离散数学

Discrete Mathematics

2020年新冠疫情网络教学版

蒋瀚

山东大学软件学院

Chapter
05

群

CONTENT

半群

定义 1　设〈S，$\circ$〉为一代数系统，

若

其中运算“$\circ$”满足结合律，即 $\forall x, y, z \in S$，有 $(x \circ y) \circ z = x \circ (y \circ z)$，

则

称〈S，$\circ$〉为半群.

半群

- 例 1　〈**N**，＋〉，〈**N**，·〉，〈**Z**，＋〉，〈**Z**，·〉都是半群.
- 例 2　对任意集合A，〈$P(A)$，$\cup$〉，〈$P(A)$，$\cap$〉均为半群.
- 例 3　集合A到A的全体映射构成的集合 A^A，在复合运算下构成半群〈A^A，$\circ$〉.
- 例 4　在自然数集合**N**上定义运算“$\circ$”：

$$a \circ b = a + b + ab \qquad \forall a, b \in \mathbf{N}$$

半群

- 半群中，$a_1 \circ a_2 \circ \ldots \circ a_n$ 有意义

- 半群〈S，$\circ$〉的运算。通常叫做“乘法”，
- $a \circ b$ 常 简记为 ab

半群

定义2 设〈S，$\circ$〉为一半群，$a \in S$，n为正整数，符号a^n表示n个a的计算结果，即

$$a^n = \overbrace{a \circ a \circ \cdots \circ a}^{n}$$

指数律成立，即对任意正整数m，n和S中的元素a，有

$$a^m a^n = a^{m+n}, \quad (a^m)^n = a^{mn}.$$

半群

□例 5　在半群〈**Z**，＋〉中，

$$1^n = \overbrace{1+1+\cdots+1}^{n} = n \quad ,$$

$$2^n = \overbrace{2+2+2\cdots+2}^{n} = 2n \quad .$$

□在半群〈**Z**，·〉中，

$$1^n = \overbrace{1\cdot 1\cdot 1\cdot\cdots\cdot 1}^{n} = 1$$

$$\overbrace{2\cdot 2\cdot 2\cdot\cdots\cdot 2}^{n} = 2^n$$

$$2^n =$$

半群

- 半群〈S，$\circ$〉中的乘法满足交换律，则称〈S，$\circ$〉为可交换半群
- 在可交换半群〈S，$\circ$〉中, 乘积

$$a_1 a_2 \ldots a_n$$

中各项任意交换次序，所得运算结果相同

- 在可交换半群中有另一指数律：

$$(ab)^n = a^n b^n.$$

半群

- 对于可交换半群，其运算常用加法记号“＋”表示：
- 将 a^n 记为na，即 $na=\overbrace{a+a+a+\cdots+a}^{n}$
- 指数律形式：

$$ma+na=(m+n)a.$$

$$m(na)=(mn)a.$$

$$n(a+b)=na+nb.$$

半群

- 定义 3　若半群〈S，$\circ$〉中有单位元，即存在$e\in S$，使得$\forall x\in S$，$xe=ex=x$，则称〈S，$\circ$〉为幺半群（有1半群、独异点）.
- 例如，〈$\mathbf{N}$，＋〉，〈$\mathbf{Z}$，＋〉，〈$\mathbf{N}$，$\cdot$〉，〈$\mathbf{Z}$，$\cdot$〉等均为幺半群. 但偶数集合 E 在乘法下形成的半群〈E，$\cdot$〉不是幺半群.
- 使用加法记号时，单位元常用0表示，称为零元

半群

- 设〈S，$*$〉为幺半群，如果 $a \in S$的逆元存在，则由于。满足结合律，其逆元必是唯一的.
- 在幺半群〈S，$*$〉中用a^{-1}表示a的唯一逆元，即$a^{-1} \in S$，且

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

- 当采用加法记号时，a^{-1}常记作$-a$，且称为a的负元.

半群

定理 1　对幺半群 $\langle S, * \rangle$，若 $a, b \in S$ 的逆元 a^{-1}, b^{-1} 存在，则

（1）$(a^{-1})^{-1} = a.$

（2）$(ab)^{-1} = b^{-1}a^{-1}.$

证明　由定义，得 $a^{-1}a = aa^{-1} = e,$

故 $(a^{-1})^{-1} = a$；

又 $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = e.$

同理 $(b^{-1}a^{-1})(ab) = b^{-1}b = e$

故由逆元定义，$(ab)^{-1} = b^{-1}a^{-1}.$

半群

- 定义 4　设〈S，$\circ$〉为一半群，若$T \subseteq S$在S的运算$\circ$下也构成半群，则称〈T，$\circ$〉为〈S，$\circ$〉的子半群.
- 只要$T \subseteq S$对运算$\circ$封闭，则〈T，$\circ$〉即为〈S，$\circ$〉的子半群
- 例：〈$\mathbf{N}$，$\cdot$〉，〈$\mathbf{Z}$，$\cdot$〉，〈$\mathbf{Q}$，$\cdot$〉
- 例 7　$T = \{km \mid k \in \mathbf{N}\}$，是〈$\mathbf{N}$，$\cdot$〉子半群.
- 例 8　〈S，$*$〉是半群，$a \in S$，

  $T = \{a^i \mid i \in \mathbf{Z}^+\}$，则$T$是$S$的子半群.

