第八章 群
2015年09月14日

信息安全数学基础

陈恭亮　教授 博士生导师

上海交通大学信息安全工程学院

chengl@sjtu.edu.cn

对集合运算的思考

1. 一个有运算的集合应该具有什么样的性质? 举例说明.
2. 从有效性的角度而言, 一个有运算的集合应该具有什么样的性质? 举例说明.
3. 从安全性的角度而言，一个有运算的集合应该具有什么样的性质? 举例说明.
4. 同构的群具有相同的计算复杂性吗? 举例说明.
5. 如何借助同构的群来提高运算效率. 编程实现F_p 中的乘法运算, 并举例说明.
6. 如何借助同构的群来提高运算效率. 研究和实现加密算法AES中的乘法运算, 并举例说明.
7. 如何得到同构的群.
8. 研究循环群的性质. 研究置换群的性质.

1. 群的定义和基本性质.
2. 子群及其判断.
3. 陪集和拉格朗日定理.
4. 正规子群和商群.
5. 同态和同构.
6. 同态分解定理.

§8.1.1 基本定义

首先, 给出集合中关于运算的表述.

定义8.1.1 设S 是一个非空集合. 那么$S\times S$ 到S 的映射叫做S 的**结合法**或**运算**.

$$\begin{array}{ccc} S\times S & \longrightarrow & S \\ (a,b) & \longmapsto & ab \end{array}$$

对于这个映射, 元素对(a,b) 的像叫做a 与b 的**乘积**, 记成$a\otimes b$ 或$a\cdot b$ 或$a*b$ 等, 为方便起见, 该乘积简记为$a\,b$. 这个结合法叫做**乘法**.

这时, S 叫做**代数系**.

人们也常把该结合法叫做**加法**, 元素对(a,b) 的像叫做a 与b 的**和**, 记成$a\oplus b$ 或$a+b$.

其次, 对于结合法或运算, 给出4 个运算规则的表述.

1) 人们常要求结合法具有结合律. 即对于S 中的3 个元素$a,\ b,\ c$, 由两种方式得到它们的乘积$(a\,b)\,c$ 和$a\,(b\,c)$ 应相等.

结合律 设S 是一个具有结合法的非空集合. 如果对S 中的任意元素$a,\ b,\ c$, 都有

$$(a\,b)\,c = a\,(b\,c),$$

则称该结合法满足**结合律**.

定义8.1.2 设S 是一个具有结合法的非空集合. 如果S 满足结合律, 那么S 叫做S 的**半群**.

2) 人们常要求S 中有一个像整数集合$\mathbf{Z}$ 中元素1 那样的元素单位元, 与任何元素相乘都不改变该元素.

单位元 设S 是一个具有结合法的非空集合. 如果S 中有一个元素e 使得, 对S 中所有元素a , 都有

$$e\,a = a\,e = a,$$

则称该元素e 为S 中的**单位元**. 通常记作e.

当S 的结合法写作加法时, 这个e 叫做S 中的零元, 通常记作0.

性质8.1.1 设S 是一个具有结合法的非空集合. 则S 中的**单位元e 是惟一的**.

证 设e 和e' 都是S 中的单位元. 分别根据e 和e' 的单位元定义, 得到

$$e' = e\,e' = e.$$

因此, 单位元是惟一的. 证毕

3) 人们常要求S 中每个元a 都有对应的元素a' 使得它们的乘积aa' 为单位元.

可逆元 设S 是一个具有结合法的有单位元的非空集合. 设a 是S 中的一个元素. 如果S 存在一个元素a' 使得

$$a\,a' = a'\,a = e,$$

则称该元素a 为S 中的**可逆元**, a' 称为a 的**逆元**, 通常记作a^{-1}.

当S 的结合法叫做加法时, 这个a' 叫做元素a 的负元, 通常记作$-a$.

性质8.1.2 设S 是一个有单位元的半群. 则对S 中任意可逆元a, 其逆元a' 是惟一的.

证 设a' 和a'' 都是a 的逆元, 即 $a\,a' = a'\,a = e, \qquad a\,a'' = a''\,a = e.$

分别根据a' 和a'' 为a 的逆元及结合律, 得到

$$a' = a'\,e = a'\,(a\,a'') = (a'\,a)\,a'' = e\,a'' = a''.$$

因此, a 的逆元a' 是惟一的. 证毕

4) 人们常要元素的乘积运算与它们的乘积次序无关. 即对于S 中的2 个元素a, b, 由两种方式得到它们的乘积$a\,b$ 和$b\,a$ 应相等.

交换律 设S 是一个具有结合法的非空集合. 如果对S 中的任意元素a, b, 都有

$$b\,a = a\,b,$$

则称该结合法满足**交换律**.

最后, 给出常用的具有结合律、单位元及可逆元规则的代数系.

定义8.1.3 设G 是一个具有结合法的非空集合. G 叫做一个**群**, 如果G 中的结合法满足如下三个条件:

(i) 结合律, 即对任意的$a,\ b,\ c \in G$, 都有 $(a\,b)\,c = a\,(b\,c)$;

(ii) 单位元, 即存在一个元素$e \in G$, 使得对任意的$a \in G$, 都有

$$a\,e = e\,a = a;$$

(iii) 可逆性, 即对任意的$a \in G$, 都存在$a' \in G$, 使得

$$a\,a' = a'\,a = e,$$

特别地, 当G 的结合法写作乘法时, G 叫做**乘群**; 当G 的结合法写作加法时, G 叫做**加群**.

群G 的元素个数叫做群G 的**阶**, 记为$|G|$. 当$|G|$ 为有限数时, G 叫做**有限群**, 否则, G 叫做**无限群**.

如果群G 中的结合法还满足交换律, 即对任意的$a,\ b \in G$, 都有$a\,b = b\,a$, 那么, G 叫做一个**交换群**或**阿倍尔(Abel)群**.

例8.1.1 自然数集 $\mathbf{N} = \{0, 1, 2, \ldots, n, \ldots\}$ 对于通常意义下的加法有结合律和零元0, 但没有负元, 例如, 2 无负元. 而对于通常意义下的乘法, 有结合律和单位元$e = 1$, 但没有可逆元. 例如, 2 无逆元.

例8.1.2 整数集 $\mathbf{Z} = \{\ldots, -n, \ldots, -2, -1, 0, 1, 2, \ldots, n, \ldots\}$ 对于通常意义下的加法, 有结合律, 交换律和零元0, 并且每个元素a 有负元$-a$. 因此, $\mathbf{Z}$ 是一个交换加群. 非零整数集$\mathbf{Z}^* = \mathbf{Z} \setminus \{0\}$ 对于通常意义下的乘法, 有结合律, 交换律和单位1, 但不是每个元素a 都有逆元, 例如, 2 无逆元, 因此$\mathbf{Z}^*$ 不是一个群.

例8.1.3 有理数集 $\mathbf{Q}$ 对于通常意义下的加法有结合律, 交换律和零元0, 并且每个元素$\frac{a}{b}$ $(b \neq 0)$ 有负元$\frac{-a}{b}$, 因此, $\mathbf{Q}$ 是交换加群.

非零有理数集$\mathbf{Q}^* = \mathbf{Q} \setminus \{0\}$ 对于通常意义下的乘法有结合律, 交换律和单位1, 并且每个元素$\frac{a}{b}$ $(ab \neq 0)$ 都有逆元$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$, 因此,$\mathbf{Q}^*$ 是交换乘群.

类似地, 实数集 $\mathbf{R}$ 和复数集 $\mathbf{C}$ 都是对于通常意义下的加法的交换加群. 而非零实数集$\mathbf{R}^* = \mathbf{R} \setminus \{0\}$ 和非零复数集$\mathbf{C}^* = \mathbf{C} \setminus \{0\}$ 都是对于通常意义下的乘法的交换乘群.

