离散数学

大连理工大学软件学院

陈志奎 博士、教授、博士生导师

办公室： 综合楼405，Tel： 62274392
实验室：综合楼一楼

Mobile: 13478461921
Email: zkchen@dlut.edu.cn
zkchen00@hotmail.com
QQ： 1062258606

离散数学

第七章 群环域

回 顾

- 群的定义
- 群的性质
- 子群的定义
- 子群的判定定理

子群的性质

　生成子群

　中心C

　子群的交

　子群格

主要内容

- 子群的陪集，拉格朗日定理
- 循环群定义及性质
  - 生成元、n阶循环群、无限循环群
- 置换群定义及性质
- 群的同态与同构
  - 群同态映射：单一同态、满同态、群同构映射
- 环的概念与性质
- 域的概念
- 应用：群与网络安全

7.3.4 子群的陪集分解：陪集

- 定义7.17 令$<H, \odot>$是群$<G, \odot>$的子群且$a \in G$，则把下面集合：

$$a \odot H = \{a \odot h \mid h \in H\}$$

称为由元素**a**所确定的群**<G，⊙>**中的**H**的左陪集，或简称为左陪集，并简记**aH**。此外，称**a**是左陪集**aH**的代表元素。

类似地可定义由*a*所确定群<*G*，⊙>中的*H*的右陪集*Ha*。

显然，若<*G*，⊙>是Abel群，并且<*H*，⊙>是其子群，则$aH = Ha$，即任意元素的左陪集等于其右陪集。

7.3.4 子群的陪集分解：陪集

- 定义7.18 给定群<*G*，⊙>，子群<*H*，⊙>的左陪集关系，记作C_H，其定义为：

$$C_H: \;= \{\langle a, b\rangle \mid a,\ b \in G \wedge b^{-1} \odot a \in H\}$$

由此定义不难得到：

$$aC_Hb \iff a,\ b \in G \wedge b^{-1} \odot a \in H$$

可以指出，子群<*H*，⊙>的左陪集关系是群<*G*，⊙>中的一种等价关系。

(证明在下一页)

- 证明：由于$a^{-1} \odot a = e \in H$，则aC_Ha，即有自反性。

若aC_Hb，则$b^{-1} \odot a \in H$，

于是$a^{-1} \odot b = \left((a^{-1} \odot b)^{-1}\right)^{-1} = (b^{-1} \odot a)^{-1} \in H$，故$bC_Ha$，因而满足对称性。

若aC_Hb且bC_Hc，则$b^{-1} \odot a \in H$和 $c^{-1} \odot b \in H$，所以

$$c^{-1} \odot a = (c^{-1} \odot b) \odot (b^{-1} \odot a) \in H$$

故有aC_Hc，因而满足传递性。

显然，左陪集关系能把集合G划分成等价类。

若$a \in G$，则

$$[a] = \{b \mid bC_H a\} = \{b \mid \langle b, a\rangle \in C_H\}$$
$$= \{b \mid a^{-1} \odot b \in H\} = \{b \mid a^{-1} \odot b = h, h \in H\}$$
$$= \{b \mid b = a \odot h，h \in H\}$$
$$= \{a \odot h \mid h \in H\} = aH$$

其中$h = a^{-1} \odot b$。

可见，由元素a所确定群$< G，\odot >$中的H的左陪集aH与子群$< H，\odot >$的左陪集关系C_H所确定的等价类$[a]_{CH}$是完全相同的，即$aH = [a]_{CH}$。

对于右陪集关系可类似地讨论。

7.3.4 子群的陪集分解：陪集

- 例7.24

(1) 设$G = \{e, a, b, c\}$是Klein四元群，$H =< a >$是G的子群.

H所有的右陪集是：

$$He = \{e, a\} = H, \qquad Ha = \{a, e\} = H\ ,$$

$$Hb = \{b, c\}, Hc = \{c, b\}$$

不同的右陪集只有两个，即H和$\{b, c\}$.