半群

- $\langle S, * \rangle$ 有单位元 e，$\langle S, * \rangle$ 的子半群未必有单位元，即使有的话，也未必等于 e
- 例 9

  （1）偶数集 E 在乘法运算下构成的半群 $\langle E, \cdot \rangle$ 是 $\langle \mathbf{Z}, \cdot \rangle$ 的子半群

  （2）$A \neq \varnothing$，$B \subseteq A$，则 $\langle P(B), \cap \rangle$ 为 $\langle P(A), \cap \rangle$ 的子半群

半群

- 定义 5　设S是幺半群，若T是S的子半群，且S的单位元$e \in T$，则称T是S的子幺半群.
- 例10　设〈S，*〉是幺半群，$a \in S$，

  $T=\{a^i \mid i \in \mathbf{N}\}$是$S$的子幺半群，

  其中$a^0 = e$.
- 例11　设〈S，*〉是可交换幺半群，

  $T=\{a \mid a \in S, a * a = a\}$是$S$的子幺半群.

作业

习题一 2，3

CONTENT

群的概念及基本性质

定义 1　设〈G，*〉为么半群，如果

$\forall a \in G$，a的逆元a^{-1}均存在，

则称〈G，*〉为群.

一个代数系统〈G，*〉，如果满足下列条件：

（1） 结合律成立

（2） G中具有单位元

（3） $\forall a \in G$，存在$a^{-1} \in G$.

称〈G，*〉为群.

群的概念及基本性质

- 当群G中只含有有限个元素时，称其为有限群，否则称其为无限群．有限群G的元素个数称为群G的阶，并规定无限群G的阶为∞. 群G的阶也记为$|G|$.

- 一个群G，如果其运算是可交换的，则称之为交换群或Abel群.

群的概念及基本性质

- 例 1　有限交换群〈{ 1，－1 }，·〉
- 例 2　〈**Z**，＋〉，〈**Q**，＋〉，〈**R**，＋〉均为无限交换群，〈$\mathbf{Q}^+$，·〉，〈$\mathbf{R}^+$，·〉也为无限交换群，但〈**Q**，·〉，〈**R**，·〉不是群
- 例 3　〈$\mathbf{Z}_n$，$+_n$〉为有限交换群，其中零元为［0］，［i］的负元为$[-i]=[n-i]$.

群的概念及基本性质

定理 1　设〈G，$*$〉为群，则

（1）G中消去律成立.

（2）单位元e是G中唯一幂等元.

证明　（1）$\forall a, b, c \in G$，设$ab = ac$,

则　$a^{-1}(ab) = a^{-1}(ac)$

于是　$(a^{-1}a)b = (a^{-1}a)c$，　故　$b = c$.

同理，若$ba = ca$，则 $b = c$．因此G中消去律成立.

(2) 显然e是幂等元，又若 $a \in G$ 是幂等元，则$aa = a$，因此$a^{-1}aa = a^{-1}a$，故得$a = e$，因此e是G中唯一幂等元.

群的概念及基本性质

定理 2　设〈G，$*$〉，〈H，$\circ$〉是群，f 是G到H的同态．若e 为G的单位元,则$f(e)$为H的单位元，且$\forall a \in G$，有$f(a)^{-1} = f(a^{-1})$．

证明　$f(e) \circ f(e) = f(e * e) = f(e)$．

故　$f(e)$是H的幂等元，从而是单位元.

又，$\forall a \in G$

$f(a) \circ f(a^{-1}) = f(a * a^{-1}) = f(e)$，

$f(a^{-1}) \circ f(a) = f(a^{-1} * a) = f(e)$．

故　$f(a^{-1})$为$f(a)$的逆，即$f(a)^{-1} = f(a^{-1})$.

群的概念及基本性质

定理 3　设〈G，$*$〉是群，〈H，$\circ$〉是任意代数系统，若存在G到H的满同态, 则<H，$\circ$>必为群.

证明　设f: $G\sim H$，则由满同态的性质知，H中运算$\circ$满足结合律，

且G的单位元e的象$f(e)$是H的单位元，

又f为满射，$\forall y\in H$，$\exists x\in G$使$y=f(x)$，

$$y^{-1}=f(x)^{-1}=f(x^{-1})$$

所以，〈H，$\circ$〉是群.