例8.1.4 设D 是一个非平方整数. 则集合

$$\mathbf{Z}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbf{Z}\}$$

对于加法运算:

$$(a + b\sqrt{D}) \oplus (c + d\sqrt{D}) = (a + c) + (b + d)\sqrt{D}$$

有结合律, 交换律和零元0, 并且每个元素$a + b\sqrt{D}$ 有负元$(-a) + (-b)\sqrt{D}$, 因此$\mathbf{Z}(\sqrt{D})$ 构成一个交换加群.
对于乘法运算

$$(a + b\sqrt{D}) \otimes (c + d\sqrt{D}) = (ac + bdD) + (bc + ad)\sqrt{D}$$

有结合律, 交换律和单位1, 但不是每个元素$a + b\sqrt{D}$ 都有逆元, 例如, 2 无逆元, 因此$\mathbf{Z}(\sqrt{D})$ 不构成一个乘群.

例8.1.5 设n 是一个正整数. 设$\mathbf{Z}/n\mathbf{Z} = \{0, 1, 2, \ldots, n-1\}$. 证明: 集合$\mathbf{Z}/n\mathbf{Z}$ 对于加法:

$$a \oplus b = (a + b \pmod{n})$$

构成一个交换加群, 其中$a \pmod{n}$ 是整数a 模n 的最小非负剩余.
零元是0, a 的负元是$n - a$.
例如, $n = 6$

$a \setminus b$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

例8.1.6 设p 是一个素数, $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$. 设$\mathbf{F}_p^* = \mathbf{F}_p \setminus \{0\}$. 证明: 集合$\mathbf{F}_p^*$ 对于乘法:

$$a \otimes b = (a \cdot b \pmod p)$$

构成一个交换乘群.

单位元是1, a 的逆元是$(a^{-1} \pmod p)$.

例如, $n = 7$

$a \setminus b$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

例8.1.7 设n 是一个合数. 证明: 集合$\mathbf{Z}/n\mathbf{Z}\setminus\{0\}$ 对于乘法:

$$a \otimes b = (a \cdot b \pmod n)$$

不构成一个乘群.

证 集合$\mathbf{Z}/n\mathbf{Z}\setminus\{0\}$ 中有结合律和单位元是1. 但不是所有元素都是可逆元, 如n 的真因数d 没有逆元, 因为对任意的$d' \in \mathbf{Z}/n\mathbf{Z}\setminus\{0\}$, 都有

$$d \otimes d' = (d \cdot d' \pmod n) \neq 1.$$

例如, $n = 6, \quad d = 2$

$a \setminus x$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

例8.1.8 设n 是一个合数. 设$(\mathbf{Z}/n\mathbf{Z})^* = \{a \mid a \in \mathbf{Z}/n\mathbf{Z},\ (a,n)=1\}$.
证明: 集合$(\mathbf{Z}/n\mathbf{Z})^*$ 对于乘法:

$$a \otimes b = (a \cdot b \pmod n)$$

构成一个交换乘群.
具有结合律，单位元是1，a 的逆元是$(a^{-1} \pmod n)$.
例如, $n = 15$

$a \setminus x$	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

例8.1.9 设有元素在数域$\mathbf{K}$ 中的全体n 级矩阵组成的集合

$$M_n(\mathbf{K}) = \{(a_{ij})_{1\le i\le n, 1\le j\le n} \mid a_{ij}\in \mathbf{K},\ 1\le i\le n, 1\le j\le n\}.$$

1) 设$A=(a_{ij}),\ B=(b_{ij})\in M_n(\mathbf{K})$. 我们定义加法:

$$A+B=C, \qquad \text{其中 } c_{ij}=a_{ij}+b_{ij},\ 1\le i\le n, 1\le j\le n.$$

则$M_n(\mathbf{K})$ 对于加法有结合律, 交换律和零元0, 并且每个元素$A=(a_{ij})$ 有负元$-A=(-a_{ij})$, 因此$M_n(\mathbf{K})$ 构成一个交换加群.

例如, $n=2$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} \\ a_{21}+b_{21} & a_{22}+b_{22} \end{pmatrix}$$

零元$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ 的负元为$\begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix}$.

2) 设$A=(a_{ij}),\ B=(b_{ij})\in M_n(\mathbf{K})$.我们再定义乘法:

$$A\cdot B=C,\quad \text{其中 } c_{ij}=\sum_{k=1}^{n}a_{ik}b_{kj},\ 1\le i\le n, 1\le j\le n.$$

则$M_n(\mathbf{K})\setminus\{0\}$ 对于乘法不构成一个群.

例如, $\begin{pmatrix}0&1\\0&0\end{pmatrix}\cdot\begin{pmatrix}0&1\\0&0\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$

3) 可逆矩阵A (即存在A' 使得$AA'=A'A=I_n$) 所组成的集合,记为$GL_n(P)$, 对于矩阵的乘法成一个群, 通常称$GL_n(\mathbf{K})$ 为n 级**一般线性群**; $GL_n(\mathbf{K})$ 中全体行列式为1 的矩阵对于矩阵乘法也成一个群, 这个群记为$SL_n(\mathbf{K})$, 称为**特殊线性群**.

例如, $n=2$, $SL_2(\mathbf{K})$ 中的乘法为

$$\begin{pmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{pmatrix}\cdot\begin{pmatrix}b_{11}&b_{12}\\b_{21}&b_{22}\end{pmatrix}=\begin{pmatrix}a_{11}b_{11}+a_{12}b_{21}&a_{11}b_{12}+a_{12}b_{22}\\a_{21}b_{11}+a_{22}b_{21}&a_{21}b_{12}+a_{22}b_{22}\end{pmatrix}$$

单位元$\begin{pmatrix}1&0\\0&1\end{pmatrix}$, $\begin{pmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{pmatrix}$ 的逆元为$\begin{pmatrix}a_{22}&-a_{12}\\-a_{21}&a_{11}\end{pmatrix}$.

例8.1.10 设S 是一个非空集合. G 是S 到自身的所有一一对应的映射f 组成的集合. 对于$f, g \in G$, 定义f 和g 的复合映射$g \circ f$ 为: 对于任意$x \in S$,

$$(g \circ f)(x) = g(f(x)).$$

则G 对于映射的复合运算, 构成一个群, 叫做**对称群**. 恒等映射是单位元. G 中的元素叫做S 的一个**置换**.

当S 是n 元有限集时, G 叫做n 元**对称群**, 记作S_n.

映射复合如下图:

$$\underbrace{\begin{array}{ccccc} S & \overset{f}{\longrightarrow} & S & \overset{g}{\longrightarrow} & S \\ x & \longmapsto & f(x) & \longmapsto & g(f(x)) \end{array}}_{g \circ f:\ x \longmapsto g(f(x))}$$

例8.1.11 设σ 是对正方形作逆时针90^o 旋转的变换(如下图所示). 则

$$G = \{\sigma,\ \sigma^2,\ \sigma^3,\ \sigma^4 = id\}$$

对于映射的复合构成一个群.

事实上, σ^2 是对正方形作逆时针180^o 旋转的变换, σ^3 是对正方形作逆时针270^o 旋转的变换, σ^4 是对正方形作逆时针360^o 旋转的变换, 即保持正方形不变. . G 是一个群.

例8.1.12 设τ_1 是对正方形作关于$y-$ 轴的对称变换, τ_2 是对正方形作关于$x-$ 轴的对称变换(如下图所示). 则

$$G = \{\tau_1,\ \tau_2,\ \tau_2 \circ \tau_1,\ \tau_1^2 = id\}$$

对于映射的复合构成一个群.

事实上, $\tau_2 \circ \tau_1$ 是对正方形作逆时针180^o 旋转的变换, 因此, $\tau_1,\ \tau_2,\ \tau_2 \circ \tau_1$ 都是2 阶元. G 是一个群.

下面讨论n 个元素的乘积运算.

设$a_1, a_2, \ldots, a_{n-1}, a_n$ 是群G 中的n 个元素. 通常归纳地定义这n 个元素的乘积为

$$a_1 a_2 \cdots a_{n-1} a_n = (a_1 a_2 \cdots a_{n-1}) a_n.$$

当G 的结合法叫做加法时, 通常归纳地定义这n 个元素的和为

$$a_1 + a_2 + \cdots + a_{n-1} + a_n = (a_1 + a_2 + \cdots + a_{n-1}) + a_n.$$

下面的性质说明: 在有结合律的情况下, 可有序结合一些元素作乘积, 但最终的乘积结果是确定的.

