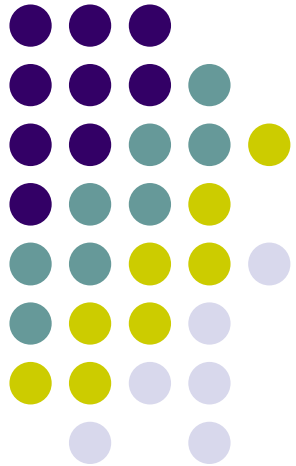
循环群与群同构

离散数学—代数结构

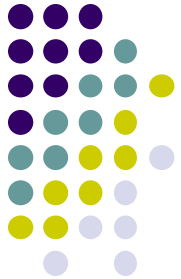
南京大学计算机科学与技术系



循环群与群同构

- 循环群与生成元
- 循环群的子群
- 群的同构与同态
- 无限循环群的同构群
- 有限循环群的同构群
- (循环)群的直积

循环群与生成元



- 定义（循环群）

$\langle G,* \rangle$为循环群（cyclic group）是指：

$$(\exists a \in G)(G = \langle a \rangle)$$

这里，$\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$，$a$称为$G$之生成元（generator）

循环群与生成元（续）

- 定义（有限循环群）：若循环群G的生成元a的阶为n，则称G为有限循环群，即n阶循环群。

  $\boldsymbol{G=\{a^0,a^1,a^2,\cdots,a^{n-1}\}}$，其中$a^0$为单位元。

- 定义（无限循环群）：若循环群G的生成元a为无限阶元，则称G为无限循环群。

  $\boldsymbol{G=\{a^0,a^{\pm1},a^{\pm2},\cdots\}}$，其中$a^0$为单位元。

循环群与生成元（续）

- 例1：无限循环群$\langle \mathbb{Z}, + \rangle$

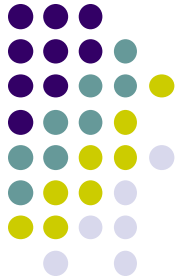
$\langle \mathbb{Z}, + \rangle$是循环群，恰有2个生成元：1和$-1$

$\because n$为$\mathbb{Z}$之生成元$\Leftrightarrow \mathbb{Z} = \langle n \rangle \Leftrightarrow (\exists k \in \mathbb{Z}) n^k =$

$1 \Leftrightarrow (\exists k \in \mathbb{Z})(k \cdot n = 1) \Leftrightarrow n \in \{1, -1\}$

$\therefore$ 1和-1均是其生成元

循环群与生成元（续）



- 例2：有限循环群

模6剩余加群$\langle \mathbb{Z}_6, \oplus_6 \rangle$是循环群，恰有2个生成元：1 和 5

$$5^0 = 0,\ 5^1 = 5,\ 5^2 = 4,$$

$$5^3 = 3,\ 5^4 = 2,\ 5^5 = 1.$$

循环群与生成元（续）

- 例3：非循环群

Klein四元群$(V,*)$不是循环群，因为对任何$x \in V$，

$\langle x \rangle = \{e, x\}$：

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

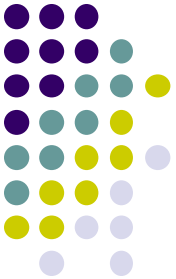
无限循环群的生成元

- 命题：若a是无限循环群的生成元，则a^{-1}也是该无限循环群的生成元

  - 设群$G=\langle a\rangle=\{a^k \mid a\in G, k\in\mathbb{Z}\}$，$a^k=(a^{-1})^{-k}$，

    令$p=-k$，则$G=\{(a^{-1})^p \mid p\in\mathbb{Z}\}$，故$G=\langle a^{-1}\rangle$

无限循环群的生成元（续）

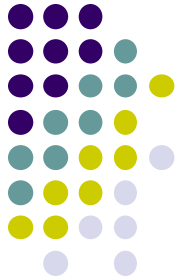


- 命题：无限循环群有且只有2个生成元
- ∵ 设群$G = \langle a \rangle = \{a^k | a \in G, k \in \mathbb{Z}\}$，若$b$亦为$G$的生成元，则：$(\exists m, t \in \mathbb{Z})(a^m = b \wedge b^t = a)$，故$a = b^t = (a^m)^t = a^{mt}$，由消去律，$a^{mt-1} = e$ ∵ a是无限阶元 $\therefore mt - 1 = 0 \Rightarrow (m = t = 1) \vee (m = t = -1)$，故有$b = a$或者$b = a^{-1}$

