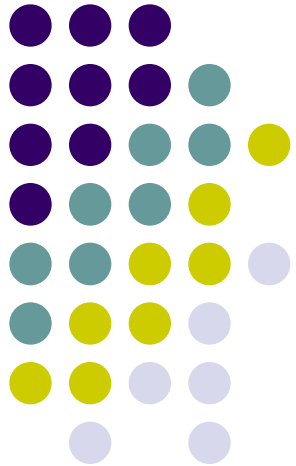
循环群与群同构

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

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

  存在*一一对应*的函数(同构映射)f: $G_1 \to G_2$, 满足：

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

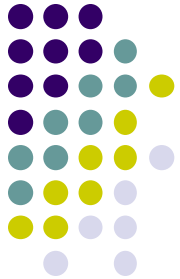
  “先(G_1中的)运算后映射 等于先映射后运算(G_2中的)”

- 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$(G,\circ)$, $G\cong G$
  - 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$f\circ g$

3阶群的唯一性

- 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

2个四阶群

	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$(G_1, \circ)$与$(G_2, *)$*同态* $(G_1 \sim G_2)$当且仅当：

  存在函数f: $G_1 \to G_2$, 满足：

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

  注意：同态保持单位元与逆元: $f(e_1) = e_2$，$f(x^{-1}) = f(x)^{-1}$

- 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 $f: Z \to \{e,o\}$:

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

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

- 需要证明： $(G_1,\circ)$到$(G_2,*)$的*任何同态*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。

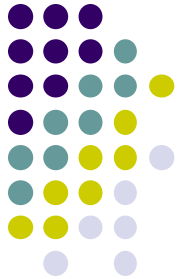
  假设存在$f: Q-\{0\}\to Q$,是同构映射，

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

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

  因此： $f(-1)=0=f(1)$，f 不是一对一的。

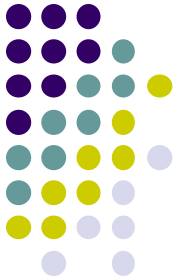
群中元素的阶



- 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, $a^k=e \Leftrightarrow$ r能整除k
  - $\Rightarrow$ 令 $k = mr+i$ (m, i均为非负整数，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$|a^{-1}|$整除r，即$|a^{-1}|$整除$|a|$。
  - 同理可得， $|a|$整除$|a^{-1}|$。

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，
  - $G=\{a^0, a^{\pm1}, a^{\pm2}, \ldots\}$

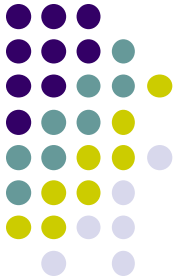
循环群的例子

- 无限循环群
  - 整数加群 $(Z,+)$: 1是生成元素，对任意整数i, $i = 1^i$。
  - 注意: (1) 这里“乘幂”是对加法而言的;

    (2) i <0时， 1^i是负数;

    (3) –1同样是生成元素，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：
    - $[5]^0=[0]$, $[5]^1=[5]$, $[5]^2=[4]$, $[5]^3=[3]$, $[5]^4=[2]$, $[5]^5=[1]$。

无限循环群的生成元素



- 若a是无限循环群的生成元，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：$a^m=b$, $b^t=a$。
  - 所以$a=b^t=(a^m)^t=a^{mt}$, 从而$a^{mt-1}=e$。
  - a是无限阶元素，得$mt-1=0$, 从而$m=t=1$或者$m=t=-1$。
  - 所以$b=a$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 ⇔ a^r是G的生成元。
  - ⇒ 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$(a^r)^{uk}$。
  - ⇐ 设a^r是G的生成元，令gcd(n,r)=d且r=dt, 则$(a^r)^{n/d}=(a^n)^t=e$, $\therefore |a^r|$整除(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。
  - 这是n的函数, 即欧拉函数φ(n)
    - 备注：φ(1)=1

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) = p^k\left(1 - \frac{1}{p}\right).$$

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，$a^{qm} \in H$, $\therefore a^r=a^{t-qm} \in H$。
    - 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$H_1=<a^m>$也是d阶子群，则$a^{md}=e$, 所以n|md, 也就是n/d|m, 因此： $a^m=(a^{n/d})^k \in H$, 即$H_1 \subseteq H$, 又H_1与H等势（d阶），所以 $H_1=H$