性质8.1.3 设$a_1, \ldots, a_n$ 是群G 中$n \geq 2$ 个元素. 则对任意的$1 \leq i_1 < \ldots < i_k < n$, 有

$$(a_1 \cdots a_{i_1}) \cdots (a_{i_k+1} \cdots a_n) = a_1 a_2 \cdots a_{n-1} a_n.$$

证 对n 作数学归纳法.

$n=3$ 时, 根据结合律得到$a_1(a_2a_3)=(a_1a_2)a_3=a_1a_2a_3$. 结论成立.

假设$n-1$ 时, 结论成立.

对于n, 如果$i_{k+1}=n$, 则根据归纳假设,

$$(a_1\cdots a_{i_1})\cdots(a_{i_k+1}\cdots a_n)=(a_1a_2\cdots a_{n-1})a_n=a_1a_2\cdots a_{n-1}a_n.$$

如果$i_{k+1}<n$, 则根据归纳假设和结合律,

$$\begin{aligned}(a_1\cdots a_{i_1})\cdots(a_{i_{k-1}+1}\cdots a_{i_k})(a_{i_k+1}\cdots a_n) &= (a_1\cdots a_{i_k})\cdot(a_{i_k+1}\cdots a_{n-1})a_n\\ &= (a_1a_2\cdots a_{n-1})a_n\\ &= a_1a_2\cdots a_{n-1}a_n.\end{aligned}$$

因此, 结论对于n 成立. 根据数学归纳法原理, 结论对任意n 成立.

证毕

性质8.1.4 设$a_1, a_2, \ldots, a_{n-1}, a_n$ 是群G 中的任意$n \geq 2$ 个元素. 则

$$(a_1a_2\cdots a_{n-1}a_n)^{-1} = a_n^{-1}a_{n-1}^{-1}\cdots a_2^{-1}a_1^{-1}.$$

证 对n 作数学归纳法.

$n = 2$ 时, 根据性质8.1.3, 有

$$(a_1a_2)(a_2^{-1}a_1^{-1}) = a_1(a_2a_2^{-1})a_1^{-1} = a_1a_1^{-1} = e$$

和
$$(a_2^{-1}a_1^{-1})(a_1a_2) = a_2^{-1}(a_1^{-1}a_1)a_2 = a_2^{-1}a_2 = e$$

所以,$(a_1a_2)^{-1} = a_2^{-1}a_1^{-1}$, 结论成立.

假设$n-1$ 时, 结论成立. 对于n, 由情形$n = 2$ 及归纳假设, 有

$$\begin{aligned}(a_1a_2\cdots a_{n-1}a_n)^{-1} &= ((a_1a_2\cdots a_{n-1})a_n)^{-1}\\ &= a_n^{-1}(a_1a_2\cdots a_{n-1})^{-1}\\ &= a_n^{-1}a_{n-1}^{-1}\cdots a_2^{-1}a_1^{-1}.\end{aligned}$$

因此, 结论对于n 成立. 由数学归纳法原理, 结论对任意n 成立证毕

性质8.1.5 设$a_1, a_2, \ldots, a_{n-1}, a_n$ 是交换群G 中的任意$n \geq 2$ 个元素. 则对$1, 2, \ldots, n$ 的任一排列$i_1, i_2, \ldots, i_n$, 有

$$a_{i_1} a_{i_2} \cdots a_{i_n} = a_1 a_2 \cdots a_n.$$

证 对n 作数学归纳法.

$n = 2$ 时, 根据交换得到$a_2 a_1 = a_1 a_2$. 结论成立.

假设$n - 1$ 时, 结论成立. 对于n, 如果$i_n = n$, 则根据结合律和归纳假设,

$$a_{i_1} \cdots a_{i_{n-1}} a_{i_n} = (a_{i_1} \cdots a_{i_{n-1}}) a_n = (a_1 a_2 \cdots a_{n-1}) a_n = a_1 a_2 \cdots a_{n-1} a_n.$$

如果$i_n < n,\ i_k = n$, 则根据结合律, 交换律及前面的结果,

$$\begin{aligned} a_{i_1} \cdots a_{i_k-1} a_{i_k} a_{i_k+1} \cdots a_{i_n} &= (a_{i_1} \cdots a_{i_k-1}) a_n (a_{i_k+1} \cdots a_{i_n}) \\ &= (a_{i_1} \cdots a_{i_k-1})(a_{i_k+1} \cdots a_{i_n}) a_n \\ &= a_1 a_2 \cdots a_{n-1} a_n. \end{aligned}$$

因此, 结论对于n 成立. 根据数学归纳法原理, 结论对任意n 成立.

证毕

设n 是正整数.如果$a_1 = a_2 = \cdots = a_n = a$, 则记$a_1 a_2 \cdots a_n = a^n$, 称之为$a$ 的n 次幂. 特别地, 定义$a^0 = e$ 为单位元, $a^{-n} = (a^{-1})^n$ 为逆元a^{-1} 的n 次幂.

性质8.1.6 设a 是群G 中的任意元，则对任意的整数m, n, 我们有

$$a^m a^n = a^{m+n}, \quad (a^m)^n = a^{mn}.$$

证 我们分如下几种情况证明:

(i) $m > 0,\ n > 0$. 根据性质8.1.5, 有 $a^m a^n = a^{m+n}, \quad (a^m)^n = a^{mn}$.

(ii) $m = 0,\ n > 0$. 有

$$a^m a^n = e a^n = a^{m+n}, \quad (a^m)^n = (a^0)^n = e = a^{mn}.$$

(iii) $m < 0,\ n > 0$. 有

$$a^m a^n = (a^{-1})^{-m} a^n = \begin{cases} a^{n-(-m)} = a^{m+n} & \text{如果} \ -m < n \\ e = a^{m+n} & \text{如果} \ -m = n \\ (a^{-1})^{-m-n} = a^{m+n} & \text{如果} \ -m > n \end{cases},$$

$$(a^m)^n = ((a^{-1})^{-m})^n = (a^{-1})^{-mn} = a^{mn}.$$

(iv) $n = 0$.

$$a^m a^n = a^m e = a^m = a^{m+n}, \quad (a^m)^n = e = a^{mn}.$$

(v) $m > 0,\ n < 0$. 有

$$a^m a^n = a^m (a^{-1})^{-n} = \begin{cases} a^{m-(-n)} = a^{m+n} & \text{如果 } m > -n \\ e = a^{m+n} & \text{如果 } m = -n \\ (a^{-1})^{-n-m} = a^{m+n} & \text{如果 } m < -n \end{cases},$$

$$(a^m)^n = ((a^m)^{-1})^{-n} = ((a^{-1})^m)^{-n} = (a^{-1})^{-mn} = a^{mn}.$$

(vi) $m < 0,\ n < 0$. 有

$$a^m a^n = (a^{-1})^{-m} (a^{-1})^{-n} = (a^{-1})^{-m-n} = a^{m+n},$$

$$(a^m)^n = ((a^m)^{-1})^{-n} = (a^{-m})^{-n} = a^{mn}.$$

因此, 性质8.1.6 成立. 证毕

最后, 通过方程求解来描述一个集合是否构成一个群.

定理8.1.1 设G 是一个具有结合法的非空集合. 如果G 是一个群, 则方程

$$a\,x = b, \quad y\,a = b$$

在G 中有解. 反过来, 如果上述方程在G 中有解, 并且结合法满足结合律，则G 是一个群.

证 设G 是一个群. 在方程$a\,x = b$ 两端左乘a^{-1}, 得到

$$a^{-1}\,(a\,x) = a^{-1}\,b,$$

即$x = a^{-1}\,b$ 是方程$a\,x = b$ 的解. 同理, $y = b\,a^{-1}$ 是方程$y\,a = b$ 的解.

$$\underline{a\,x = b, \quad y\,a = b}$$

反过来, 设方程$a\,x = b, \quad y\,a = b$在G 中有解. 因为G 非空, 所以G 中有元素c, 并且$c\,x = c$ 有解$x = e_r$. 这个e_r 是G 中的(右)单位元. 事实上, 对任意$a \in G$, 因为$y\,c = a$ 有解, 所以

$$a\,e_r = (y\,c)\,e_r = y\,(c\,e_r) = y\,c = a.$$

同理, $y\,c = c$ 的解$y = e_l$ 是G 中的(左)单位元. 事实上, 对任意$a \in G$, 因为$c\,x = a, \; y\,c = a$ 有解, 所以

$$e_l\,a = e_l\,(c\,x) = (e_l\,c)\,x = c\,x = a.$$

因此, $e_r = e_l e_r = e_l = e$ 是G 中的单位元.
对G 中任意元素a, 设方程$a\,x = e, \quad y\,a = e$在G 中的解分别为$x = a', \; y = a''$. 则

$$a' = e\,a' = (a''\,a)\,a' = a''\,(a\,a') = a''\,e = a''.$$

因此, a' 是a 在G 中的逆元. 故G 是一个群. 证毕

8.1.2.1 子群及其基本性质

本节讨论具有运算的子集合.

