，称为n元对称群. n元对称群的子群称为n元置换群.

因为:

(1) “置换乘积”运算封闭;

(2) 单位元是恒等置换;

(3) 每个n元置换均有逆元.

Note:

对称群是变换群的特例.

置换群是有限群的典型代表.

实例

A={1,2,3}

$$p_1=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\quad p_2=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\quad p_3=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$

$$p_4=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\quad p_5=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\quad p_6=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

$\diamond$	p_1	p_2
p_1	p_1	p_2
p_2	p_2	p_1

置换群

$\diamond$	p_1	p_2	p_3	p_4	p_5	p_6
p_1	p_1	p_2	p_3	p_4	p_5	p_6
p_2	p_2	p_1	p_5	p_6	p_3	p_4
p_3	p_3	p_6	p_1	p_5	p_4	p_2
p_4	p_4	p_5	p_6	p_1	p_2	p_3
p_5	p_5	p_4	p_2	p_3	p_6	p_1
p_6	p_6	p_3	p_4	p_2	p_1	p_5

对称群

对称群的性质

定理6.12 若有限集S的阶为n, 则S的对称群$<S_n,\circ>$的阶为$n!$.

证 由排列组合理论 易证.

定理6.13 对于代数系统$<G,\circ>$, 若G有限且满足结合律和消去律, 则该代数系统是一个群.（有限群的另一种定义）

证 用群的第二个定义证明. 即只要证明$a\circ x=b$和$y\circ a=b$在G中有惟一解.

设G有n个元素$G=\{a_1, a_2, \ldots, a_n\}$, 作集合$G'=\{a\circ a_1, a\circ a_2, \ldots, a\circ a_n\}$, 则$G'\subseteq G$, 根据消去律, 当$i\neq j$时, $a\circ a_i\neq a\circ a_j$

所以G'也有n个不同的元素, 故$G'=G$.

这样, 对G中的元素b必有一a_k, 使得$b=a\circ a_k$, 而且a_k惟一.

同理, 可证$y\circ a=b$有惟一解. 得证.

群的运算表（群表）

有限群的置换运算表称为群表. 群表对研究有限群的性质很有用。设有限群$<G,\circ>$, 其中$G=\{1,2,3\}$, 其群表为:

$\circ$	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

可看出群表的一些性质:

(1) 第一行, 第一列与群元素相同, 且顺序相同;

(2) 每一行(列)内元素各不相同, 且任意两行(列)对应元素亦均不相同;

原因: 每行(列)具有$a\circ a_1, a\circ a_2, \ldots, a\circ a_n$的形式, 由定理6.13证明可知, 成立.

群表

*	e
e	e

*	e	a
e	e	a
a	a	e

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

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

群表的性质

(3) 如果一个群是可换群, 其可换性与群表的对称性一致.

由群表可知, 以上有限群<G,∘>是可换的.

Note:

(1) 一个有限代数系统是否构成群, 是否可换从群表可以看出来;

(2) 有限群<G,∘>中的每个元素对应G的一个置换. 即对$G=\{a_1, a_2, \ldots, a_n\}$, 存在一个函数$\varphi$:

$$\varphi(a_i)=\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_i\circ a_1 & a_i\circ a_2 & \cdots & a_i\circ a_n \end{pmatrix}=p_{ki}\ (i=1,2,\ldots,n)$$

由这些置换组成一个集合$P=\{p_{k1}, p_{k2}, \ldots, p_{kn}\}$. 由于置换是变换的特例, 由定理6.10可知, 这些置换与其置换乘积构成群, 且与其对应的有限群同构.

定理6.14 每个有限群均与一个置换群同构.

6.4 循环群

定义6.14 设G是群，$a\in G$，$n\in Z$，则a 的 n次幂.

$$a^n=\begin{cases} e & n=0 \\ a^{n-1}\circ a & n>0 \\ (a^{-1})^m & n<0, n=-m \end{cases}$$

群中元素可以定义负整数次幂.

在$<Z_3,\oplus>$中有

$$2^{-3}=(2^{-1})^3=1^3=1\oplus 1\oplus 1=0$$

在$<Z,+>$中有

$$(-2)^{-3}=2^3=2+2+2=6$$

元素的阶

定义6.15 设G是群，$a\in G$，使得等式$a^k=e$成立的最小正整数k称为a的阶(或周期)，记作$|a|=k$，称a为k阶元. 若不存在这样的正整数k，则称a为无限阶元.

例如，在$<Z_6,\oplus>$中，

2和4是3阶元，

3是2阶元，

1和5是6阶元，

0是1阶元.

在$<Z,+>$中，0是1阶元，其它整数的阶都不存在.

幂运算规则

定理6.15 设G为群，则G中的幂运算满足：

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

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

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

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

(5) 若G为交换群，则 $(a \circ b)^n = a^n \circ b^n$.