7.3.4 子群的陪集分解：陪集

(2) 设$A=\{1,2,3\}$，$f_1, f_2, \ldots, f_6$是A上的双射函数. 其中

$$f_1=\{<1,1>,<2,2>,<3,3>\}，\quad f_2=\{<1,2>,<2,1>,<3,3>\}$$

$$f_3=\{<1,3>,<2,2>,<3,1>\}，\quad f_4=\{<1,1>,<2,3>,<3,2>\}$$

$$f_5=\{<1,2>,<2,3>,<3,1>\}，\quad f_6=\{<1,3>,<2,1>,<3,2>\}$$

令 $G = \{f_1, f_2, \ldots ,f_6\}$，则$G$ 关于函数的复合运算构成群. 考虑 G 的子群$H=\{f_1, f_2\}$. 做出 H 的全体右陪集如下：

$$Hf_1=\{f_1\circ f_1, f_2\circ f_1\}=H\ ,\ Hf_2=\{f_1\circ f_2, f_2\circ f_2\}=H$$

$$Hf_3=\{f_1\circ f_3, f_2\circ f_3\}=\{f_3, f_5\},\ Hf_5=\{f_1\circ f_5, f_2\circ f_5\}=\{f_5, f_3\}$$

$$Hf_4=\{f_1\circ f_4, f_2\circ f_4\}=\{f_4, f_6\},\ Hf_6=\{f_1\circ f_6, f_2\circ f_6\}=\{f_6, f_4\}$$

结论： $Hf_1=Hf_2$，$Hf_3=Hf_5$，$Hf_4=Hf_6$.

7.3.4 子群的陪集分解：陪集的性质

- **定理7.15** 设H是群G的子群，则

  (1) $He = H$

  (2) $\forall a \in G$ 有$a \in Ha$

- 证明：

  (1) $He = \{ he \mid h \in H \} = \{ h \mid h \in H \} = H$

  (2) 任取 $a \in G$，由$a = ea$ 和 $ea \in Ha$ 得 $a \in Ha$

7.3.4 子群的陪集分解：陪集的性质

- 定理7.16 设H是群G的子群，则$\forall a, b \in G$有

$$a \in Hb \Leftrightarrow ab^{-1} \in H \Leftrightarrow Ha = Hb$$

- 证明： 先证$a \in Hb \Leftrightarrow ab^{-1} \in H$

$$a \in Hb \Leftrightarrow \exists h(h \in H \wedge a = hb)$$

$$\Leftrightarrow \exists h(h \in H \wedge ab^{-1} = h) \Leftrightarrow ab^{-1} \in H$$

再证 $a \in Hb \Leftrightarrow Ha = Hb$.

充分性. 若$Ha = Hb$，由$a \in Ha$ 可知必有 $a \in Hb$.

必要性. 由 $a \in Hb$ 可知存在 $h \in H$ 使得 $a = hb$，即$b = h^{-1}a$

任取 $h_1a \in Ha$，则有

$$h_1a = h_1(hb) = (h_1h)b \in Hb$$

从而得到 $Ha \subseteq Hb$. 反之，任取$h_1b \in Hb$，则有

$$h_1b = h_1(h^{-1}a) = (h_1h^{-1})a \in Ha$$

从而得到$Hb \subseteq Ha$. 综合上述，$Ha = Hb$得证.

7.3.4 子群的陪集分解：陪集的性质

- 定理7.17 设H是群G的子群，在G上定义二元关系R:

$$\forall a,b\in G,\langle a,b\rangle\in R \iff ab^{-1}\in H$$

则 R是G上的等价关系，且$[a]_R$=Ha.

- 证明：先证明R为G上的等价关系.

自反性. 任取$a\in G$，$aa^{-1}=e\in H \iff \langle a,a\rangle\in R$

对称性. 任取$a,b\in G$，则

$$\langle a,b\rangle\in R\Rightarrow ab^{-1}\in H\Rightarrow (ab^{-1})^{-1}\in H\Rightarrow ba^{-1}\in H\Rightarrow \langle b,a\rangle\in R$$

传递性. 任取$a,b,c\in G$，则

$$\langle a,b\rangle\in R\land\langle b,c\rangle\in R \Rightarrow ab^{-1}\in H\land bc^{-1}\in H$$

$$\Rightarrow ac^{-1}\in H \Rightarrow \langle a,c\rangle\in R$$

下面证明：$\forall a\in G$，$[a]_R=Ha$. 任取$b\in G$，

$$b\in[a]_R \iff \langle a,b\rangle\in R \iff ab^{-1}\in H \iff Ha=Hb \iff b\in Ha$$

7.3.4 子群的陪集分解：推论

- 推论 设H是群G的子群, 则

  (1) $\forall a, b \in G$，$Ha = Hb$ 或 $Ha \cap Hb = \varnothing$

  (2) $\cup \{Ha \mid a \in G\} = G$

- 证明：由等价类性质可得.