定义8.1.4 设H 是群G 的一个子集合. 如果对于群G 的结合法, H 成为一个群, 那么H 叫做群G 的**子群**, 记作$H \leq G$.

$H = \{e\}$ 和$H = G$ 都是群G 的子群, 叫做群G 的**平凡子群**. 群G 的子群H 叫做群G 的**真子群**, 如果H 不是群G 的平凡子群.

例8.1.3 设H 是$\mathbf{Z}$ 的真子群. 则存在正整数n, 使得$H = n\mathbf{Z} = \{k \cdot n \mid k \in \mathbf{Z}\}$.

证 因为H 是真子群, 所以存在非零整数$a \in H$. 又因为H 是子群, 所以$-a \in H$. 这说明H 中有正整数. 设H 中的最小正整数为n, 则有$H = n\mathbf{Z}$. 事实上, 对任意的$a \in H$, 不妨设$a > 0$, 根据欧几里得除法(定理1.1.10), 存在正整数q 及整数r 使得

$$a = q \cdot n + r, \quad 0 \leq r < n.$$

如果$r \neq 0$, 则$r = a + q(-n) \in H$, 这与n 的最小性矛盾. 因此, $r = 0$, $a = q \cdot n \in n\mathbf{Z}$. 故$H \subset n\mathbf{Z}$. 但显然有$n\mathbf{Z} \subset H$. 因此, $H = n\mathbf{Z}$. 证毕

下面给出子群的判断.

定理8.1.2 设H 是群G 的一个非空子集合. 则H 是群G 的子群的充要条件是: 对任意的$a,\ b\in H$, 有$a\,b^{-1}\in H$.

证 必要性是显然的. 我们来证充分性.

因为G 非空, 所以G 中有元素a. 根据假设, 我们有$e=a\,a^{-1}\in H$. 因此, H 中有单位元. 对于$e\in H$ 及任意a, 再应用假设, 我们有$a^{-1}=e\,a^{-1}\in H$, 即H 中每个元素a 在H 中有逆元. 因此, H 是群G 的子群. 证毕

我们考虑多个子群的交集.

定理8.1.3 设G 是一个群, $\{H_i\}_{i\in I}$ 是G 的一族子群. 则$\bigcap\limits_{i\in I} H_i$ 是G 的一个子群.

证 对任意的$a,\ b \in \bigcap\limits_{i\in I} H_i$, 有$a,\ b \in H_i,\ i \in I$. 因为$H_i$ 是G 的子群, 根据定理8.1.2, 我们有$a\,b^{-1} \in H_i,\ i \in I$. 进而, $a\,b^{-1} \in \bigcap\limits_{i\in I} H_i$. 根据定理8.1.2, $\bigcap\limits_{i\in I} H_i$ 是G 的一个子群. 证毕

根据定理8.1.3, 人们可给出一个非空子集X 生成一个子群的表述, 即包含X 的最小子群.

注 多个子群的并集不一定是子群.

8.1.2.2 子群的生成

利用定理8.1.3, 我们可以包含一个子集X 的最小子群或由子集X 生成的子群.

定义8.1.5设G 是一个群, X 是G 的子集. 设$\{H_i\}_{i\in I}$ 是G 的包含X 的所有子群. 则$\bigcap_{i\in I} H_i$ 叫做G 的由X **生成的子群**. 记为$< X >$. X 的元素称为子群$< X >$ 的**生成元**. 如果$X = \{a_1, \ldots, a_n\}$, 则记$< X >$ 为$< a_1, \ldots, a_n >$. 如果$G =< a_1, \ldots, a_n >$, 则称G 为有**限生成的**. 特别地, 如果$G =< a >$, 则称G 为a 生成的**循环群**.

下面给出$< X >$中元素的显示表示. 先考虑交换群中由有限个元素生成的群.

定理8.1.4 设G 是交换群, $X =< a_1, a_2, \ldots, a_t >$ 是G 的子集. 则

(i) 当G 为乘法群时, 由X 生成的子群为

$$< X >= \{a_1^{n_1} \cdots a_t^{n_t} \mid a_i \in X,\ n_i \in \mathbf{Z},\ 1 \le i \le t\}.$$

特别, 对任意的$a \in G$, 有 $< a >= \{a^n \mid n \in \mathbf{Z}\}$.

(ii) 当G 为加法群时, 由X 生成的子群为

$$< X >= \{n_1a_1 + \cdots + n_ta_t \mid a_i \in X,\ n_i \in \mathbf{Z},\ 1 \le i \le t\}.$$

特别, 对任意的$a \in G$, 有 $< a >= \{na \mid n \in \mathbf{Z}\}$.

证 (i) G 为乘法群. 令 $H = \{a_1^{n_1} \cdots a_t^{n_t} \mid a_i \in X,\ n_i \in \mathbf{Z},\ 1 \le i \le t\}$.
(则H 是G 的子群). 显然, 有$X \subset H$. 我们先证明H 是群G 的子群, 从而有$< H >\subset H$. 事实上, 对任意$a = a_1^{n_1} \cdots a_t^{n_t}$, $b = a_1^{m_1} \cdots a_t^{m_t} \in H$, 运用性质8.1.4, 有

$$a \cdot b^{-1} = a_1^{n_1} \cdots a_t^{n_t} \cdot a_t^{-m_1} \cdots a_1^{-m_t} = a_1^{n_1-m_1} \cdots a_t^{n_t-m_t} \in H.$$

因此, H 是G 的子群.

再证明$H \subset \langle X \rangle$. 设$H_j$ 是包含X 的任意子群. 则对任意$a = a_1^{n_1}\cdots a_t^{n_t} \in H$, 由$a_i \in X$, 得到$a_i \in H_j$. 又因为$H_j$ 是子群, 所以$a_i^{n_i} \in H_j$, $a = a_1^{n_1}\cdots a_t^{n_t} \in H_j$. 即$H \subset H_j$, $H \subset \bigcap_j H_j$. 因此, $H = \langle X \rangle$ 是由X 生成的子群.

(ii) G 为加法群. 令

$$H = \{n_1a_1 + \cdots + n_ta_t \mid a_i \in X,\ n_i \in \mathbf{Z},\ 1 \le i \le t\}.$$

则H 是G 的子群. 事实上, 对任意$a = n_1a_1 + \cdots n_ta_t$, $b = m_1a_1 + \cdots + m_ta_t \in H$, 运用性质8.1.4, 有

$$a - b = (n_1 - m_1)a_1 + \cdots + (n_t - m_t)a_t \in H.$$

因此, H 是G 的子群.

再设H_j 是包含X 的任意子群. 则对任意$a = n_1a_1 + \cdots + n_ta_t \in H$, 由$a_i \in X$, 得到$a_i \in H_j$. 又因为$H_j$ 是子群, 所以$n_ia_i \in H_j$, $a = n_1a_1 + \cdots + n_ta_t \in H_j$. 即$H \subset H_j$, $H \subset \bigcap_j H_j$. 因此, $H = \langle X \rangle$ 是由X 生成的子群. 证毕

例8.1.14 设$G=\langle g\rangle=\{g^r \mid g^r \neq 1,\ 1 \leq r < n,\ g^n = 1\}$. 则 G 是n阶循环群, 且$\langle g^d\rangle=\{g^{dk} \mid k \in \mathbf{Z}\}$ 是G 的子群.

再考虑一般的群G 及非空子集X.

