第 5 章 群论初步

从本章起开始讲述群、环、域、格等代数对象的基本性质，它是学习和研究理论计算机科学不可缺少的工具.

今后我们主要研究对象不是代数结构中的元素特性，而是各种代数结构本身和不同代数结构之间的相互联系(同态). 掌握其中体现的丰富的数学思想和方法，比背诵定义和名词要重要得多.

5.1 群的定义与简单性质

定义 5.1. G是非空集合，$*$是G上的乘法运算，如果他们满足如下要求：

1° G对于乘法$*$是封闭的，即$\forall a,b\in G$，$a*b\in G$；

2° 对$\forall a,b,c\in G$，$a*(b*c)=(a*b)*c$. $*$满足结合律；

3° 存在$e\in G$，$\forall a\in G$，$e*a=a*e=a$. e称为单位元；

4° $\forall a\in G$，存在$a'\in G$，使得$a'*a=a*a'=e$. a'称为a的逆元.

那么G连同$*$称为一个**群**，记为$\langle G,*\rangle$.

如果只满足1°，2°，则称$\langle G,*\rangle$为**半群**.

如果只满足1°，2°，3°，则称$\langle G,*\rangle$为带1半群.

定义 5.2. 在群$\langle G,*\rangle$中，如果对任意$a,b\in G, a*b=b*a$，则称$\langle G,*\rangle$为**交换群**(或称为**阿贝尔群**).

例 5.1. A是非空集合. $\langle\mathscr{P}(A),\cup\rangle$是带1半群. $\varnothing\in\mathscr{P}(A)$是单位元.

例 5.2. 字母表Σ上的所有非空字组成集合Σ^+，对于字的连接运算$\bullet$构成半群$\langle\Sigma^+,\bullet\rangle$.

例 5.3. 有理数集合Q，在普通加法运算下形成交换群$\langle Q,+\rangle$. 其单位元为0，每个元素的逆元就是它的负数.

例 5.4. 非零实数集合R^*，在普通乘法运算下形成交换群$\langle R^*,\bullet\rangle$. 其单位元为1. 每个元素的逆元就是它的倒数.

例 5.5. 令$G=\{1,-1,\mathrm{i},-\mathrm{i}\}$，对于复数乘法构成的有限交换群$\langle G,*\rangle$. G中的任意两个元素的乘积可用下面的群表示.

$*$	1	-1	i	$-\mathrm{i}$
1	1	-1	i	$-\mathrm{i}$
-1	-1	1	$-\mathrm{i}$	i
i	i	$-\mathrm{i}$	-1	1
$-\mathrm{i}$	$-\mathrm{i}$	i	1	-1

例 5.6. 令$Z_n=\{[0],[1],\cdots,[n-1]\}$，其中$[i]$是模$n$同余$i$的所有整数构成的集合，规定$Z_n$上的$+$运算，$[a]+[b]=[a+b]$. 由模$n$同余定义知，如果$[a_1]=[a_2]$，$[b_1]=[b_2]$，那么$[a_1+b_1]=[a_2+b_2]$，即同余类的加法定义与同余类的代表元选取无关，所以这样的加法定义是确定的，我们称它是“可定义”的. 不难验证$\langle Z_n,+\rangle$是交换群，$[0]$是他的单位元，$[a]$的逆元是$[-a]$.

根据群的定义，我们可以定义群G中元素的方幂

$$a^n=\overbrace{a*a*\cdots*a}^{n}$$

显然$a^m*a^n=a^{m+n}$，$(a^m)^n=a^{m*n}$. 如果将G中元素a的逆元$a^{'}$记为a^{-1}，那么

$$a*a^{'}=a*a^{-1}=a^0,$$

即$a^0=e$. 显然$a^{-n}=(a^{-1})^n=(a^{'})^n$.

在群$\langle G,*\rangle$中的运算$*$不一定满足交换律. 当运算$*$满足交换律时，一般写作“$+$”. 群的单位元称为零元，元素的逆元称为负元. 在交换群中，

$$\begin{aligned}na&=\overbrace{a+a+\cdots+a}^{n},\\ ma+na&=(m+n)a,\\ m(na)&=(m\cdot n)a.\end{aligned}$$

定理 5.1. 在群$\langle G,*\rangle$中，左消去律和右消去律成立，即$\forall a,b\in G$，如果$a*b=a*c$，则必有$b=c$，如果$b*a=c*a$，则必有$b=c$.