- 定理7.18 设H是群G的子群，则

$$\forall a \in G，H \approx aH(\text{等势})$$

- 证明：令$f \in (aH)^H$如下:

$f(h) = a \odot h$，其中$h \in H$ 则f是双射。满射是显然的，下面再证它是单射。

假定它不是单射，即$h_1 \neq h_2$，h_1，$h_2 \in H$，$f(h_1) = f(h_2)$，也就是$a \odot h_1 = a \odot h_2$，则根据群的可约律知$h_1 = h_2$，这与$h_1 \neq h_2$矛盾

附：左陪集小结

设G是群，H是G的子群，H 的左陪集，即

$$aH = \{ah \mid h \in H\},\ a \in G$$

关于左陪集有下述性质：

(1) $eH = H$

(2) $\forall a \in G$，$a \in aH$

(3) $\forall a, b \in G$，$a \in bH \Leftrightarrow b^{-1}a \in H \Leftrightarrow aH = bH$

(4) 若在G上定义二元关系R，

$$\forall a, b \in G,\quad \langle a, b \rangle \in R \Leftrightarrow b^{-1}a \in H$$

则R是G上的等价关系，且$[a]_R = aH$.

(5) $\forall a \in G$，$H \approx aH$ (等势)

7.3.5 拉格朗日定理

- **定理7.19(Lagrange)** 如果**G**是一个有限群和**H**是**G**一个的子群，则

$$[\boldsymbol{G}:\boldsymbol{H}] = \frac{|\boldsymbol{G}|}{|\boldsymbol{H}|}$$

其中$|\boldsymbol{G}|$和$|\boldsymbol{H}|$分别是**G**和**H**的阶数。

- 证明： 设$[G:H] = r, a_1, a_2, \ldots, a_r$分别是H 的r个右陪集的代表元素，

$$G = Ha_1 \cup Ha_2 \cup \cdots \cup Ha_r$$

$$|G| = |Ha_1| + |Ha_2| + \ldots + |Ha_r|$$

由$|Ha_i| = |H|$，$i = 1,2, \ldots, r$, 得

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

7.3.5 拉格朗日定理

- 每一个G的子群的阶数（和每一个G内元素的阶数）都必须为$|G|$的因子。

- 若对于每个在G内的a，$aH = Ha$，则H称之为正规子群。每一个指数2的子群皆为正规的：左陪集和右陪集都简单地为此一子群和其补集。

7.3.5 拉格朗日定理

- 例7.25 证明6阶群中必含有3阶元。

- 证明：设G是6阶群，由拉格朗日定理可知G中的元素只能是1阶，2阶3阶或6阶元。

  若G中含有6阶元，设这6阶元为a，则a^2是3阶元。

  若G中不含6阶元，下面证明G中必含有3阶元。若不然，G中只含有1阶和2阶元，即$\forall a \in G$，有$a^2 = e$，可知G是Abel群，取G中的两个不同的2阶元a和b，令$H = \{e，a，b，ab\}$易知H是G的子群，但$|H| = 4$，$|G| = 6$，与拉格朗日定理矛盾。

  综上所述，6阶群中必含有3阶元。

7.3.6 集合的置换

- **定义7.19** 集合的置换：令X是非空有限集合，从X到X的双射函数，称为集合X中的**置换**，并称$|X|$为置换的**阶**。

集合上的所有**置换（双射）**与**复合运算**，构成的代数系统是一个群，称为**对称群**。

由n个元素的集合而构成的所有$n!$个n阶置换的集合S_n与复合置换运算◇构成群$<S_n$，◇$>$，它便是n次$n!$阶对称群。

若$Q \subseteq P_x = S_{|x|}$，则称由$Q$和◇构成的群$<Q$，◇$>$为**置换群**。

集合的置换

- 例7.26 设G是n个字母的对称群， G'={0,1}，+是如下表定义在G'上的运算，易知G'是一个群。f: $G \to G'$定义如下：对于$p \in G$，有

$$f(p)=\begin{cases}0, & p \in A_n\text{（}G\text{中所有偶置换的子群）} \\ 1, & p \notin A_n\end{cases}$$