证 (1) $(a^{-1})^{-1}$是a^{-1}的逆元，a也是a^{-1}的逆元. 根据逆元唯一性，等式得证.

(2) $(b^{-1} \circ a^{-1}) \circ (a \circ b) = b^{-1} \circ (a^{-1} \circ a) \circ b = b^{-1} \circ b = e$,

同理 $(a \circ b) \circ (b^{-1} \circ a^{-1}) = e$,

故$b^{-1} \circ a^{-1}$是$a \circ b$的逆元. 根据逆元的唯一性等式得证.

元素的阶

定理6.16 $<G,\circ>$为群，$a\in G$且$|a|=r$. 设k是整数，则

(1) $a^k=e$当且仅当$r\mid k$ （r 整除 k） 因此r 又称为a的周期）

(2)$|a^{-1}|=|a|$

证 (1) 充分性. 由于$r|k$，必存在整数m使得$k=mr$，所以有

$$a^k=a^{mr}=(a^r)^m=e^m=e.$$

必要性. 根据除法，存在整数 m 和 i 使得

$$k=mr+i,\ 0\le i\le r-1$$

从而有 $$e=a^k=a^{mr+i}=(a^r)^m\circ a^i=e\circ a^i=a^i$$

因为$|a|=r$，必有$i=0$. 这就证明了$r\mid k$.

(2) 由 $$(a^{-1})^r=(a^r)^{-1}=e^{-1}=e$$

可知 a^{-1} 的阶存在. 令$|a^{-1}|=t$，根据上面的证明有$t\mid r$.

a又是a^{-1}的逆元，所以 $r\mid t$. 从而证明了$r=t$，即$|a^{-1}|=|a|$

a的逆元的阶是a的阶的因子

循环群

定义6.16 设G是群，若存在$a \in G$使得

$$G=\{a^k \mid k \in \mathbf{Z}\}$$

则称G是循环群，记作$G=\langle a\rangle$，称 a 为G 的生成元.

循环群的分类：n 阶循环群和无限循环群.

设$G=\langle a\rangle$是循环群，若a是n 阶元，则

$$G = \{ a^0=e, a^1, a^2, \dots , a^{n-1} \}$$

那么$|G| = n$，称 G 为 n 阶循环群.

若a 是无限阶元，则

$$G = \{ a^0=e, a^{\pm 1}, a^{\pm 2}, \dots \}$$

称 G 为无限循环群.

例如$\langle \mathbf{Z},+\rangle$是无限循环群，生成元是1和-1； $\langle \mathbf{Z}_6,\oplus\rangle$是6阶循环群，生成元是1和5.（生成元不唯一）

循环群的性质

定理6.17 设$G=\langle a\rangle$是循环群.

(1) 若G是无限循环群，则G与$\langle \mathbf{Z},+\rangle$同构;

(2) 若G是 n 阶循环群，则G与$\langle \mathbf{Z}_n,\oplus\rangle$同构.

证明 略.

Note:

(1) 无限循环群同构于整数加法群;

(2) 周期为n的循环群同构于模n加法群.

(3) 我们对整数加法群和模n加法群的研究很充分.

6.5 子群与群的陪集分解

回忆：

子代数：

设A=<S，*，△，k>是一代数，如果

(1) S' $\subseteq$ S

(2) S'对S上的运算*和△封闭

(3) k∈S'

那么A' = <S'，，△,k>是A的子代数.

子群

定义6.17 设G是群，H是G的非空子集，

(1) 如果H关于G中的运算构成群，则称H是G的子群, 记作$H \leq G$.

(2) 若H是G的子群，且$H \subset G$，则称H是G的真子群，记作$H < G$.

例如 $n\mathbf{Z}$ (n是自然数) 是整数加群$<\mathbf{Z},+>$ 的子群. 当$n \neq 1$时，$n\mathbf{Z}$是$\mathbf{Z}$的真子群.

对任何群G都存在子群. G和$\{e\}$都是G的子群，称为G的平凡子群.

子群判定定理1

定理6.19（判定定理一）

设G为群，H是G的非空子集，则H是G的子群当且仅当

(1) $\forall a,b\in H$有$a\circ b\in H$

(2) $\forall a\in H$有$a^{-1}\in H$.

证 必要性是显然的.

证明充分性。结合律、么元、逆元

只需证明$e\in H$.

因为H非空，存在$a\in H$. 由条件(2) 知$a^{-1}\in H$，根据条件(1) $a\circ a^{-1}\in H$，即$e\in H$.

子群判定定理2

定理6.20 （判定定理二）

设G为群，H是G的非空子集. H是G的子群当且仅当$\forall a,b\in H$有$a\circ b^{-1}\in H$.

证　必要性: H为群必有$b^{-1}\in H$，从而有$a\circ b^{-1}\in H$.

充分性. 因为H非空，必存在$a\in H$.

根据给定条件得$a\circ a^{-1}\in H$，即$e\in H$.