定理8.1.5 设G 是一个群, X 是G 的非空子集. 则由X 生成的子群为

$$\langle X\rangle=\{a_1^{n_1}\cdots a_t^{n_t} \mid t \in \mathbf{N},\ a_i \in X,\ n_i \in \mathbf{Z},\ 1 \leq i \leq t\}.$$

特别, 对任意的$a \in G$, 有

$$\langle a\rangle=\{a^n \mid n \in \mathbf{Z}\}.$$

证 因为X 非空, 所以

$$H_0 = \{a_1^{n_1} \cdots a_t^{n_t} \mid t \in \mathbf{N},\ a_i \in X,\ n_i \in \mathbf{Z},\ 1 \le i \le t\}$$

非空. 则对任意$x = a_1^{n_1} \cdots a_t^{n_t}$, $y = a_{t+1}^{n_{t+1}} \cdots a_s^{n_s} \in H_0$, 运用性质8.1.4, 有

$$x \cdot y^{-1} = a_1^{n_1} \cdots a_t^{n_t} \cdot a_s^{-n_s} \cdots a_{t+1}^{-n_{t+1}} \in H_0.$$

因此, H_0 是G 的子群. 再设H_j 是包含X 的任意子群. 则对任意$a = a_1^{n_1} \cdots a_t^{n_t} \in H_0$, $a_i \in X$, 有$a_i \in H_j$. 因为H_j 是子群, 所以$a \in H_j$. 即$H_0 \subset H_j$, $H_0 \subset \bigcap\limits_j H_j$.

因此, $H_0 =< X >$ 是由X 生成的子群. 证毕

8.2 正规子群和商群

8.2.1 陪集 拉格朗日定理

类似于模同余分类, 人们可以通过群G 的子群H 对群G 进行分类(定理8.2.1)

$$aH = \{c \mid c \in G,\ a^{-1}c \in H\}.$$

定义8.2.1 设H 是群G 的子群, a 是G 中任意元. 那么集合

$$aH = \{ah \mid h \in H\} \quad (\text{对应地}\ \ Ha = \{ha \mid h \in H\})$$

分别叫做G 中H 的左(对应地 右)陪集. aH (对应地Ha)中的元素叫做aH (对应地Ha) 的代表元. 如果$aH = Ha$, 则 aH 叫做G 中H 的陪集

例8.2.1 设$n > 1$ 是整数. 则$H = n\mathbf{Z}$ 是$\mathbf{Z}$ 的子群, 子集

$$a + n\mathbf{Z} = \{a + k \cdot n \mid k \in \mathbf{Z}\}$$

就是$n\mathbf{Z}$ 的陪集. 这个陪集就是模n 的剩余类.

定理8.2.1 设H 是群G 的子群, 则

(i) 对任意$a \in G$, 有

$$aH = \{c \,|\, c \in G,\ a^{-1}c \in H\} \ \ (\text{对应地 } Ha = \{c \,|\, c \in G,\ ca^{-1} \in H\}).$$

(ii) 对任意$a,\ b \in G$, $aH = bH$ 的充要条件$b^{-1}a \in H$ (对应地$Ha = Hb$ 的充要条件$ab^{-1} \in H$).

(iii) 对任意$a,\ b \in G$, $aH \cap bH = \emptyset$ 的充要条件$b^{-1}a \notin H$ (对应地$Ha \cap Hb = \emptyset$ 的充要条件$ab^{-1} \notin H$).

(iv) 对任意$a \in H$, 有$aH = H = Ha$.

证 (i) 令$H_{al} = \{c \,|\, c \in G,\ a^{-1}c \in H\}$. 要证明: $aH = H_{al}$. 对任意的$c \in aH$, 存在$h \in H$ 使得$c = ah$. 从而, $a^{-1}c = h \in H$, 即$c \in H_{al}$. 因此, $aH \subset H_{al}$. 反过来, 对任意的$c \in H_{al}$, 有$a^{-1}c \in H$, 从而存在$h \in H$ 使得$a^{-1}c = h$. 由此, $c = ah \in aH$. 因此, $H_{al} \subset aH$. 故$aH = \{c \,|\, c \in G,\ a^{-1}c \in H\}$.

同理可得, $Ha = \{c \,|\, c \in G,\ ca^{-1} \in H\}$.

(ii) 设$aH = bH$. 则$a = ae \in aH = bH$. 故$b^{-1}a \in H$. 反过来, 设$b^{-1}a = h_1 \in H$. 对任意$c \in aH$, 存在$h_2 \in H$ 使得$c = ah_2$. 进而,

$$c = b(b^{-1}a)h_2 = b(h_1h_2) \in bH.$$

因此, $aH \subset bH$. 同样, 对任意$c \in bH$, 存在$h_3 \in H$ 使得$c = bh_3$. 进而,

$$c = a(b^{-1}a)^{-1}h_3 = a(h_1^{-1}h_2) \in aH.$$

因此, $bH \subset aH$. 故$aH = bH$.

同理可得, $Ha = Hb$ 的充要条件$ab^{-1} \in H$.

(iii) 由(ii) 知必要性成立. 再证充分性. 若不然, $aH \cap bH \neq \emptyset$, 则存在$c \in aH \cap bH$. 根据(i), 我们有$a^{-1}c \in H$ 及$b^{-1}c \in H$. 进而,

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

这与假设条件矛盾.

同理可得, $Ha \cap Hb = \emptyset$ 的充要条件$ab^{-1} \notin H$.

(iv) 因为$e,\ a^{-1} \in H$, 所以结论成立. 证毕

推论 设H 是群G 的子群. 则群G 可以表示为不相交的左(对应右)陪集的并集.

$$G = \bigcup_{i \in I} a_i H$$

类似于完全剩余类组成新集合, 左陪集全体也可组成新集合.

定义8.2.2 设H 是群G 的子群. 则H 在G 中不同左(对应右)陪集组成的新集合

$$\{aH \mid a \in G\}, \quad (\text{对应地}\ \{Ha \mid a \in G\},)$$

叫做H 在G 中的**商集**, 记作G/H.

$$G/H = \{aH \mid a \in G\} = \{a_i H \mid i \in I\}$$

G/H 中不同左(对应右)陪集的个数叫做H 在G 中的**指标**，记为$[G : H]$.

定理8.2.2 设H 是群G 的子群, 则

$$|G| = [G:H]|H|.$$

更进一步, 如果K, H 是群G 的子群, 且K 是H 的子群, 则

$$[G:K] = [G:H][H:K].$$

如果其中两个指标是有限的, 则第三个指标也是有限的.

证 根据定理8.2.1, 我们有

$$G = \bigcup_{i \in I} a_i H \quad \text{和} \quad |G| = \sum_{i \in I} |a_i H|.$$

因为H 到a_iH 的映射: $f: h \longrightarrow a_i h$ 是一一对应的, 所以$|a_iH| = |H|$. 进而,

$$|G| = \sum_{i \in I} |a_i H| = \sum_{i \in I} |H| = [G:H]|H|.$$

进一步, 如果K, H 是群G 的子群, 且K 是H 的子群, 根据定理8.2.1, 我们有 $G = \bigcup_{i\in I} a_i H$, $H = \bigcup_{j\in J} b_j K$,
其中$|I| = [G:H]$, $|J| = [H:K]$. 从而, $G = \bigcup_{i\in I}\bigcup_{j\in J}(a_i b_j)K$.
我们证明: $\{(a_i b_j)K\}$, $i \in I$, $j \in J$ 是不同的陪集. 假设

$$(a_i b_j)K = (a_{i'} b_{j'})K,$$

因为b_j, $b_{j'} \in H$, 上式两端右乘子群H, 得到 $a_i H = a_{i'} H$.
根据定理8.2.1 (ii), 我们得到$a_i = a_{i'}$. 从而, $b_j K = b_{j'} K$.
再根据定理8.2.1 (ii), 我们得到$b_i = b_{i'}$.
因此, 我们有

$$|G| = \sum_{i\in I}\sum_{j\in J} |(a_i b_j)K| = \sum_{i\in I}\sum_{j\in J} |K| = [G:H][H:K]|K|.$$

但我们有 $|G| = [G:K]|K|$.
故 $[G:K] = [G:H][H:K]$. 证毕

推论 (Lagrange). 设H 是有限群G 的子群, 则子群H 阶是$|G|$ 的因数.

8.2.2 陪集的进一步性质

下面考虑群G 的两个子群组成的集合.