表

+	0	1
0	0	1
1	1	0

那么f是一个同态。

集合的置换

- 定义7.20 集合X是无限的，令T_x表示所有从集合X到X的变换的集合，具有下列性质：

$$(\forall f)(\forall g)(f,g \in T_x \to f \circ g, g \circ f \in T_x)$$

$$(\forall f)(\forall g)(\forall h)\big(f,g,h \in T_x, \to (f \circ g) \circ h = f \circ (g \circ h)\big)$$

$$(\exists idA)\big(idA \in T_x \wedge (\forall f)(f \in T_x \to idA \circ f = f \circ idA = f)\big)$$

$$(\forall f)\big(f \in T_x \to (\exists f^{-1})(f^{-1} \in T_x \wedge f \circ f^{-1} = f^{-1} \circ f = idA)\big)$$

$\langle T_x, \circ \rangle$构成群，在代数中称为变换群。置换群是变换群的特例。

集合的置换

- 定义7.21 设p是集合$X=\{x_1,x_2,\cdots,x_n\}$上的n阶置换，若$p(x_1)=x_2$，$p(x_2)=x_3$，⋯，$p(x_{n-1})=x_n$，$p(x_n)=x_1$，并且X中其余元素保持不变，则称p为X 上的n 阶轮换，记为$(x_1x_2\cdots x_n)$，若$n=2$，称p为X上的对换。

由轮换的定义可知，轮换中任何元素均可排在首位，他们表示是一个轮换，如$(x_1x_2\cdots x_n)=\left(x_ix_{i+1}\cdots x_j\right)$。

- 例7.27 令$S=\{1,2,3,4,5\}$，S上的5阶置换$p=\binom{12345}{24315}$是S上的3阶轮换（1 2 4）。

7.4 循环群

- **定义7.22** 设$\langle \boldsymbol{G}, \otimes \rangle$是群，若$\exists \boldsymbol{a} \in \boldsymbol{G}$，对$\forall \boldsymbol{x} \in \boldsymbol{G}, \exists \boldsymbol{k} \in \boldsymbol{Z}$,有$\boldsymbol{x} = \boldsymbol{a}^{\boldsymbol{k}}$，则称$\langle \boldsymbol{G}, \otimes \rangle$是**循环群**，记作$\boldsymbol{G} = \langle \boldsymbol{a} \rangle$，称**a** 是群$\langle \boldsymbol{G}, \otimes \rangle$的**生成元**。

- **定义7.23** 若存在$\boldsymbol{a} \in \boldsymbol{G}$，使得$\boldsymbol{G} = \langle \boldsymbol{a} \rangle$，则称**G**是**循环群**，称**a** 为**G**的**生成元**。

7.4.1 循环群

循环群G=<a>根据生成元a的阶可以分为两类：n阶循环群和无限循环群。

设G=<a>是循环群，若a是n阶元，则

$$G=\{a^0=e,a^1,\cdots,a^{n-1}\}$$

那么$|G|=n$，称G为n阶循环群。

若a是无限阶元，则

$$G=\{a^0=e,a^{\pm 1},a^{\pm 2}\cdots\}$$

这时称G为无限循环群。

7.4.1 循环群

- 定理7.20 设$G=\langle a\rangle$是循环群。

  若G是无限循环群，则G只有两个生成元，即a和a^{-1}。

  若G是 n 阶循环群，则G含有$\varphi(n)$个生成元，对与任何小于n且与n互素的自然数r，a^r是G的生成元。

- 定理7.21

  （1）设$G=<a>$是循环群，则G的子群仍是循环群。

  （2）若$G=<a>$是无限循环群，则G的子群除$\{e\}$以外都是无限循环群。

  （3）若$G=<a>$是n阶循环群，则对于n的每个正因子d，G恰好含有一个d阶子群。

7.4.1 循环群

- 例7.28 设G_1是整数加群，G_2是模12加群，求出G_1和G_2的所有子群。

解：G_1的生成元为1和-1，易知$1^m = m$，$m \in N$。所以G_1的子群是mZ，$m \in N$。即

$$\langle 0 \rangle = \{0\} = 0Z$$

$$\langle m \rangle = \{mz | z \in Z\} = mz, m > 0$$

G_2是12阶循环群。

12的正因子是1,2,3,4,6和12，因此G_2的子群是：

<12>=<0>={0}	1阶子群	<6>={0,6}	2阶子群
<4>={0,4,8}	3阶子群	<3>={0,3,6,9}	4阶子群
<2>={0,2,4,6,8,10}	6阶子群	<1>=Z_{12}	12阶子群