证明: 如果$a*b=a*c$，由群定义中4°知，G中每个元素都有逆元. 令元素a的逆元为$a^{'}$. 我们用$a^{'}$左乘这个等式，

$$a^{'}*(a*b)=a^{'}*(a*c)$$

又由群定义中的2°知，运算*满足结合律，得到$(a^{'}*a)*b=(a^{'}*a)*c$. 从逆元的定义和单位元e的定义知$a^{'}*a=e$，$e*b=b$，$e*c=c$，于是最后得到$b=c$. 这表明在群G的等式中可以消去等式两边最左的公因子，即左消去律成立.

同理可以证明右消去律成立.

定理 5.2. 在群$\langle G,*\rangle$中，方程$a*x=b$与$y*a=b$有唯一解.

证明: 令$x=a^{'}*b$代入方程$a*x=b$中，使得

$$a*(a^{'}*b)=(a*a^{'})*b=e*b=b$$

它说明$x=a^{'}*b$是方程$a*x=b$的解.

现假设x_1和x_2都是方程$a*x=b$的解，即$a*x_1=b$，$a*x_2=b$. 于是有$a*x_1=a*x_2$，利用左消去律可得$x_1=x_2$. 这就是说如果方程$a*x=b$有两个解，那么它们必须相等.

综上知在群$\langle G,*\rangle$中方程$a*x=b$有解，并且解是唯一的.

同理可以证明方程$y*a=b$有唯一解.

定理 5.3. 群$\langle G,*\rangle$中单位元和逆元是唯一的.

证明: 假设e_1和e_2都是群G的单位元. 因为e_1是单位元，$\forall a\in G$，$a*e_1=a$，特别取$a=e_2$，那么$e_2*e_1=e_2$. 又因e_2是单位元，$\forall a\in G$，$e_2*a=a$. 特别取$a=e_1$，那么$e_2*e_1=e_1$. 从而$e_1=e_2$，即群G的单位元是唯一的.

假设$a_1,a_2\in G$都是a的逆元. 由逆元定义知$a_1*a=e$，$a_2*a=e$，即$a_1*a=a_2*a$. 再用右消去律得到$a_1=a_2$，即群G中元素a的逆元是唯一的.

定理 5.4. 在群$\langle G,*\rangle$中，$\forall a,b\in G$，则有

1° $(a^{'})^{'}=a$;

2° $(a*b)^{'}=b^{'}*a^{'}$.

证明:

1° $(a^{'})^{'}$是$a^{'}$的逆元，$a^{'}$是a的逆元，由逆元的定义知$(a^{'})^{'}*a^{'}=e$，$a*a^{'}=e$，即$(a^{'})^{'}*a^{'}=a*a^{'}$. 由右消去律知$(a^{'})^{'}=a$.

2° $(a*b)*(b^{'}*a^{'})=a*(b*b^{'})*a^{'}=a*a^{'}=e$,

$(b^{'}*a^{'})*(a*b)=b^{'}*(a^{'}*a)*b=b^{'}*b=e$.

由逆元的唯一性知$(a*b)^{'}=b^{'}*a^{'}$.

注意，在群中乘积求逆满足脱衣规则.

定义 5.3. 在群$\langle G,*\rangle$中，G是有限集合，则称$\langle G,*\rangle$是**有限群**，其阶数为$|G|$.

定义 5.4. 在群$\langle G,*\rangle$中，$a\in G$，如果存在n，它是满足$a^n=e$的最小正整数，则称元素a是n**阶**的. 如果那样的n不存在，则称元素a是**无限阶**的.

我们考虑集合A，其中$a\in G$，Z^*为非零整数集合

$$A=\{i|i\in Z^*,\ a^i=e\}.$$

当$A=\varnothing$时，a是无限阶元. 当$A\neq\varnothing$时，那么A中必有正整数. (这是因为如果$-m<0$，且$-m\in A$即$a^{-m}=e$，那么必有$a^m=e$，即$m>0$且$m\in A$.)这时a是有限阶的，其阶数是A中的最小正整数n. 集合A有如下性质:

1° 若$m,l\in A$，则$m\pm l\in A$.

2° 若$m\in A,c\in Z^*$，则$cm\in A$.

不难证明:

$$A=\{kn|k\in Z^*\}.$$

也就是说，如果$a^m=e$，那么m必是元素a阶的整数倍数.

例 5.7. 在整数加群$\langle Z,+\rangle$中，除零元0的阶为1以外，所有元素的阶都是无限的.

例 5.8. 模6同余类群$\langle Z_6,+\rangle$中，[0]是1阶元，[1],[5]是6阶元，[2],[4]是3阶元，[3]是2阶元.

例 5.9. 在群$\langle G,*\rangle$中，$a,b\in G$，它们分别是m阶、n阶元，$(m,n)=1$. 如果$a*b=b*a$，则$a*b$是$m\cdot n$阶元.

