循环群与群同构

赵建华 陶先平

内容

- 同构与同态
- 循环群与生成元
- 循环群的子群
- 无限循环群与整数加群同构
- 有限循环群与相应的剩余加群同构

群同构与同构映射

- 群$(G_1, \ )$与$(G_2,*)$同构 $(G_1 \cong G_2)$ 当且仅当：

  存在双射(同构映射)f: $G_1 \to G_2$, 满足：

  对任意$x,y \in G_1$, $f(x \quad y) = f(x) * f(y)$

  "先(G_1中的)运算后映射 等于先映射后运算(G_2中的)"

- 例： 正实数乘群$(R^+,\bullet)$和实数加群$(R,+)$

  同构映射f: $R^+ \to R$: $f(x)=\ln x$

  注意：可能有多个同构映射，如$f(x)=\lg x$也是。

同构关系是等价关系

- 自反：对任意群(G,), G≅G
  - 恒等映射 $f(x)=x$ 是同构映射
- 对称：对任意群G_1, G_2, 若$G_1 \cong G_2$, 则$G_2 \cong G_1$
  - 设从G_1到G_2的同构映射为f, 则从G_2到G_1的同构映射是f^{-1}
- 传递：对任意群G_1, G_2, G_3, 若$G_1 \cong G_2$, 且$G_2 \cong G_3$，则$G_1 \cong G_3$,
  - 设从G_1到G_2的同构映射为f, 从G_2到G_3的同构映射为g, 则设从G_1到G_3的同构映射$f \quad g$

3阶群的唯一性

- 任意两个三阶群同构

1→a 2→b 3→c

∘	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

*	a	b	c
a	a	b	c
b	b	?	a

设a是单位元，cb=a必然成立，否则

- 如果cb=b，则$c=cbb^{-1}=bb^{-1}=a$；
- 如果cb=c，则$b=c^{-1}cb=c^{-1}c=a$

类似地，bc=a必然成立。

由ab=b, cb=a可知bb必然是c。

由ac=c, bc=a可知cc必然是b。

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

- 系统(G_1，)与(G_2,*)同态， 记做 ($G_1 \sim G_2$)当且仅当：

  存在函数f: $G_1 \to G_2$, 满足：

  对任意$x, y \in G_1$, $f(x \quad y) = f(x) * f(y)$

  注意：同构要求一一映射
- 如果上述f是满射，则称为满同态
- 同构是同态的特例。
- 例：整数加系统(Z,+)和对3剩余加系统(Z_3,$+_3$)
  - 同态映射：f: $Z \to Z_3$, $f(3k+r)=r$，这是满同态

一个满同态的例子

定义系统： $(\{e, o\},*)$

运算“*”的运算表如下：

$*$	e	o
e	e	o
o	o	e

则 $f: Z \rightarrow \{e,o\}$:

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

是从(Z,+)到$(\{e, o\}, *)$的满同态映射。

这可以用来证明：1,2,...,1000这1000个自然数，按照任意的组合实施加/减，得到的结果不可能是1001。

如何证明两个群不同构

- 一定要证明：$(G_1,)$到$(G_2,*)$的任何映射都不可能是同构映射!
  - 例：非零有理数乘群$(Q-\{0\},\bullet)$和有理数加群$(Q,+)$不同构。

    假设存在$f: Q-\{0\}\to Q$,是同构映射,

    注意：必有$f(1)=0$ (否则, $f(1\bullet x)\neq f(1)+ f(x)$)

    而$f(-1)+f(-1)= f((-1)\bullet(-1))=f(1)=0$

    因此：$f(-1)=f(1)$，f 不是一对一的。

群中元素的阶

- 设a是群(G,*)中任一元素。正整数r是a的**阶**(记为|a|=r)：
  - $a^r = e$ (e是群G的单位元素)
  - 对任意正整数k, 若$a^k = e$, 则$k \geq r$