7.4.2 置换群

- 定义7.25 设$S=\{1,2,\cdots,n\}$，S上的任何双射函数∂：$S\to S$称为S上的n元置换。
- 定义7.26 设∂，σ是n元置换，∂，σ的复合$\partial^\circ\sigma$也是n元置换，称为∂和σ的乘积，记作$\partial\sigma$。
- 定义7.27 一个置换群是一个群G，其元素是一个给定集M的置换，而其群作用是G中的置换（可以看作是从M到自身的双射）的复合；其关系经常写作(G,M)。注意所有置换的群是对称群；置换群通常是指对称群的一个子群。

7.4.2 置换群

- n个元素的置换群记为S_n；若M是任意有限或无限集合，则所有M的置换组成的对称群通常写作$Sym(M)$。

- 设$S \neq \emptyset$，$|S| < +\infty$，S上的一个一一变换被称为置换。当S上的某些置换关于乘法运算构成群是，就成它为置换群。

- 若$|S| = n$，设$\{n = 1,2，…，n\}$，其置换全体组成的集合一般表示为S_n；经过n次恒等变换的群称为n次对称群。

7.4.2 置换群

- 例7.24 具体写出三次对称群$\boldsymbol{S_3}$。

解：设$S=\{1,2,3\}$，于是$|S_3|=3!\ =6$，这6个置换分别是

$$e=\begin{pmatrix}123\\123\end{pmatrix},\sigma_1=\begin{pmatrix}123\\132\end{pmatrix},\sigma_2=\begin{pmatrix}123\\213\end{pmatrix},$$

$$\sigma_3=\begin{pmatrix}123\\321\end{pmatrix},\sigma_4=\begin{pmatrix}123\\312\end{pmatrix},\sigma_5=\begin{pmatrix}123\\231\end{pmatrix},$$

其运算表在下页。

7.4.2 置换群

运算表

$\cdot$	e	σ_1	σ_2	σ_3	σ_4	σ_5
e	e	σ_1	σ_2	σ_3	σ_4	σ_5
σ_1	σ_1	e	σ_4	σ_5	σ_2	σ_3
σ_2	σ_2	σ_5	e	σ_4	σ_3	σ_1
σ_3	σ_3	σ_4	σ_5	e	σ_1	σ_2
σ_4	σ_4	σ_3	σ_1	σ_2	σ_5	e
σ_5	σ_5	σ_2	σ_3	σ_1	e	σ_4

7.4.2 置换群

由此表可知，*e*为恒等元。

${\sigma_1}^{-1} = \sigma_1$，${\sigma_2}^{-1} = \sigma_2$，${\sigma_3}^{-1} = \sigma_3$，${\sigma_4}^{-1} = \sigma_5$，${\sigma_5}^{-1} = \sigma_4$，

同时，$\sigma_1\sigma_2 = \sigma_4$，$\sigma_2\sigma_1 = \sigma_5$。

所以它是不能交换的群。这是一个很典型的6（含有6个元素）阶的群。

7.5 群的同态与同构

- 定义7.23 给定群$\langle G,\odot\rangle$和$\langle H,*\rangle$，则$\langle G,\odot\rangle \simeq \langle H,*\rangle$:

$$(\forall g)\left(g \in H^G \wedge (\forall a)(\forall b)(a,b \in G \to g(a\odot b) = g(a) * g(b))\right)$$

并称g为从群$\langle G,\odot\rangle$到群$\langle H,*\rangle$的群同态映射。

  - 群同态保持幺元，逆元和子群。

7.5 群的同态与同构

- 定理7.21 设g为从群$\langle G,\odot\rangle$到群$\langle H,*\rangle$的群同态映射，则

  (1) 若e_G和e_H分别为两群的幺元，那么，$g(e_G)=e_H$。

  (2) 若$a\in G$，那么，$g(a^{-1})=(g(a))^{-1}$。

  (3) 若$\langle S,\odot\rangle$是群$\langle G,\odot\rangle$的子群且$g(S)=\{g(a)|\ a\in S\}$，那么，$\langle g(S),*\rangle$为群$\langle H,*\rangle$的子群。

- 定理7.22 给定群$\langle G,\odot\rangle$和代数系统$\langle H,*\rangle$，若g是从群$\langle G,\odot\rangle$到$\langle H,*\rangle$的满同态映射，则$\langle H,*\rangle$为群。

根据g是单射、满射和双射，群同态分别称为群单一同态映射、群满同态映射和群同构映射。

作 业

- 11-16