有限循环群的生成元

- **命题：**设有限群$G=\langle a\rangle$，且$|a|=n$，则对任意不大于n的正整数r，$\boldsymbol{G=\langle a^r\rangle \Leftrightarrow \gcd(n,r)=1}$
  - “$\Leftarrow$”：设$\gcd(n,r)=1$，则$(\exists u,v\in\mathbb{Z})(ur+vn=1)$，因此$a=a^{ur+vn}=(a^r)^u(a^n)^v=(a^r)^u$。故而$G$中任意元素$a^k$可表为$(a^r)^{uk}$，故有$G=\langle a^r\rangle$；
  - “$\Rightarrow$”：设a^r是G的生成元，令$\gcd(n,r)=d$且$r=dt$，则$(a^n)^t=(a^n)^{r/d}=(a^r)^{n/d}=e$，故$|a^r|\,|(n/d)$，但$|a^r|=n$故$n|\frac{n}{d}\Rightarrow d=1$，故有$\gcd(n,r)=1$即$n$与$r$互质

有限循环群的生成元（续）



- n阶循环群G的生成元的个数恰好等于不大于n且与n互质的正整数的个数，即Euler函数$\varphi(n)$，其生成元集为：

$$\{i \mid 0 < i \leq n \wedge \gcd(i,n) = 1\}$$

有限循环群的生成元（续）

例（1）设 $G=\{e,a,\ldots,a^{11}\}$是 12 阶循环群，则$\varphi(12)=4$. 小于或等于 12 且与 12 互素的数是 1, 5, 7, 11，由定理 11.19 可知 a，a^5，a^7 和 a^{11} 是 G 的生成元.

(2) 设 $G=\langle Z_9,\oplus\rangle$是模 9 的整数加群，则$\varphi(9)=6$. 小于或等于 9 且与 9 互素的数是 1, 2, 4, 5, 7, 8. 根据定理 11.19，G 的生成元是 1, 2, 4, 5, 7 和 8.

(3) 设 $G=3Z=\{3z \mid z \in Z\}$,G 上的运算是普通加法. 那么 G 只有两个生成元：3 和−3.

循环群的子群

- 命题：设$G=\langle a\rangle$为循环群

(1) G的子群为循环群

(2) 若$|a|=\infty$，则G的子群除$\{e\}$外皆为无限循环群

证:

(1) 令$(H,\ *)\leqslant(G,\ *)$,从而$H\subseteq\langle a\rangle$,若$H=\{e\}$ 自然成立

否则取a^m为H中最小正方幂元.下证$H=\langle a^m\rangle$ 只需证$H\subseteq\langle a^m\rangle$,任取$h\in H\subseteq\langle a\rangle$,故$h=a^n$。

令$n=qm+r,\ 0\leq r<m$,从而$h=a^n=a^{qm+r}=(a^m)^q a^r$,从而$a^r=h(a^m)^{-q}\in H$，故由$m$的最小性得$r=0$，从而$h=(a^m)^q\in\langle a^m\rangle$，因此$H$为循环群。

(2) 设$H\leqslant G$，由(1)得$H=\langle a^m\rangle$，若$H\neq\{e\}$则$m\neq 0$,从而若$|H|$有穷则$|a^m|$有穷与$|a|$无穷矛盾。

循环群的子群（续）

- 命题：对n的每个因子d，n阶循环群G中恰有一个d阶子群
- 证明：
  - 令$H=\langle a^{n/d}\rangle$，显然H是G的d阶子群
  - 若令$H_1=\langle a^m\rangle$亦为d阶子群，则$(a^m)^d=a^{md}=e$，故有$n|md$，即$\frac{n}{d}|m$，因此$a^m=\left(a^{n/d}\right)^k\in H$，即$H_1\subseteq H$，但$H_1\approx H$，故有$H_1=H$

循环群的子群（续）

$G=Z_{12}$ 是 12 阶循环群. 12 的正因子是 1,2,3,4,6 和 12，因此 G 的子群是:

1 阶子群　　$\langle 12\rangle=\langle 0\rangle=\{0\}$

2 阶子群　　$\langle 6\rangle=\{0,6\}$

3 阶子群　　$\langle 4\rangle=\{0,4,8\}$

4 阶子群　　$\langle 3\rangle=\{0,3,6,9\}$

6 阶子群　　$\langle 2\rangle=\{0,2,4,6,8,10\}$

12 阶子群　　$\langle 1\rangle=Z_{12}$

群同构与同构映射

- 定义（群同构）：群$\langle G_1,\circ\rangle$与$\langle G_2,*\rangle$同构($G_1 \cong G_2$)当且仅当存在双射函数$f: G_1 \to G_2$，满足：

$$\forall x, y \in G_1,\ f(x \circ y) = f(x) * f(y)$$

- 例：

正实数乘群$\langle \mathbb{R}^+,\cdot\rangle$和实数加群$\langle \mathbb{R},+\rangle$，同构映射

$f: \mathbb{R}^+ \to \mathbb{R}: f(x) = \ln x$

群同构与同构映射（续）

- 任意两个三阶群同构

$1 \to a \quad 2 \to b \quad 3 \to c$

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

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

群同构与同构映射（续）

- 2个不同构的四阶群

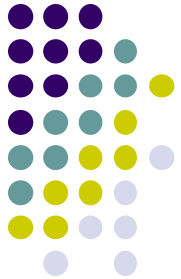
	1	2	3	4
1	1	2	3	4
2	2	3	4	1
3	3	4	1	2
4	4	1	2	3