如果这样的k不存在，则称a有无限阶

元素阶的性质

- 设a的阶是r, 对任意正整数k, $a^k=e$ 当且仅当 r能整除k
  - $\Rightarrow$ 令 $k = mr+i$ (m, i均为正整数， 且$0 \le i \le r-1$), 则$a^{mr+i} = (a^r)^m * a^i = a^i = e$ 因为$i<r$, i只能是0, 即$k = mr$
  - $\Leftarrow$ 令$k = mr$， 则$a^k = a^{mr} = (a^r)^m = e^m = e$

- 任何元素与其逆元素有相同的阶
  - 设$|a|=r$, $(a^{-1})^r=(a^r)^{-1}=e$, 因此$(|a^{-1}|)|r$ 。
  - 令$|a^{-1}|=t$, $a^t=((a^{-1})^{-1})^t = ((a^{-1})^t)^{-1} = e$， 因此$r|(|a^{-1}|)$,
  - 所以$|a^{-1}|=r$

循环群与生成元素

- 定义
  - 设G是群，若存在$a \in G$，使得$G=\{a^k | k \in Z\}$，则G称为***循环群***。
  - 记法：<a>。
  - a 称为 ***生成元***。

循环群的阶与生成元素的阶

- 有限(n阶)循环群:
  - 生成元a的阶为n,
  - $G=\{a^0,a^1,a^2,\ldots,a^{n-1}\}$, 其中$a^0$是单位元素。

- 无限循环群:
  - 生成元素a为无限阶元,
  - $G=\{a^0,a^{\pm1},a^{\pm2},\ldots\}$

循环群的例子

- 无限循环群：
  - 整数加群 (Z,+): 1是生成元素，对任意整数i, $i = 1^i$。

  1. 这里“乘幂”是对加法而言的

  2. $i<0$时， 1^i是负数；

  3. -1同样是生成元，如： $5=(-1)^{-5}$。

- 有限循环群：
  - 剩余加群 $(Z_6, +_6)$: [1]是生成元素。
  - 注意：[5]也是生成元：
    - $[5]^0=[0]$； $[5]^1=[5]$； $[5]^2=[4]$；
    - $[5]^3=[3]$； $[5]^4=[2]$； $[5]^5=[1]$；

无限循环群与整数加群同构

- 建立$G=\{a^0,a^{\pm1},a^{\pm2},\ldots\}$与$Z=\{0,\pm1,\pm2,\pm3,\ldots\}$之间的一一对应函数：

  $f:G\to Z$, 对任意$a^k\in G$, $f(a^k)=k$ (k是整数)

  - 只要$a^k=a^h$, 必有$k=h$, 否则$a^{k-h}=e$, a有有限阶 $k-h$(不妨设$k>h$)。因此f是函数。
  - 显然是双射
  - $f(a^k\ \ a^h)=f(a^{k+h})=k+h=f(a^k)+f(a^h)$

n阶循环群与n阶剩余加群同构

- 建立$G=\{a^0,a^1,a^2,\ldots,a^{n-1}\}$到$Z_n=\{0,1,2,\ldots, n-1\}$的一一对应的函数：

  f:G→Z, 对任意$a^k\in G$, $f(a^k)=[k]$ (k是整数)

  – 注意：只要$a^k=a^h$, 必有$[k]=[h]$, 否则，k,h除以n余数不同，即$k-h=qn+r$(q是整数，$r\in\{1,2,\ldots,n-1\}$),
  – 但$a^{k-h}=e$ (不妨设$k>h$)，即$a^{k-h}=a^{qn+r}=a^r=e$，与a的阶是n矛盾。所以f是函数。
  – 显然是双射
  – $f(a^k\ \ a^h)=f(a^{k+h})=[k+_nh]=[k]+_n[h]=f(a^k)+_n f(a^h)$