群的概念及基本性质

定理 4　设〈G，$*$〉是一个半群，且

（1）G中有一左单位元 e，使

$$e\,a = a \quad , \quad \forall\, a \in G.$$

（2）G中任一元素a，均有一“左逆元”

a^{-1}，使 $a^{-1}a = e$.

则G为群.

证明　1)“左逆元”也是“右逆元”；2）左单位元也是右单位元

故知G为群。

群的概念及基本性质

1) “左逆元” 也是 “右逆元”

$\forall\, a \in G$，有 $a^{-1} \in G$ 使 $a^{-1}\, a = e$，

又对 $a^{-1} \in G$，有 $(a^{-1})^{-1} \in G$ 使 $(a^{-1})^{-1}\, a^{-1} = e$，

因此，

$$
\begin{aligned}
a\, a^{-1} &= e\ (a\, a^{-1}) \\
&= ((a^{-1})^{-1}\, a^{-1})\ (a\, a^{-1}) \\
&= (a^{-1})^{-1}\ (a^{-1}\, a)\, a^{-1} \\
&= (a^{-1})^{-1}\, e\, a^{-1} \\
&= (a^{-1})^{-1}\, a^{-1} \\
&= e
\end{aligned}
$$

群的概念及基本性质

□2） 左单位元 也是 右单位元

$\forall\, a \in G,$

$$a\,e$$

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

$$= (aa^{-1})\,a$$

$$= ea$$

$$= a.$$

故e确为右单位元.

群的概念及基本性质

定理 5　设〈G，$*$〉是半群，如果$\forall\, a$，$b\in G$，方程

$$ax=b,\qquad ya=b$$

在G中总有解，则G是群.

证明　证G有左单位元、每个元素有“左逆元”。

1) 任取 $b\in G$ 令 $y\,b=b$ 的一个解为e，则$e\,b=b$.

$\forall\, a\in G$，设$b\,x=a$的解为c，即　$bc=a$

则　　$e\,a=e(bc)=(e\,b)\,c=bc=a$；

2) 任取$a\in G$，$y\,a=e$有解，设a'为一解，则$a'\,a=e$，

由定理 4 可知，G是群.

群的概念及基本性质

定理 6　有限半群，如果消去律成立则必为群.

证明　证明 $\forall a，b\in G，ax=b，ya=b$均有解

设G中有n个元素：$G=\{a_1，a_2，\ldots，a_n\}$，

$\forall a，b\in G$,若$ax=b$，令$aG=\{aa_1，aa_2，\ldots，aa_n\}$，则 $aG\subseteq G$，由消去律知：当$i\neq j$时，$aa_i\neq aa_j$

因此，aG中也含有n个元素，故 $aG=G$，从而知$b\in aG$　故$\exists\, k$ 使得$aa_k=b$，或者说$ax=b$有解.

同理可证$ya=b$也必有解.

综上可得，G为群。

群的概念及基本性质

定理 7 〈G，$*$〉是有限群，则其运算表中每一行（列）都是G中元素的一个全排列.

证明 设 $G = \{a_1, a_2, \ldots, a_n\}$，

则其运算表中第i行为

$$a_i a_1,\ a_i a_2,\ \ldots,\ a_i a_n$$

这是G中元素的一个全排列(只需证明其中任意两项必不相同)：

若$a_i a_j = a_i a_k$，$j \neq k$，

则由消去律得$a_j = a_k$，矛盾。

群的概念及基本性质

- 一、二、三阶群唯一
- 四阶群有两个：

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

Klein四元群

群的概念及基本性质

- $G=\{e, a\}$，则$G\times G$的运算表为

$\circ$	$<e,e>$	$<e,a>$	$<a,e>$	$<a,a>$
$<e,e>$	$<e,e>$	$<e,a>$	$<a,e>$	$<a,a>$
$<e,a>$	$<e,a>$	$<e,e>$	$<a,a>$	$<a,e>$
$<a,e>$	$<a,e>$	$<a,a>$	$<e,e>$	$<e,a>$
$<a,a>$	$<a,a>$	$<a,e>$	$<e,a>$	$<e,e>$