四元循环群

	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	1	2
4	4	3	2	1

Klein四元群

同态与同态映射



- 定义（群同态）：群$\langle G_1,\circ\rangle$与$\langle G_2,*\rangle$同态$(G_1 \sim G_2)$当且仅当存在函数$f: G_1 \to G_2$，满足：

$$\forall x, y \in G_1,\ f(x \circ y) = f(x) * f(y)$$

- 如果上述映射是满射，则称为满同态；如映射是单射，则称为单同态；若$G_1 = G_2$，则称φ为自同态

同态与同态映射（续）

- 命题：设f为从群$\langle G,*\rangle$到群$\langle H,\circ\rangle$的同态，则

(1) $\boldsymbol{f(e_G)=e_H}$；

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

证明：(1) $\because f(e_G)=f(e_Ge_G)=f(e_G)f(e_G)$

$\therefore f(e_G)=f(e_G)(f(e_G))^{-1}=e_H$

(2) $\because f(a^{-1})f(a)=f(a^{-1}a)=f(e_G)=e_H$

$f(a)f(a^{-1})=f(aa^{-1})=f(e_G)=e_H$

$\therefore f(a^{-1})=(f(a))^{-1}$

同态与同态映射（续）

- 例：整数加系统$\langle \mathbb{Z}, + \rangle$与模3剩余加系统$\langle \mathbb{Z}_3, \oplus_3 \rangle$同态，同态映射为

$$f: \mathbb{Z} \to \mathbb{Z}_3，\ f(3k + r) = r，\ k \in \mathbb{Z}$$

该态射亦为满同态

- 趣味问题：由$1, 2, \cdots, 1000$这一千个自然数按照任意的组合进行加减，能否得到1001？

同态与同态映射（续）

- 趣味问题：由$1,2,\cdots,1000$这一千个自然数按照任意的组合进行加减，能否得到1001？
- 定义系统（奇偶加群）：$\langle\{e,o\},*\rangle$，运算表如下：

$*$	e	o
e	e	o
o	o	e

则 $f:\mathbb{Z}\to\{e,o\}$

$$f(x)=\begin{cases}e & x\text{是偶数}\\ o & x\text{是奇数}\end{cases}$$

是从$(\mathbb{Z},+)$到$(\{e,o\},*)$的满同态映射

无限循环群的同构群

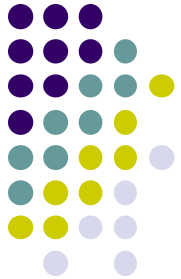
- 定理：设$\langle G,*\rangle$为无限循环群，则$\langle \boldsymbol{G},*\rangle \cong \langle \mathbb{Z},+\rangle$
- 证明：$|a|=\infty$，令$f:\mathbb{Z}\to G$如下：$f(n)=a^n$，

$\because f(n+m)=a^{n+m}=a^n*a^m=f(n)*f(m)\therefore f$为同态；又$\because f(n)=f(m)\Rightarrow a^n=a^m\Rightarrow a^{|n-m|}=e\Rightarrow |n-m|=0\Rightarrow n=m\therefore f$为1-1，onto易见，从而$\langle G,*\rangle \cong \langle \mathbb{Z},+\rangle$

有限循环群的同构群

- 定理：设$\langle G,*\rangle$为有限循环群，则$\langle \boldsymbol{G},*\rangle \cong \langle \mathbb{Z}_{\boldsymbol{n}},\oplus_{\boldsymbol{n}}\rangle$
- 证明：$|a|=n>0$从而$G=\{a^0,a^1,\cdots,a^{n-1}\}$，令$f:\mathbb{Z}_n\to G$如下：$f(i)=a^i(i=0,1,\cdots,n-1)$，由于$f(i\oplus_n j)=a^{i\oplus_n j}=a^i*a^j=f(i)*f(j)$，故$f$为同态。又由于$f(i)=f(j)\Rightarrow a^i=a^j\Rightarrow a^{|i-j|}=e\Rightarrow n||i-j|\Rightarrow i\equiv j(\mathrm{mod}\,n)\Rightarrow i=j$，故$f$为单射，$f$的满射性易见，因此$\langle G,*\rangle\cong\langle \mathbb{Z}_n,\oplus_n\rangle$