设G 是一个群, H, K 是G 的子集. 我们用HK 表示集合

$$HK = \{hk \mid h \in H,\ k \in K.\}$$

如果写成加法, 我们用$H + K$ 表示集合

$$H + K = \{h + k \mid h \in H,\ k \in K.\}$$

例8.2.2 设H, K 是交换群G 的两个子群. 则HK 是G 子群.

证 对于$x, y \in HK$, 存在$h_1 \in H,\ k_1 \in K$ 以及$h_2 \in H,\ k_2 \in K$, 使得$x = h_1k_1$, $y = h_2k_2$, 从而,由G 是交换群, 有

$$xy^{-1} = (h_1k_1)(h_2k_2)^{-1} = (h_1k_1)(k_2^{-1}h_2^{-1}) = (h_1h_2^{-1})(k_1k_2^{-1}) \in HK,$$

因此, HK 是G 子群. 证毕

定理8.2.3 设H, K 是有限群G 的子群. 则$|HK| = |H||K|/|H \cap K|$.

证 因为$H \cap K$ 是H 的子群, 所以$|H \cap K| \mid |H|$. 令$n = \dfrac{|H|}{|H \cap K|}$, H 关于$H \cap K$ 的左陪集分解式为

$$H = h_1(H \cap K) \cup \cdots \cup h_n(H \cap K), \quad h_i \in H, \; h_i^{-1}h_j \notin K.$$

由于$(H \cap K)K = K$, 得到

$$\begin{aligned} HK &= (h_1(H \cap K) \cup \cdots \cup h_n(H \cap K))\, K \\ &= h_1(H \cap K)K \cup \cdots \cup h_n(H \cap K)K \\ &= h_1K \cup \cdots \cup h_nK. \end{aligned}$$

再证 $h_iK \cap h_jK = \emptyset$. 若不然, 则有$k_i, k_j \in K$ 使得

$$h_ik_i = h_jk_j,$$

从而$h_i^{-1}h_j = k_ik_j^{-1} \in K$, 矛盾.故 $|HK| = n|K| = |H||K|/|H \cap K|$.
证毕

定理8.2.4 设H, K 是群G 的子群. 则

$$[H : H \cap K] \leq [G : K].$$

如果$[G : K]$ 是有限的, 则$[H : H \cap K] = [G : K]$ 当且仅当$G = KH$.

证 考虑H 关于$H \cap K$ 的左陪集

$$H/H \cap K = \{h_i(H \cap K) \mid h_i \in H,\ h_i^{-1}h_j \notin H \cap K\},$$

以及G 关于K 的左陪集,

$$G/K = \{a_iK \mid a_i \in G,\ a_i^{-1}a_j \notin K\}.$$

作$H/H \cap K$ 到G/K 的映射

$$\varphi : h(H \cap K) \longrightarrow hK.$$

则φ 是单射. 事实上, 若有$h_iK = h_jK$, 则$h_i^{-1}h_j \in K$, $h_i^{-1}h_j \in H \cap K$, 矛盾. 故φ 是单射, 从而

$$[H : H \cap K] \leq [G : K].$$

假设$[G:K]$有限. 若$[H:H\cap K]=[G:K]$, 则单射φ也是满射. 即我们有

$$\{h_iK \mid h_i\in H, h_i^{-1}h_j\notin K\}=\{a_iK \mid a_i\in G, a_i^{-1}a_j\notin K\}.$$

因此, 对任意$x\in G$, 有$a_i\in G$以及$h_j\in H$使得

$$x\in xK=a_iK=h_jK\subseteq HK,$$

从而$G\subseteq HK, G=HK$.
反之,若$G=HK$,则对任意左陪集$a_iK\ (a_i\in G)$, 有

$$a_i=h_jk, \quad (h_j\in H,\ k\in K).$$

从而

$$\varphi(h_j(H\cap K))=h_jK=h_jkK=a_iK.$$

φ是满射, 故

$$[H:H\cap K]=[G:K].$$

定理成立. 证毕

定理8.2.5 设H, K 是群G 的有限指标子群. 则$[G:H\cap K]$ 是有限的, 且

$$[G:H\cap K]\le [G:H][G:K].$$

进一步, $[G:H\cap K]=[G:H][G:K]$ 当且仅当$G=HK$.

证 因为$H\cap K\le H\le G$, 所以

$$[G:H\cap K]=[G:H][H:H\cap K].$$

又因为$[G:H]$与$[G:K]$都有限, 故由定理4知,

$$[H:H\cap K]\le [G:K].$$

于是$[G:H\cap K]\le [G:H][G:K]$. 因为

$$[G:H\cap K]=[G:H][G:K]\Leftrightarrow [H:H\cap K]=[G:K],$$

而由定理8.2.4, 知$[H:H\cap K]=[G:K]\Leftrightarrow G=HK$, 故

$$[G:H\cap K]=[G:H][G:K]\Leftrightarrow G=HK.$$

定理成立. 证毕

8.2.3 正规子群和商群

最后, 讨论商集G/H 构成一个群的条件(H 为正规子群).

定理8.2.6 设N 是群G 的子群, 则如下条件是等价的:

(i) 对任意$a \in G$, 有$aN = Na$;

(ii) 对任意$a \in G$, 有$aNa^{-1} = N$.

(iii) 对任意$a \in G$, 有$aNa^{-1} \subset N$, 其中$a\,N\,a^{-1} = \{a\,n\,a^{-1} \mid n \in N\}$.

证 易知, (i) 蕴含(ii) 及(ii) 蕴含(iii) 是显然的.

现在从(iii) 推出(i). 对任意$a \in G,\ n \in N$, 因为$a\,n\,a^{-1} \in a\,N\,a^{-1} \subset N$, 所以$a\,n\,a^{-1} = n',\ \ n' \in N$. 进而, $a\,n = n'\,a \in Na$ 及$aN \subset Na$. 特别, 也有$a^{-1}N \subset Na^{-1}$ 或$Na \subset aN$. 故$aN = Na$. 定理成立. 证毕

定义8.2.3 设N 是群G 的子群. 称N 为群G 的**正规子群**, 如果它满足定理8.2.6 的条件.

定理8.2.7 设N 是群G 的正规子群, G/N 是由N 在G 中的所有(左)陪集组成的集合. 则对于结合法

$$(aN)(bN) = (a\,b)N,$$

G/H 构成一个群.

证 首先, 要证明结合法的定义不依赖于陪集的代表元选择. 即要证明: $aN = a'N, bN = b'N$时, $(a\,b)N = (a'\,b')N$. 事实上, 根据定理**??**, 我们有

$$(a\,b)N = a(bN) = a\,(b'N) = a(Nb') = (aN)b' = (a'N)b' = (a'\,b')N.$$

其次, $eN = N$ 是单位元. 事实上, 对任意$a \in G$, 有

$$(aN)(eN) = (a\,e)N = aN, \quad (eN)(aN) = (e\,a)N = aN.$$

最后, aN 的逆元是$a^{-1}N$. 事实上,

$$(aN)(a^{-1}N) = (a\,a^{-1})N = eN, \quad (a^{-1}N)(aN) = (a^{-1}\,a)N = eN.$$

因此, G/H 构成一个群. 证毕

定理8.2.7 中的群叫做群G 对于正规子群H 的**商群**.

如果群G 的运算写作加法, 则G/N 中的运算写作 $(a + N) + (b + N) = (a + b) + N$.

8.3 同态和同构

本节讨论两个群之间的关系: 同态与同构.

8.3.1 基本概念

定义8.3.1 设G, G' 都是群, f 是G 到G' 的一个映射. 如果对任意的a, $b \in G$, 都有

$$f(a\,b) = f(a)\,f(b),$$

那么, f 叫做G 到G' 的一个**同态**.

注 同态可称作保持运算的映射:

$$f(\underbrace{a \cdot b}_{G\text{中运算}}) = \underbrace{f(a)\,f(b)}_{G'\text{中运算}}.$$

如果f 是一对一的, 则称f 为**单同态**; 如果f 是满的, 则称f 为**满同态**; 如果f 是一一对应的, 则称f 为**同构**.

当$G = G'$ 时, 同态f 叫做**自同态**, 同构f 叫做**自同构**.