证明： 设$a*b$的阶为k，

$$(a*b)^{mn}=a^{mn}*b^{mn}=(a^m)^n*(b^n)^m=e*e=e,$$

得知$k|mn$.

由于$a*b$的阶是k，$(a*b)^k=e$，

$$e=(a*b)^{km}=(a^m)^k*(b^k)^m=b^{km}.$$

因为b的阶为n，故$n|km$，又由$(m,n)=1$知$n|k$. 同理可以证明$m|k$. 从而$[m,n]|k$，即$mn|k$.

综上知$k=m\cdot n$.

5.2 群定义的进一步讨论

本节介绍群的几个等价的定义，从而更进一步探讨群的性质.

定理 5.5. G是非空集合，$*$是G上的运算. 如果

(1) $\forall a,b\in G,a*b\in G$;

(2) $\forall a,b,c\in G,a*(b*c)=(a*b)*c$;

(3) 存在$e_r\in G$，对一切$a\in G$, $a*e_r=a$. e_r称为右单位元;

(4) $\forall a\in G$，存在$a'\in G$使得$a*a'=e_r$. a'称为a的右逆，那么$\langle G,*\rangle$为群.

证明： 对照定义5.1，我们只要证明右单位元一定是左单位元，右逆一定是左逆.

先证右逆一定是左逆，即已知$a*a'=e_r$，证明$a'*a=e_r$. 现设a''是a'的右逆，$a'*a''=e_r$.

$$a'*a=(a'*a)*e_r=(a'*a)*(a'*a'')=e_r.$$

a'也是a的左逆.

再证右单位元一定是左单位元，a'是a的逆元

$$e_r * a = (a * a') * a = a * (a' * a) = a * e_r = a.$$

定理 5.6. G是非空集合，$*$是G上的运算，如果

(1) $\forall a, b \in G, a * b \in G$;

(2) $\forall a, b, c \in G, (a * b) * c = a * (b * c)$;

(3) $\forall a, b \in G$，方程$a * x = b$和$y * a = b$在G中都有解. 那么$\langle G, * \rangle$为群.

证明: 与定理5.5比较，我们要证明从(3)推出G中有右单位元并且任意元素均有右逆.

由(3)知方程$a * x = a$在G中有解，我们选取其中一个解记为e_r，即$a * e_r = a$. 任取G的任意元素b，由(3)知$y * a = b$在G中有解，我们选取一个解记为d，即$d * a = b$. 那么

$$b * e_r = (d * a) * e_r = d * (a * e_r) = d * a = b.$$

这说明e_r是G的右单位元. 又由(3)知$a * x = e_r$在G中有解，并记为a'，即$a * a' = e_r$，那么a'是a的右逆.

定理5.5和定理5.6是与定义5.1等价的两个群定义. 它们的等价性证明过程图5.1所示.

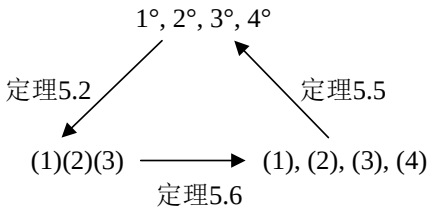

图 5.1: 等价性证明过程

定理 5.7. G是非空集合，$*$是G上的运算. 如果

1° $\forall a, b \in G, a * b \in G$;

2° $\forall a, b, c \in G, (a * b) * c = a * (b * c)$;

3° $\forall a \in G$，$a * x_1 = a * x_2$推出$x_1 = x_2$，并且$\forall a \in G, y_1 * a = y_2 * a$推出$y_1 = y_2$. 那么$\langle G, * \rangle$为群.

证明： 令$G=\{a_1,a_2,\cdots,a_n\}$. 任取G中的元素a，用a左乘G中的每个元素，所有乘积构成一个集合G'，

$$G'=\{a*a_1,a*a_2,\cdots,a*a_n\}.$$

由1°知$a*a_i\in G$，$1\le i\le n$，即$G'\subseteq G$. 又由3°知当$i\ne j$时，$a*a_i\ne a*a_j$，于是$|G'|=|G|=n$. 显然得出$G=G'$. 这表明任取G的元素a，b，方程$a*x=b$均有解.

同样，考虑$G''=\{a_1*a,a_2*a,\cdots,a_n*a\}$，可以证明任取$G$的元素$a$，$b$，方程$y*a=b$均有解.

由定理5.6知$\langle G,*\rangle$为群.