循环群的同构群



- 定理：设$\langle G,* \rangle$为无限循环群，则$\langle \boldsymbol{G},* \rangle \cong \langle \mathbb{Z},+ \rangle$
- 定理：设$\langle G,* \rangle$为有限循环群，则$\langle \boldsymbol{G},* \rangle \cong \langle \mathbb{Z}_{\boldsymbol{n}},\oplus_{\boldsymbol{n}} \rangle$

推论：循环群皆为阿贝尔群

群的直积

- 给定两个群: $(S, \circ)$, $(T, *)$, 定义笛卡儿乘积$S \times T$上的运算$\otimes$如下：

  $\langle s_1, t_1 \rangle \otimes \langle s_2, t_2 \rangle = \langle s_1 \circ s_2, t_1 * t_2 \rangle$

- $(S \times T, \otimes)$是群
  - 结合律： $\langle (r_1 \circ s_1) \circ t_1, (r_2 * s_2) * t_2 \rangle$

    $= \langle r_1 \circ (s_1 \circ t_1), r_2 * (s_2 * t_2) \rangle$
  - 单位元素：$\langle 1_S, 1_T \rangle$
  - 逆元素：$\langle s, t \rangle$ 的逆元素是 $\langle s^{-1}, t^{-1} \rangle$
    - (其中： $s, s^{-1} \in S$, $t, t^{-1} \in T$)

循环群的直积

- $C_m \times C_n \cong C_{mn}$ *iff* m与n互质。 其中C_k表示k阶循环群。
  - ⇐若m与n互质，只需证明$C_m \times C_n$含有阶为mn的元素。
    - $(a,b)^{mn} = e$, 其中a,b分别是C_m和C_n的生成元素。
    - 若$(a,b)^k = e$, k必是m,n的公倍数，因m与n互质，故k是mn的倍数。所以，(a,b)的阶是mn。
  - ⇒若$C_m \times C_n \cong C_{mn}$，则$C_m \times C_n$是循环群，设其生成元是(s,t), 则(s,t)的阶是mn, 若gcd(m,n)=k>1, 则$(s,t)^{mn/k} = e$, 这与(s,t)的阶是mn矛盾。

注意：$s^m = e_1$, $t^n = e_2$,

欧拉函数(phi)

- 如果***m***与***n***互质，则 φ(***m***)φ(***n***) =φ(***mn***).

$$
\begin{aligned}
\varphi(n) &= \varphi(p_1^{k_1})\varphi(p_2^{k_2})\cdots\varphi(p_r^{k_r}) \\
&= p_1^{k_1}\left(1-\frac{1}{p_1}\right)p_2^{k_2}\left(1-\frac{1}{p_2}\right)\cdots p_r^{k_r}\left(1-\frac{1}{p_r}\right) \\
&= p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right) \\
&= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right).
\end{aligned}
$$

$$
\varphi(n) = n\prod_{p|n}\left(1-\frac{1}{p}\right),
$$

欧拉函数(phi)

- C_n中元素按其阶分类，*d*阶元素共有φ(*d*)个，*d*|*n*.

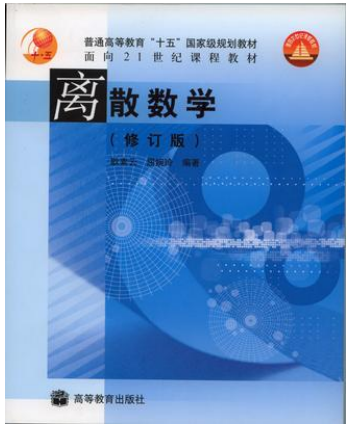
$$\sum_{d|n} \varphi(d) = n,$$

- (Euler定理）若正整数*a*与*n*互质，则

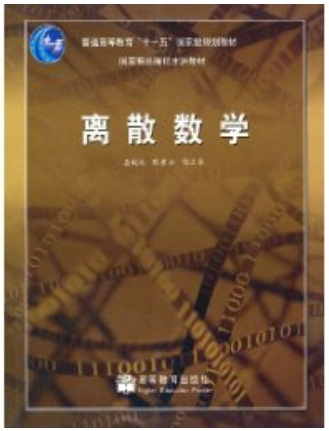
$$a^{\varphi(n)} \equiv 1 \mod n.$$

小于*n*且与*n*互质的正整数及乘法（模*n*）构成一个群

作业



- p. 231
  - 30—35



- pp. 204
  - 25—28