性质8.3.1 设G, G', G'' 都是群, f 是G 到G' 的一个同态映射, g 是G' 到G'' 的一个同态映射, 那么, $g\circ f$ 是G 到G'' 的同态映射. 而且, 当f 是G 到G' 的一个同构映射, g 是G' 到G'' 的一个同构映射, 那么, $g\circ f$ 是G 到G'' 的同构映射.

证 对任意的a, $b\in G$, 因为f, g 都是同态映射, 所以

$$(g\circ f)(a\,b) = g(f(a\,b)) = g(f(a)f(b)) = g(f(a))g(f(b)) = (g\circ f)(a)(g\circ f)(b)$$

因此, $g\circ f$ 是G 到G'' 的同态.

进一步, 当f 是G 到G' 的一个同构映射, g 是G' 到G'' 的一个同构映射, 有f 是G 到G' 的一一对应映射, g 是G' 到G'' 的一一对应映射, 从而, $g\circ f$ 是G 到G'' 的一一对应映射. 故$g\circ f$ 是G 到G'' 的同构映射. 证毕

定义8.3.2 我们称G 与G' **同构**, 如果存在一个G 到G' 的同构. 记作$G \cong G'$.

注 在同构的意义下, 两个同构的群可以看作相同的, 即我们可以通过已知的群的性质来研究另一个群的性质(如循环群, 定理9.1.2), 还可提高计算效率(如例5.1.9):

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

定理8.3.1 设f 是群G 到群G' 的一个同态. 则

(i) $f(e) = e'$, 即同态将单位元映到单位元.

(ii) 对任意$a \in G$, $f(a^{-1}) = f(a)^{-1}$, 即同态将a 的逆元映到$f(a)$ 的逆元.

(iii) $\ker f = \{a \mid a \in G,\ f(a) = e'\}$ 是G 的子群, 且f 是单同态的充要条件是

$$\ker f = \{e\}.$$

(iv) $f(G) = \{f(a) \mid a \in G\}$ 是G' 的子群, 且f 是满同态的充要条件是$f(G) = G'$.

(v) 设H' 是群G' 的子群, 则集合$f^{-1}(H') = \{a \in G \mid f(a) \in H'\}$ 是G 的子群.

证 (i) 因为$f(e)^2 = f(e^2) = f(e)$, 此式两端同乘$f(e)^{-1}$, 得到$f(e) = e'$. 结论成立.

(ii) 因为$f(a^{-1})\,f(a) = f(a^{-1}\,a) = f(e) = e'$, $f(a)\,f(a^{-1}) = f(a\,a^{-1}) = e'$, 所以$f(a^{-1}) = f(a)^{-1}$.

(iii) 对任意$a,\ b \in \ker f$, 有$f(a) = e',\ f(b) = e'$. 从而,

$$f(a\,b^{-1}) = f(a)\,f(b^{-1}) = f(a)\,f(b)^{-1} = e'.$$

因此, $a\,b^{-1} \in \ker f$. 根据定理8.1.2, $\ker f$ 是G 的子群.
若f 是单同态, 则满足$f(a) = e' = f(e)$ 的元素只有$a = e$. 因此, $\ker f = \{e\}$.
反过来, 设$\ker f = \{e\}$. 则对任意的$a,\ b \in G$ 使得$f(a) = f(b)$, 有

$$f(a\,b^{-1}) = f(a)\,f(b^{-1}) = f(a)\,f(b)^{-1} = e'.$$

这说明, $ab^{-1} \in \ker f = \{e\}$ 或$a = b$. 因此, f 是单同态.
(iv) 对任意$x,\ y \in f(G)$, 存在$a,\ b \in G$ 使得$f(a) = x,\ f(b) = y$. 从而,

$$x\,y^{-1} = f(a)\,f(b)^{-1} = f(a\,b^{-1}) \in f(G).$$

根据定理8.1.2, $f(G)$ 是G' 的子群, 且f 是满同态的充要条件是$f(G) = G'$.

(v) 对任意$a, b \in f^{-1}(H')$, 根据(ii) 及H' 为子群, 我们有

$$f(a\,b^{-1}) = f(a)\,f(b^{-1}) = f(a)\,f(b)^{-1} \in H',$$

因此, $a\,b^{-1} \in f^{-1}(H')$. $f^{-1}(H')$ 是G 的子群. 证毕

$\ker f$ 叫做同态f 的**核子群**, $f(G)$ 叫做**像子群**.

例8.3.1 加群$\mathbf{Z}$ 到乘群$G =< g >= \{g^n \mid n \in \mathbf{Z}\}$ 的映射

$$f : n \longmapsto g^n$$

是$\mathbf{Z}$ 到$< g >$ 的一个同态.
事实上, 对任意的$a, b \in \mathbf{Z}$, 我们有

$$f(a+b) = g^{a+b} = g^a \cdot g^b = f(a)f(b).$$

例8.3.2 加群$\mathbf{R}$ 到乘群$\mathbf{R}^* = \mathbf{R} \setminus \{0\}$ 的映射$f : a \longmapsto e^a$ 是$\mathbf{R}$ 到$\mathbf{R}^*$ 的一个同态.
事实上, 对任意的$a, b \in \mathbf{R}$, 我们有

$$f(a+b) = e^{a+b} = e^a \cdot e^b = f(a)f(b).$$

例8.3.3 加群$\mathbf{Z}$ 到加群$\mathbf{Z}/n\mathbf{Z}$ 的映射$f : k \longmapsto k + n\mathbf{Z}$ 是一个同态.

例8.3.4 加群$\mathbf{Z}$ 到乘群$G = \{\theta^k \mid \theta = e^{\frac{2\pi i}{n}},\ k \in \mathbf{Z}\}$ 的映射$f : k \longmapsto \theta^k$ 是一个同态.

例8.3.5 加群$\mathbf{Z}/n\mathbf{Z}$ 到乘群$G = \{\theta^k \mid \theta = e^{\frac{2\pi i}{n}},\ k = 0,\ 1,\ \ldots, n-1\}$ 的映射

$$f : k + n\mathbf{Z} \longmapsto \theta^k$$

是一个同构.

例8.3.6 设a 是群G 的一个元. 那么映射

$$f : b \longmapsto a\,b\,a^{-1}$$

是G 自同态. 事实上,

$$f(b\,c) = a\,(b\,c)\,a^{-1} = (a\,b\,a^{-1})\,(a\,c\,a^{-1}) = f(a)\,f(b).$$

8.3.2 同态分解定理

在群的研究中, 我们有时是借助于与之同构的群来进行研究(见定义8.3.2 及其注). 这就需要我们构造相应的同构. 但直接构造同构并不是很容易的事, 因此我们通常是构造同态, 再借助于如下同态分解定理(定理8.3.3)来诱导出同构映射.

定理8.3.2 设f 是群G 到群G' 的同态, 则f 的核$\ker(f)$ 是G 的正规子群. 反过来, 如果N 是群G 的正规子群, 则映射

$$\begin{aligned} s: G &\longrightarrow G/N \\ a &\longmapsto aN \end{aligned}$$

是核为N 的同态.

证 对任意$a \in G$, $b \in \ker f$, 我们有

$$f(a\,b\,a^{-1}) = f(a)\,f(b)\,f(a^{-1}) = f(a)\,e'\,f(a)^{-1} = e'.$$

这说明$a\,b\,a^{-1} \in \ker f$. 根据定理8.2.6, $\ker(f)$ 是G 的正规子群.
反过来, 设N 是群G 的正规子群, 则G 到G/N 的映射s 满足:

$$s(a\,b) = (a\,b)N = (aN)\,(bN) = s(a)\,s(b),$$

同时, $s(a) = N$ 的充分必要条件是$a \in N$. 因此, s 是核为N 的同态.
证毕

映射$s : G \longrightarrow G/N$ 称为G 到G/N **自然同态**.