注意：d是n的整除因子

无限循环群与整数加群同构

- 定义$G=\{a^0, a^{\pm1}, a^{\pm2}, \ldots\}$与$Z=\{0, \pm1, \pm2, \ldots\}$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是有限阶的，矛盾。因此f是函数。
  - 易证f是双射
  - $f(a^k\circ a^h)=f(a^{k+h})=k+h=f(a^k)+f(a^h)$

n阶循环群与n阶剩余加群同构

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

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

  - 注意：只要$a^k=a^h$, 必有$[k]=[h]$, 否则，不妨设$k>h$，$k-h=qn+r$(q是整数，$r\in\{1,2,\ldots,n-1\}$), 则$e=a^{k-h}=a^{qn+r}=a^r$, 与a的阶是n矛盾。所以f是函数。
  - 易证f是双射
  - $f(a^k\circ a^h)=f(a^{k+h})=[k+h]_n=[k]_n+[h]_n=f(a^k)+f(a^h)$

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

- $C_m \times C_n \cong C_{mn}$ ⇔m与n互质。 其中C_k表示k阶循环群。
  - ⇐若m与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。
    - $(a,b)^{mn} = e$, 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(***mn***) = φ(***m***)φ(***n***).

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

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

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*.

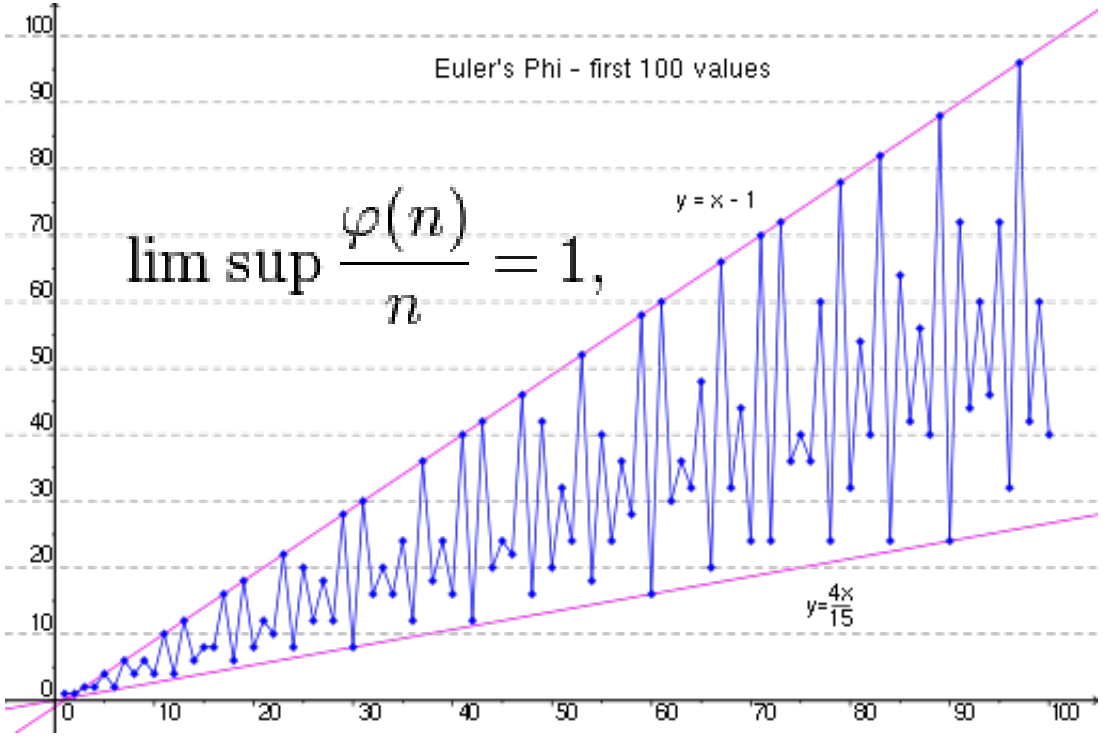
$$\sum_{d|n} \varphi(d) = n,$$

- (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

欧拉函数(phi)



$$\limsup \frac{\varphi(n)}{n} = 1,$$

$$\liminf \frac{\varphi(n)}{n} \log\log n = e^{-\gamma}.$$

欧拉常数 γ = 0.577215665...

作业

- **pp. 204**
  - **25—28**