- $<G\times G, \circ>$是Klein四元群

*	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

*	0	2	1	3
0	0	2	1	3
1	1	3	2	0
2	2	0	3	1
3	3	1	0	2

*	0	2	1	3
0	0	2	1	3
2	2	0	3	1
1	1	3	2	0
3	3	1	0	2

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

作业

- 习题二 1，2，5，6

CONTENT

子群与元素的周期

- 定义 1　设〈G，*〉是一个群，$H \subseteq G$，如果H在G的运算下也构成群，则称
  〈H，*〉为〈G，*〉的子群.
- 例 1　任何群G都有两个平凡子群：｛e｝，G，其它子群称为真子群.
- 例 2　〈$\mathbf{Z}$，＋〉，〈$\mathbf{Q}$，＋〉，〈$\mathbf{R}$，＋〉中，前者均为后者的子群.
- 例 3　记$\boldsymbol{R}^* = \boldsymbol{R}$-{0}，则〈$\boldsymbol{R}^*$，·〉是群，
  <{ 1 ，－ 1 }，· >，<$\boldsymbol{R}^+$，·>均为$\boldsymbol{R}^*$ 的子群，但不是〈$\mathbf{R}$，＋〉的子群.

子群与元素的周期

- 例 4　设〈G，$*$〉，〈H，$\circ$〉为两个群，f是G到H的同态，A是G的子群，则$f(A)$是H的子群.
- 证明　$\forall y_1, y_2 \in f(A)$，$\exists x_1, x_2 \in A$，使

$$f(x_1) = y_2,\ f(x_2) = y_2$$

故　　$y_1 \circ y_2 = f(x_1) \circ f(x_2) = f(x_1 * x_2) \in f(A)$.

故，$f(A)$对$\circ$是封闭的，〈$f(A)$，$\circ$〉是代数系统.

由于

$$f|_A: A \sim f(A)$$

由上节定理 3 [1]，〈$f(A)$，$\circ$〉是群，从而$f(A)$是H的子群.

[1] §2　定理 3　设〈G，$*$〉是群，〈H，$\circ$〉是任意代数系统，若存在G到H的满同态, 则<H，$\circ$>必为群.

子群与元素的周期

定理 1 设H是群G的子群，则H的单位元 e' 就是G的单位元e．对$a\in H$，a在H中的逆元 a' 就是a在G中的逆元a^{-1}.

证明 （1） e'是H的单位元，则$e'e'=e'$，故 e' 为G的幂等元，但G的单位元e是唯一幂等元，故$e'=e$.

（2）$\forall\, a\in H$， a'为a 在H中的逆元，且$e'=e$，故 $a'a=aa'=e'=e$.

因而，a' 为a在G中的逆元.

子群与元素的周期

定理 2 设H是群$\langle G, * \rangle$的非空子集，则

H是G的子群 当且仅当

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

（2）$\forall a \in H$，a在G中的逆元$a^{-1} \in H$.

证明

$\Rightarrow$: 设H是G的子群，则由定义知（1）必成立．又由定理 1 知，a在G中的逆元$a^{-1} \in H$.

$\Leftarrow$: 设（1）、（2）成立，则由（1）知H为半群．H非空，取$a \in H$，由（2），$a^{-1} \in H$，由（1），$a * a^{-1} = e \in H$，显然，e是H的单位元．

又，$\forall a \in H$，$a^{-1} \in H$必是a在H中的逆元．故H是子群．

子群与元素的周期

推论 设〈G，$*$〉为群，S是G的非空子集，则

$$S\text{是}G\text{的子群} \Leftrightarrow \forall\, a，b\in S \quad a * b^{-1} \quad \in S.$$

证明 必要性显然；充分性：

$S\neq\varnothing$，取 $a\in S$，于是，$e=a * a^{-1} \in S$. 从而，$\forall\, a \in S$，$a^{-1}=e * a^{-1} \in S$. 完了没？

$\forall\, a, b\in S$，由以上所证，$b^{-1} \in S$，故

$$a * b = a * (b^{-1})^{-1} \in S,$$

从而S是G的子群.

子群与元素的周期

例 5　设G是群，

$$C=\{a|a\in G,\ \forall x\in G:\ ax=xa\},$$

则C为G的子群，称为群G的中心.

证明　$\forall x\in G$，$ex=xe$，故$e\in C$，即C非空. 设a，$b\in C$，则$\forall x\in G$，

$$(ab)x=a(bx)=a(xb)=(ax)b=(xa)b=x(ab).$$

即$ab\in C$. 又设$a\in C$，则$\forall x\in G$，$ax=xa$，两边左乘a^{-1}，得$x=a^{-1}xa$，两边再右乘a^{-1}，得$xa^{-1}=a^{-1}x$. 从而得知$a^{-1}\in C$. 故C是子群.

子群与元素的周期

- 对于半群〈S，$*$〉中的元素a，

$$a^n = a * a * \ldots * a.$$

- 如果〈S，$*$〉是幺半群，e是S的单位元，$a \in S$，令$a^0 = e$

- 如果〈S，$*$〉是群，$a \in S$，n为正整数，令

$$a^{-n} = (a^{-1})^n.$$

子群与元素的周期

例 6　设G是群，$a\in G$，令

$$(a)=\{a^i \mid i\in \mathbf{Z}\},$$

则(a)是G的子群，称为由a 生成的循环子群.

