循环群与群同构

回顾

- 问题1：什么叫做群的子群，如何判别之?
  - 非空子集 + 封闭、结合律、单位元、逆元
  - 判定：根据定义或三个判定定理
- 问题2：子群一定存在么，若存在则满足什么性质?
  - 一定存在平凡子群
  - 子群H的所有陪集构成母群G的一个划分
  - 拉格朗日定理及其推论：有限群的子群阶是母群阶的因子、有限质数阶群没有非平凡子群、有限质数阶群一定是循环群

本节提要

- 问题1：什么是循环群?
- 问题2：循环群的子群是否存在、如何构造?
- 问题3：循环群是否存在统一的规律性?

循环群与生成元

- **定义（循环群）：**

设$\langle G,*\rangle$为循环群（cyclic group）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$a^0$为幺
- **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$a^0$为幺

例

- **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

例

- 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

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

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

例

- **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$G=\{(a^{-1})^p|p\in\mathbb{Z}\}$，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

- $\because$ 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，$a^{mt-1}=e$ $\because$ 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：

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

例

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.

本节提要

- 问题1：什么是循环群?
  - 可通过某个元素（生成元）生成所有元素
  - 无限循环群有两个生成元，有限循环群有$\Phi(n)$个生成元
- 问题2：循环群的子群是否存在、如何构造?
- 问题3：循环群是否存在统一的规律性?

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$H_1 = H$

例

$G=Z_{12}$ 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 $\langle 1\rangle=Z_{12}$

本节提要

- 问题1：什么是循环群?
  - 看通过某个元素（生成元）生成所有元素
  - 无限循环群有两个生成元，有限循环群有$\Phi(n)$个生成元
- 问题2：循环群的子群是否存在、如何构造?
  - 对于n阶循环以及n的因子d，恰有一个d阶子群，为$<a^{n/d}>$
- 问题3：循环群是否存在统一的规律性?

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：

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

- 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

群同态与同态映射（续）

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

（1） $f(e_G)=e_H$；

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

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

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

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

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

本节小结

- 问题1：什么是循环群?
  - 通过某个元素（生成元）生成所有元素
  - 无限循环群有两个生成元，有限循环群有Φ(n)个生成元
- 问题2：循环群的子群是否存在、如何构造?
  - 对于n阶循环以及n的因子d，恰有一个d阶子群，为$<a^{n/d}>$
- 问题3：循环群是否存在统一的规律性?
  - 无限循环群皆与整数加群同构，n阶有限群循环群皆与模n加法群同构

例：群的直积

- 给定两个群: (S, ∘), (T,*), 定义笛卡儿乘积S×T上的运算⊗如下：

  $<s_1,t_1> \otimes <s_2,t_2> = <s_1 \circ s_2,\ t_1 * t_2>$

- 证明：(S×T, ⊗)是群
  - 结合律：$<(s_1 \circ s_2) \circ s_3,\ (t_1 * t_2) * t_3>$

    $= <s_1 \circ (s_2 \circ s_3),\ t_1 * (t_2 * t_3)>$
  - 单位元素：$<1_S,\ 1_T>$
  - 逆元素：$<s, t>$ 的逆元素是 $<s^{-1}, t^{-1}>$
    - (其中： $s, s^{-1} \in S$, $t, t^{-1} \in T$)

例：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：$s^m=e_1$, $t^n=e_2$,

欧拉函数和欧拉定理

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

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

  - n的每个因子d，恰有一个d阶子群
  - d阶子群生成元个数是$\varphi(d)$，每个生成元都是d阶元素

例

$G=Z_{12}$ 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 $\langle 1\rangle=Z_{12}$

欧拉函数和欧拉定理

- **(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（模*n*）乘法构成一个群

例如，n=12，群元素{1,5,7,11}，该群的单位元是1。假设某个满足条件(a,n)=1的元素a的阶是k，即 $a^k \equiv 1$ (mod *n*)；<a>是一个子群，由拉格朗日定理有φ(n)=k*M，于是有a^φ(n)= a^{kM} = (a^k)^M = 1^M =1　mod n

作业

- 见课程主页