无限循环群的生成元素

- 若a是无限循环群的生成元素，则a^{-1}(a的逆元素)也是。
  - $a^k = (a^{-1})^{-k}$。
- 无限循环群只有两个生成元
  - 设G=<a>。*若b也是G的生成元*。则存在整数*m*和*t*, 满足： $a^m=b$, $b^t=a$, $\therefore a=b^t=(a^m)^t=a^{mt}$, $\therefore a^{mt-1}=e$, a是无限阶元素， $\therefore mt-1=0$, $\therefore m=t=1$或者$m=t=-1$, $\therefore$ *$b=a$或者$b=a^{-1}$* 。

有限循环群的生成元

- 设G=<a>，且|a|=n，则对任意不大于n的正整数*r*, gcd(n,r)=1 ***iff.*** a^r是G的生成元。
  - $\Rightarrow$ 设gcd(n,r)=1, 则存在整数u,v，使得：ur+vn=1, $\therefore a=a^{ur+vn}=(a^r)^u(a^n)^v=(a^r)^u$。则：G中任意元素$a^k$可以表示为$(a^r)^{uk}$。
  - $\Leftarrow$ 设a^r是G的生成元，令gcd(n,r)=d且r=dt, 则$(a^r)^{n/d}=(a^n)^t=e$, $\therefore |a^r| | (n/d)$, 但$|a^r|=n$, $\therefore d=1$

*n*阶循环群的生成元素的阶必定是*n*

有限循环群的生成元

- 有限循环群不同的生成元素的个数

  n阶循环群G的生成元的个数恰好等于不大于n的与n互质的正整数的个数。

  – 这个量是n的函数：欧拉函数$\varphi(n)$

循环群的子群

- 循环群的子群*仍然*是循环群
  - *子群H中最小正方幂元即为H的生成元。*
  - 设最小正方幂元素为a^m, 证明H=<a^m>
    - 任给$a^t \in H$, 令$t=qm+r$, 其中q为整数，$0 \le r \le m-1$。
    - 由子群的封闭性，$a^{qm} \in H$, $\therefore a^{-qm} \in H$, $a^{t-qm}=a^r \in H$。
    - 但H中最小正方幂元素为a^m, $\therefore r$只能是0。
    - $\therefore\ a^t = a^{qm} = (a^m)^q$

循环群的子群

无限循环群的生成元必是无限阶的

- 无限循环群只有唯一的有限子群：{e}
  - 假设G有t阶有限子群H, 且H≠{e}, 则设H的最小正方幂元为a^m, 则$a^{mt}=e$, 矛盾。
- N阶循环群中，对n的每一个整除因子d，n阶循环群G恰好有一个d阶子群
  - 有：以$a^{n/d}$为生成元可构成一个d阶子群，设它为H。
  - 恰有一个：如果$H_1=\langle a^m \rangle$也是d阶子群，则$a^{md}=e$, 所以kn=md, 也就是m=k(n/d), 因此： $a^m=(a^{n/d})^k \in H$, 即$H_1 \subseteq H$, 但H_1与H等势，所以 $H_1=H$

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：

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

- (S×T, ⊗) 是群
  - 结合律： $\langle (r_1 \quad s_1) \quad t_1, (r_2*s_2)*t_2\rangle$

    $= \langle r_1 \quad (s_1 \quad t_1), r_2*(s_2*t_2)\rangle$
  - 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

- $C_m \times C_n \cong C_{mn}$当且仅当m,n互质。其中$C_k$表示k阶循环群。
  - 若m,n互质，要证明$C_m \times C_n \cong C_{mn}$只需证明$C_m \times C_n$是循环群。这只需证明$C_m \times C_n$含有阶为mn的元素。
    - $(a,b)^{mn} = (e_1,e_2)$, 其中a,b, e_1,e_2分别是C_m和C_n的生成元素和单位元。
    - 若$(a,b)^k = (e_1,e_2)$, k必是m,n的公倍数，如果k<mn, 则m,n有公约数mn/k>1, 这与m,n互质矛盾。
    - 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$(s,t)^{mn/k} = (e_1,e_2)$, 这与(s,t)的阶是mn矛盾。

作业

- p.204-
  - 26-28