证明　显然(a)非空，又$\forall a^i, a^j\in(a)$,

$$a^i a^j = a^{i+j}\in (a);$$

又，$\forall\, a^i\in (a)$由指数律

$$(a^i)^{-1} = a^{-i}\in (a)$$

故(a)为G的子群.

子群与元素的周期

- 例 7　对$<\mathbf{Z}, +>$, $(2)=\{2i \mid i\in\mathbf{Z}\}$, $(1)=\{i \mid i\in\mathbf{Z}\}=\mathbf{Z}$

  对于$\langle R^+, \cdot\rangle$，$(2)=\{2^i \mid i\in\mathbf{Z}\}$，$(1)=\{1\}$

- 例 8　考虑$\langle \mathbf{Z}_6, +_6\rangle$则

  $([2])=\{[0], [2], [4]\}$

  $([5])=\{[0], [5], [4], [3], [2], [1]\}=\mathbf{Z}_6$

  $([3])=\{[0], [3]\}$

- (a)既可以是有限群，也可以是无限群

子群与元素的周期

- 定义 2　设G是群，$a \in G$，若存在正整数n，使$a^n = e$，则将满足该条件的最小正整数n称为a的周期（阶），若这样的n不存在，称a的周期为∞.

- a的周期为n，则$a^n = e$且$0<m<n$时$a^m \neq e$.

- 用$|a|$表示a的周期（阶）．并将周期（阶）为n的元素称为n阶元素.

子群与元素的周期

例 9　在〈$\mathbf{Z}$，＋〉中，0 的周期为 1，

$\forall i \in \mathbf{Z}$，$i \neq 0$，i的周期为 ∞；

在〈$\mathbf{Z}_6$，$+_6$〉中，［2］的周期为 3，［5］的周期为 6，［3］的周期为 2．

子群与元素的周期

定理 3　设G是一个群，$a \in G$，

（1）a的周期等于a生成的循环子群（a）的阶，即

$$|a| = |(a)|$$

（2）若a的周期为$n < \infty$，则

$$a^m = e \Leftrightarrow n \mid m.$$

子群与元素的周期

- 证明$|a|=|(a)|$
- **证明** （1）分两种情况证明$|a|=|(a)|$

（i）a的周期n为有限数，往证 $(a)=\{a^0, a^1, \ldots, a^{n-1}\}$ 且 $a^0, a^1, \ldots, a^{n-1}$ 互不相同.

$\forall a^i \in (a)$，令$i = kn + r$，$k, r \in \mathbf{Z}$，$0 \le r < n$

则 $a^i = a^{kn+r} = a^{kn} a^r = a^r$

故 $a^i \in \{a^0, a^1, \ldots, a^{n-1}\}$

因此 $(a) \subseteq \{a^0, a^1, \ldots, a^{n-1}\}$

又显然 $\{a^0, a^1, \ldots, a^{n-1}\} \subseteq (a)$，

所以 $(a) = \{a^0, a^1, \ldots, a^{n-1}\}$.

子群与元素的周期

- 证明| a |=|（a）|
- 下面说明 a^0，a^1，…，a^{n-1}互不相同

  若 $a^i = a^j$　　$0 \le i, j < n$，$i \ne j$

  不妨设$i>j$，则 $a^{i-j} = e$，　$0 < i-j < n$，与a的周期为n矛盾.

  所以 a^0，a^1，…，a^{n-1}互不相同，

  从而 |（a）|= n，即有 |a|=|（a）|.

子群与元素的周期

- 证明$|a|=|(a)|$
- （ii）a的周期为∞，这时

$$a^1,\ a^2,\ \ldots,\ a^i\ \ldots$$

互不相同，故$|(a)|=\infty$，

因此也有$|a|=|(a)|$.

总之，$|a|=|(a)|$成立.

子群与元素的周期

□证明$a^m = e \Leftrightarrow n \mid m$

□（2）设$a^m = e$，令

$$m = kn + r, \qquad 0 \le r < n$$

则 $$a^m = a^{kn+r} = a^{kn} a^r = a^r$$

因此 $$a^r = e, \quad 0 \le r < n$$

由于a的周期为n，故必有$r = 0$，即$n \mid m$.

反之，若$n \mid m$，显然$a^m = e$.