定理8.3.3 (同态分解) 设f 是群G 到群G' 的同态, 则存在惟一的$G/\ker(f)$ 到像子群$f(G)$ 的同构$\overline{f} : a\ker(f) \longmapsto f(a)$ 使得$f = i \circ \overline{f} \circ s$, 其中$s$ 是群G 到商群$G/\ker(f)$ 的自然同态, $i : c \longmapsto c$ 是$f(G)$ 到G' 的恒等同态. 即有如下的交换图:

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \mathrm{s}\downarrow & & \uparrow\mathrm{i} \\ G/\ker(f) & \xrightarrow{\overline{f}} & f(G) \end{array}$$

证 根据定理8.3.2, $\ker(f)$ 是G 的正规子群, 所以存在商群$G/\ker(f)$. 现在要证明: $\overline{f} : a\ker(f) \longmapsto f(a)$ 是$G/\ker(f)$ 到像子群$f(G)$ 的同构.

首先, $\overline{f}$ 是$G/\ker(f)$ 到$f(G)$ 的同态. 事实上, 对任意的$a\ker(f),\ b\ker(f) \in G/\ker(f)$,

$$\overline{f}((a\ker(f))(b\ker(f)) = \overline{f}((ab)\ker(f))$$

$$= f(ab) = f(a)f(b) = \overline{f}(a\ker(f))\overline{f}(b\ker(f)).$$

访问主页
标题页
目录页
第64页共73页
返回
全屏显示
关闭
退出

其次, $\overline{f}$ 是一对一. 事实上, 对任意$a\ker(f) \in \ker(\overline{f})$, 有$\overline{f}(a\ker(f)) = f(a) = e'$. 由此, $a \in \ker(f)$ 以及$a\ker(f) = \ker(f)$.

最后, $\overline{f}$ 是满同态. 事实上, 对任意$c \in f(G)$, 存在$a \in G$ 使得$f(a) = c$. 从而, $\overline{f}(a\ker(f)) = f(a) = c$. 即$a\ker(f)$ 是c 的像源.

因此, $\overline{f}$ 是同构, 并且有$f = i \circ \overline{f} \circ s$. 事实上, 对任意$a \in G$, 有

$$i \circ \overline{f} \circ s(a) = i(\overline{f}(s(a))) = i(\overline{f}(a\ker(f))) = i(f(a)) = f(a).$$

假如还有同构$g : G/\ker(f) \longrightarrow f(G)$ 使得$f = i \circ g \circ s$, 则对任意$a\ker(f) \in G/\ker(f)$, 我们有

$$g(a\ker(f)) = i(g(s(a))) = (i \circ g \circ s)(a) = f(a) = \overline{f}(a\ker(f)).$$

因此, $g = \overline{f}$. 证毕

8.3.3 同态分解定理的进一步性质

定理8.3.4 设K 是群G 的正规子群, H 是G 的包含K 的子群. 则$\overline{H} = H/K$ 是商群$\overline{G} = G/K$ 的子群, 且映射$H \longmapsto \overline{H}$ 是G 的包含K 的子群集到$\overline{G}$ 的子群集的一一对应. $H(\supset K)$ 是G 的正规子群当且仅当$\overline{H}$ 是$\overline{G}$ 的正规子群. 这时,

$$\frac{G}{H} \cong \frac{\overline{G}}{\overline{H}} = \frac{G/K}{H/K}.$$

证 首先证明$\overline{H} = H/K$ 是商群$\overline{G} = G/K$ 的子群. 因为K 是群G 的正规子群,所以对于任意$h \in H \subseteq G$, 有$hK = Kh$, 因而K 是群H 的正规子群, $\overline{H} = H/K$ 是商群. 又对于任意$h_1K, h_2K \in H/K$, 有$(h_1K)(h_2K)^{-1} = (h_1K)(h_2^{-1}K) = (h_1h_2^{-1})K \in H/K$,所以$\overline{H} = H/K$ 是商群$\overline{G} = G/K$ 的子群.

其次, 证明映射$H \longmapsto \overline{H}$ 是G 的包含K 的子群集到$\overline{G}$ 的子群集的一一对应.

a) 映射是一对一的. 假设H_1, H_2 使得$H_1K = H_2K$, 则对任意$h_1 \in H_1$, 有$h_1K \in H_1K = H_2K$, 因此存在$h_2 \in H_2$, 使得$h_1K = h_2K$. 从而$h_2^{-1}h_1 \in K$, $h_1 = h_2k \in H_2$ 以及$H_1 \subseteq H_2$. 同理, 也有$H_2 \subseteq H_1$. 故$H_1 = H_2$.

b) 映射是满的. 假设$\overline{H}$ 是$\overline{G}$ 的子群, 则$\overline{H}$ 是一些陪集a_iK (包括逆元$a_i^{-1}K$) 组成的集合

$$\overline{H} = \{a_iK \mid a_i \in G, i \in I\}.$$

取这些陪集的并集为

$$H = \bigcup_{i \in I} a_iK.$$

对任意h_1, $h_2 \in H$, 有h_1K, $h_2^{-1}K \in \overline{H}$ 以及

$$(h_1h_2^{-1})K = (h_1K)(h_2^{-1}K) \in \overline{H},$$

从而$h_1h_2^{-1} \in H$. 因此H 是G 的子群, 也是$\overline{H}$ 的像源.

再次, 证明$H(\supset K)$ 是G 的正规子群当且仅当$\overline{H}$ 是$\overline{G}$ 的正规子群. 必要性是显然的. 现证充分性. 对任意$h \in H$, 以及任意$g \in G$, 有$(hgh^{-1})K = (hK)(gK)(h^{-1}K) \in \overline{H}$, 所以$hgh^{-1} \in H$, H 为G 的正规子群.

最后, 构造G 到$\overline{G}/\overline{H}$ 的同态f. 因为H 为G 的正规子群时, $\overline{H}$ 为$\overline{G}$ 的正规子群, 因而有商群$\overline{G}/\overline{H}$. 考虑$G$ 到G/K 的自然同态s_1 与$\overline{G} = G/K$ 到$\overline{G}/\overline{H}$ 的自然同态s_2 的复合$f = s_2 \circ s_1$:

$$\underbrace{\begin{array}{ccccc} G & \xrightarrow{s_1} & G/K & \xrightarrow{s_2} & \overline{G}/\overline{H} \\ a & \longmapsto & aK & \longmapsto & (aK)\overline{H} = a\overline{H} \end{array}}_{f=s_2\circ s_1:\ a\ \longmapsto\ a\overline{H}}$$

显然, f 是同态, 因为f 是同态映射的复合. 再证$\ker(f) = H$. 对任意$a \in \ker(f)$, 有$(aK)\overline{H} = a\overline{H} = \overline{H}$, 存在$h \in H$, 使得$aK = hK$, 因而有$a = hk \in H$, $\ker(f) = H$. 根据同态分解定理8.3.3, 知

$$\frac{G}{H} \cong \frac{\overline{G}}{\overline{H}} = \frac{G/K}{H/K}.$$

证毕

定理8.3.5 设H 是群G 的子群, K 是G 的正规子群. 则$HK = \{hk \mid h \in H, k \in K\}$ 是G 的包含K 的子群, $H \cap K$ 是H 的正规子群, 且映射

$$h(H \cap K) \longrightarrow hK, \quad h \in H$$

是$H/H \cap K$ 到HK/K 的同构.

证 对于任意$h_1, h_2 \in H$, $k_1, k_2 \in K$, 因为K 是G 的正规子群, 所以$h_2(k_1k_2^{-1})h_2^{-1} \in K$, 从而

$$(h_1k_1)(h_2k_2)^{-1} = (h_1h_2^{-1})(h_2(k_1k_2^{-1})h_2^{-1}) \in HK$$

因此, HK 是G 的子群, 且K 是HK 的正规子群.

作映射H 到HK/K 的映射$f: h \longmapsto hK$. 则f 是同态. 事实上, 对于任意$h_1, h_2 \in H$, 有$f(h_1h_2) = (h_1h_2)K = (h_1K)(h_2K) = f(h_1)f(h_2)$.

再证$\ker(f) = H \cap K$. 假设$h \in \ker(f)$, 则$hK = K$. 因此, $h \in K$ 以及$h \in H \cap K$. 故$\ker(f) = H \cap K$, $H \cap K$ 是H 的正规子群. 根据同态分解定理8.3.3, 我们有同构$\overline{f}$

$$\overline{f}: h(H \cap K) \longrightarrow hK, \quad h \in H.$$

证毕

访问主页
标题页
目录页
第 69 页 共 73 页
返回
全屏显示
关闭
退出