任取$a\in H$, 由$e,a\in H$ 根据给定条件 $e\circ a^{-1}\in H$，即$a^{-1}\in H$.

任取$a,b\in H$，知$b^{-1}\in H$. 再利用给定条件得$a\circ(b^{-1})^{-1}\in H$，即$a\circ b\in H$.

综合上述，可知H是G的子群.

子群判定定理3

定理6.21 （判定定理三）

设G为群，H是G的非空有限子集，则H是G的子群当且仅当$\forall a,b\in H$有$a\circ b\in H$.

证 必要性显然. 为证充分性，只需证明有限集H是一个代数系统, 并且满足结合律和消去律即可.

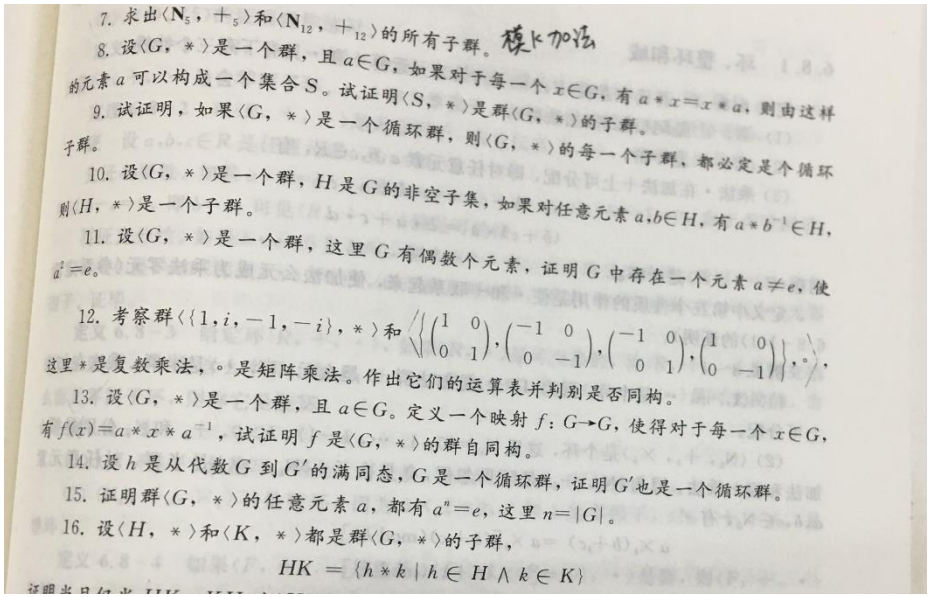
由于G满足结合律和消去律, H是G的子集, 故也满足; 由$a\circ b\in H$可知H是一个代数系统, 故得证.

例：

$<\{[0],[2]\},+_4>$是$<Z_4,+_4>$的子群。

作业

方　p217　8　10　13　14



7. 求出$\langle \mathbf{N}_5, +_5\rangle$和$\langle \mathbf{N}_{12}, +_{12}\rangle$的所有子群。模k加法

8. 设$\langle G, *\rangle$是一个群，且$a\in G$，如果对于每一个$x\in G$，有$a*x=x*a$，则由这样的元素a可以构成一个集合S。试证明$\langle S, *\rangle$是群$\langle G, *\rangle$的子群。

9. 试证明，如果$\langle G, *\rangle$是一个循环群，则$\langle G, *\rangle$的每一个子群，都必定是个循环子群。

10. 设$\langle G, *\rangle$是一个群，H是G的非空子集，如果对任意元素$a,b\in H$，有$a*b^{-1}\in H$，则$\langle H, *\rangle$是一个子群。

11. 设$\langle G, *\rangle$是一个群，这里G有偶数个元素，证明G中存在一个元素$a\neq e$，使$a^2=e$。

12. 考察群$\langle\{1, i, -1, -i\}, *\rangle$和$\left\langle\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}-1&0\\0&-1\end{pmatrix}, \begin{pmatrix}-1&0\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\0&-1\end{pmatrix}\right\}, \cdot\right\rangle$，这里$*$是复数乘法，$\cdot$是矩阵乘法。作出它们的运算表并判别是否同构。

13. 设$\langle G, *\rangle$是一个群，且$a\in G$。定义一个映射$f: G\to G$，使得对于每一个$x\in G$，有$f(x)=a*x*a^{-1}$，试证明f是$\langle G, *\rangle$的群自同构。

14. 设h是从代数G到G'的满同态，G是一个循环群，证明G'也是一个循环群。

15. 证明群$\langle G, *\rangle$的任意元素a，都有$a^n=e$，这里$n=|G|$。

16. 设$\langle H, *\rangle$和$\langle K, *\rangle$都是群$\langle G, *\rangle$的子群，

$$HK = \{h*k \mid h\in H \wedge k\in K\}$$

证明当且仅当 $HK=KH$