子群与元素的周期

- **推论** 设G为群，$a\in G$，若a的周期为n（或等价地说（a）的阶为n），则

$$(a)=\{a^0, a^1, \ldots, a^{n-1}\}$$

- 例10 设a，b是群G的元素．$|a|=2$，$|b|=3$，且$ab=ba$，则$|ab|=6$．
- **证明** 因$(ab)^6=a^6b^6=e$，故ab必有有限周期，设$|ab|=n$，则$n|6$，故n只有四种可能，$n=1$，2，3或6．若$n=1$，则$ab=e$，$b=a^{-1}$，$b^2=(a^{-1})^2=(a^2)^{-1}=e$，矛盾，故$n\neq 1$．又$(ab)^2=a^2b^2=b^2\neq e$，故$n\neq 2$．$(ab)^3=a^3b^3=a\neq e$，故$n\neq 3$．
- 因此，$n=6$．

作业

- 习题三 1，4，6，8

CONTENT

循环群

- 定义 1　设G是一个群，如果存在$a \in G$，使$G = (a) = \{a^i \mid i \in \mathbf{Z}\}$，称$G$为由$a$生成的循环群，$a$称为其生成元.

- 由定义可见，G是由a生成的循环群，意味着G的任何元素x，均可表示成a的方幂形式，即

  G是由a生成的循环群 $\Leftrightarrow \forall\, x \in G$，$\in i \in \mathbf{Z}$使$x = a^{\,i}$.

循环群

例 1　〈**Z**，＋〉是循环群．事实上，

$$\mathbf{Z}=(1),\ Z=(-1)$$

例 2　〈**Q**，＋〉不是循环群．事实上，0 显然不是**Q**的生成元，而对**Q**中任何非零元素a，$a/2$ 不能表成 na（$n\in\mathbf{Z}$）的形式，即

$$a/2 \notin (a)$$

例 3　〈$\mathbf{Z}_n$，$+_n$〉是循环群，$\mathbf{Z}_n=([1])$.

循环群

□设〈G，$\circ$〉是由下面的运算表定义的四阶群,则$G=(b)$.

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

循环群

定理 1　设〈G，$*$〉是一个循环群，

若G是无限群，则

$$\langle G, * \rangle \cong \langle \mathbf{Z}, + \rangle ,$$

若G是n阶群，则

$$\langle G, * \rangle \cong \langle \mathbf{Z}_n, +_n \rangle .$$

循环群

证明 （1）设G是无限循环群，设a为其生成元，

$$G=(a)=\{\ldots,\ a^{-2},\ a^{-1},\ a^{0},\ a^{1},\ a^{2},\ \ldots\}$$

令f：$\mathbf{Z}\to G$，定义如下：

$$f(i)=a^{i},\quad \forall\, i\in\mathbf{Z}.$$

显然f为满射．下证f为单射，$\forall\, i,\ j\in\mathbf{Z}$若$f(i)=f(j)$，即$a^{i}=a^{j}$，要证$i=j$．若$i\neq j$，不妨设$i>j$，则

$$a^{i-j}=e,\quad i-j>0$$

因此a必有有限周期，从而$G=(a)$为有限群，矛盾．所以，$i=j$，从而f为单射．总之f是双射．

又$\forall i,\ j\in\mathbf{Z}$，$f(i+j)=a^{i+j}=a^{i}*a^{j}=f(i)*f(j)$

即f保持运算，从而f：$\mathbf{Z}\cong G$.

循环群

- （2）设G为n阶循环群，a为其生成元，则$|a|=n$，且

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

其中$a^0, a^1, a^2, \ldots, a^{n-1}$互不相同，令

$$f([i]) = a^i \quad , \quad \forall [i] \in \mathbf{Z}_n$$

则显然f是$\mathbf{Z}_n$到G的满射，又设

$$f([i]) = f([j])，即 a^i = a^j，则 a^{i-j} = e,$$

由周期的性质可知，$n \mid i-j$即$i \equiv j \mod n$.

因此$[i] = [j]$. 从而知f是单射. 总之f是双射.

下证f是同态. $\forall [i], [j] \in \mathbf{Z}_n$,

$$f([i]+_n[j]) = f([i+j]) = a^{i+j} = a^i * a^j = f([i]) * f([j])$$

- 因此 $f: \mathbf{Z}_n \cong G.$

循环群

定理 2　循环群的子群必为循环群.

证明　设G是由a生成的循环群，H是其子群，

若$H=\{a^0\}=\{e\}$，则H是由e生成的循环群，

若$H\neq\{e\}$，则必有$n\neq 0$使$a^n\in H$，由于H为子群，故$a^{-n}\in H$．n与$-n$中必有一个为正整数，因此H中必有a的正整数次幂．令

$$i_0=\min\{i\mid a^i\in H,\quad i>0\}$$

即i_0是H中a的最小正指数．往证$H=(\quad)$，$\forall\, a^i\in H$，令

$$i=ki_0+r,\quad 0\leq r<i_0$$

则　　$a^{ki_0+r}=a^{ki_0}$

$a^r=$　　

由此易知$a^r\in H$，由于$0\leq r<i_0$并注意到i_0的定义，可知必有$r=0$．

即　　$i=ki_0$，　　$a^i=(\quad)^k$.

从而　　$H=(\quad)$.

循环群

定理 3　设〈G，*〉是n阶循环群，m是正整数且 $m \mid n$，则G中存在唯一一个m阶子群.

证明　由于$m|n$，设$n = dm$，则$(a^d)^m = a^{dm} = a^n = e$.

又,$\forall h \in \mathbf{Z}$，若 $0 < h < m$，则 $0 < dh < n$，故由周期的定义,

$(a^d)^h = a^{dh} \neq e$.

从而a^d的周期为m，因此，a^d生成的循环子群$A = (a^d)$是G的m阶子群.

下面再证G中m阶子群是唯一的. 在G中任取一m阶子群H，由定理 2 知，H是循环群，设H的生成元为a^i，即 $H = (a^i)$，则 a^i 的周期为m，因此

$$a^{im} = (a^i)^m = e.$$

所以　　$n \mid im$，即　　$md \mid im$，可见 $d \mid i$，不妨设$i = kd$，则

$$a^i = a^{kd} = (a^d)^k$$

因此，$a^i \in A$. 从而，对任何$j \in \mathbf{Z}$，$(a^i)^j \in A$，因而$H \subseteq A$，又H与$A = (a^d)$均有m个元素，所以有$H = (a^d)$，这样就证明了G中有唯一的m阶子群.

作业

- 习题四 1，2，3，4

CONTENT

置换群

- 定义 1　有限集S到自身的双射称为S上的置换，当$|S|=n$时，S上的置换也称为n次置换.

- A=｛1，2，3，4｝

- f_1={<1,2>,<2,3>,<3,4>,<4,1>}是A上的置换

置换群

- 设$S=\{1, 2, \ldots, n\}$，S上的一个置换σ，可以表示成如下形式

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

$$\sigma=\begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ \sigma(i_1) & \sigma(i_2) & \cdots & \sigma(i_n) \end{pmatrix}$$

置换群

- A={ 1， 2， 3， 4 }
- f_1={<1,2>,<2,3>,<3,4>,<4,1>}是A上的置换

$$f_1=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}=\begin{pmatrix}1&3&4&2\\2&4&1&3\end{pmatrix}$$

置换群

- 置换的复合也称为置换的乘法. 两置换σ，τ 进行复合的结果$\sigma\circ\tau$ 也称为σ与τ的乘积，简记为 $\sigma\tau$

$$\tau=\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix}\qquad \sigma=\begin{pmatrix}i_1 & i_2 & \cdots & i_n\\ j_1 & j_2 & \cdots & j_n\end{pmatrix}$$

$$then\quad \sigma\tau=\begin{pmatrix}i_1 & i_2 & \cdots & i_n\\ j_1 & j_2 & \cdots & j_n\end{pmatrix}\begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix}=\begin{pmatrix}1 & 2 & \cdots & 3\\ j_1 & j_2 & \cdots & j_n\end{pmatrix}$$

置换群

例

$$let \quad \varphi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \varphi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$then \quad \varphi_1\varphi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\varphi_1^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 3 & 2 & 1 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

置换群

□定义 2　S上如下形状的置换

$$\sigma=\begin{pmatrix} i_1 & i_2 & \cdots & i_{d-1} & i_d & i_{d+1} & \cdots & i_n \\ i_2 & i_3 & \cdots & i_d & i_1 & i_{d+1} & \cdots & i_n \end{pmatrix}$$

称为循环置换，记为（i_1，i_2，…，i_d），d为循环长度．当$d=2$时称为对换．

□单位置换即恒等映射也视为循环置换，并记为（1）或（n）

置换群

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} = (1\ \ 2\ \ 4)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} = (2\ \ 3)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = (1)$$

置换群

- 设$S=\{1, 2, \ldots, n\}$，所有n次置换（即$S=\{1, 2, \ldots, n\}$上的所有置换）构成的集合将用符号S_n表示.
- **定理 1**　S_n在置换乘法运算下构成群.
- 证明　$\forall f, g \in S_n$，$g \circ f \in S_n$，即S_n对运算。封闭，而。满足结合律，故知〈S_n，。〉是一个半群，显然，恒等映射$Is \in S_n$，且是〈Sn，。〉中单位元，又，对任意$f \in S_n$，f的逆函数$f^{-1} \in S_n$且$f^{-1} \circ f = f \circ f^{-1} = Is$. 即$f^{-1}$为$f$在〈$S_n$，。〉中的逆元，从而〈$Sn$，。〉是群.

置换群

定理 2　$|S_n| = n!$

定义 3　S_n称为*n*次对称群，其子群称为*n*次置换群.

例 3　会不会写出〈S_3，∘〉的元素与运算表？

置换群

例 4　设$S=\{a, b, c, d\}$

$$\varphi_1=\begin{pmatrix} a & b & c & d \\ a & c & b & d \end{pmatrix},\quad \varphi_2=\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}$$

则$\{\varphi_1, \varphi_2\}\subseteq S_4$，且〈$\{\varphi_1, \varphi_2\}$，$\circ$〉构成群，因此〈$\{\varphi_1, \varphi_2\}$，$\circ$〉是一个$S$上的 2 阶置换群.

定理 3 （Cayley定理）

□任意n阶群必同构于一个n次置换群.

□证明

1）设G为一个n阶群，G_n是G上的所有置换构成的n次对称群

2）构造一个G上的置换群 F_G.

3）证明 $G \cong F_G$

4）定理得证.

定理3（Cayley定理）-续

2）构造一个G上的置换群 F_G

$\forall a \in G$，令 $f_a(x) = ax$ ， $\forall x \in G$

则 f_a 是一个G上的置换（WHY？），

令 $F_G = \{f_a \mid a \in G\}$， 则 F_G是G_n的子群：

$\forall fa, fb \in F_G$，$(fa\, fb)(x) = f_a(f_b(x)) = abx = f_{ab}(x)$

$f_e = I_G$; 又对任意 $f_a \in F_G$，

$$f_a f_{a^{-1}}(x) = f_a(f_{a^{-1}}(x)) = f_a(a^{-1}x) = a(a^{-1}x) = x$$

定理 3 （Cayley定理）-续

□3）证明 $G \cong F_G$

令 $h: G \to F_G,\quad h(a) = f_a,\quad \forall a \in G$

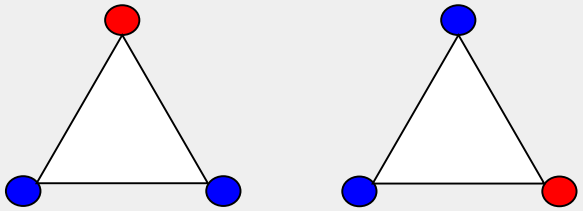
显然h为满射，

又若$a \neq b$，则$f_a(e) \neq f_b(e)$，故$f_a \neq f_b$，因此h也是单射. 从而，h是双射. 又，

$$h(ab) = f_{ab} = f_a f_b = h(a)h(b)$$

即h保持运算，故知 $h: G \cong F_G$，

置换群



作业：

- 习题五 3

CONTENT

陪集

□模m同余关系 R_m

□$\forall\ a,\ b\in\mathbf{Z}$,

$$a\equiv b \bmod m$$

$$\Leftrightarrow m \mid a-b$$

$$\Leftrightarrow\ a-b\in\{km \mid k\in\mathbf{Z}\}$$

$$\Leftrightarrow\ a+(-b)\in(m)\ (Z\text{的子群})$$

陪集

定义 1　设G是一个群，H是其子群，利用H在G上按如下方式定义关系R_H，

$$a\,R_H\,b \Leftrightarrow b^{-1}a \in H$$

称R_H为模H左同余关系，

将$a\,R_H\,b$记为　$a \equiv b \bmod H$，

陪集

定理 1　设H是群$\langle G, * \rangle$的子群，则G中的模H左同余关系R_H是等价关系.

定理 2　设H是G的子群，则$a \in G$所在的模H左同余关系等价类

$$[a] = \{ah \mid h \in H\}.$$

以后将用aH表示$[a]$

陪集

定义 2　设H是群G的子群，H的所有左陪集构成的集合，即集合族

$$S_L=\{aH\mid a\in G\}$$

称为G对H的左商集

定义 3　设H是群G的子群，H的左（右）陪集数称为H在G内的指数，记为

$[G:H]$.

陪集

定理 6 （拉格朗日定理）

设G是有限群，H是其子群，则H的阶必整除G的阶,且

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

陪集

推论 1　素数阶群必为循环群.

证明　设G是p阶群，p是素数，则$p>1$，因此可取$a\in G$，$a\neq e$，设（a）的阶为m，则$m>1$，且由拉格朗日定理，$m|p$，由于p为素数，故$m=p$，即（a）是p阶循环子群，从而知G的p个元素均含于（a）中，故$G=$（a）.

推论 2　G为有限群，则 $\forall a\in G$，$|a|$整除 $|G|$.

推论 3　G为有限群，则 $\forall\, a\in G$，$a^{|G|}=e$.

CONTENT

CONTENT