在定理5.1中指出，群中左、右消去律成立. 在定理5.7中，如果非空集合G上的运算满足封闭性、结合律和左右消去律，那么该代数结构是群. 也就是说，当G是有限集合时. 定义5.1的1°，2°，3°，4°与定理5.7的中1°，2°，3°是等价的. 从而定理5.7可以看成有限群的定义.

一个有限群的乘法可以用一个群表来表示. 群的一些性质可以从群表(5.1节例5.5)上直接看出：由于存在单位元，表中有一行与横线边上的元素一样，表里有一列与竖线左边的元素一样. 又由消去律知，全体元素必在每行出现一次，必在每列出现一次. 下面我们来看几个低阶群.

1阶群$G_1,|G_1|=1$. 由于群必有单位元e，故$G_1=\{e\}$. 2阶群$G_2,|G_2|=2$. G_2中除去单位元之外还有一个元素a. $G_2=\{e,a\},a\ne e$. 由于运算$*$的封闭性，$a*a\in\{e,a\}$. 假设$a*a=a$. 由$a*e=a$推出$a=e$，矛盾，故不可. 所以$a*a=e$. G_1和G_2的乘法表如下

$*$	e
e	e

G_1

$*$	e	a
e	e	a
a	a	e

G_2

3阶群$G_3=\{e,a,b\},a\ne b,a,b\ne e,a*a$不能是$a$或$e$，否则推出$a=e$，所以$a*a=b$. 再根据每个元素在一行或一列中出现且只出现一次，得到$a*b=e,b*a=e,b*b=a$. 我们看到元素$b=a*a=a^2$，$e=b*a=a^3$，从而$G_3=\{e,a,a^2\}$，并且a是3阶元，$a^3=e$. 4阶群在同构的意义下只有两

个: $C_4 = \{e, a, a^2, a^3\}$且$a^4 = e$, $K_4 = \{e, a, b, c\}$且$a^2 = b^2 = c^2 = e$. 3阶群G_3和4阶群C_4, K_4的乘法表如下.

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

G_3

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

C_4

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

K_4

例 5.10. 设G是有限群, 则G的每个元素的阶必是有限的.

证明: 群G的单位元e显然是1阶元. 若$a \in G$且$a \neq e, a, a^2, a^3, \cdots, a^n, \cdots \in G$. 由于$G$是有限集合, 必然存在$i > j$, $a^i = a^j$. 等式两边同时乘以a^j的逆元$(a^j)'$,

$$a^i * (a^j)' = a^j * (a^j)' = e.$$

由$a^i = a^{i-j} * a^j$及$*$运算的结合律得到

$$a^{i-j} = e, i - j > 0.$$

那么$i - j$是上节末才提到的集合$A = \{k | k \in Z^*, a^k = e\}$的元素$A \neq \varnothing$, 这表明元素$a$是有限阶元, 其阶数是$A$中的最小正整数.

下面再给出两个非交换群的例子.

例 5.11. 全体n阶有理数方阵记为Q_n. 令$G = \{A | A \in Q_n, |A| \neq 0\}$. G对于矩阵乘法$\bullet$构成群. 若$A, B \in G$, 即$|A|, |B| \neq 0$, 而$|A \bullet B| = |A| \bullet |B| \neq 0$, 则$A \bullet B \in G$. 乘法$\bullet$在$G$中是封闭的. 矩阵乘法是可结合的.

$$I_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

是G的单位元. 当$A \in G$时, $|A| \neq 0$, A有逆矩阵A^{-1}, 且$|A^{-1}| \neq 0$, 即$A^{-1} \in G$, 且$A \bullet A^{-1} = I_n$, 故A^{-1}是A在G中的逆元. 所以$\langle G, \bullet \rangle$为群. 由于矩阵乘法是非交换的, 于是$\langle G, \bullet \rangle$为非交换群.

例 5.12. Q是有理数集合. 令

$$G = \{f_{a,b} | f_{a,b} : Q \to Q, f_{a,b}(x) = ax + b, a \neq 0, a, b \in Q\}.$$

G对于映射的合成运算构成群. 若$f_{a,b}, f_{c,d} \in G$，其中$f_{a,b}(x) = ax + b, f_{c,d}(x) = cx + d$，且$a, c \neq 0, a, b, c, d \in Q$.

$$(f_{a,b} \circ f_{c,d})(x) = f_{a,b}(cx + d) = a(cx + d) + b = f_{ac,ad+b}(x),$$

其中$a \cdot c \neq 0$，$ac, cd + b \in Q$，故$f_{a,b} \circ f_{c,d} \in G$，即$G$中$\circ$运算是封闭的. 映射合成运算是可结合的. $f_{1,0} \in G$是G的单位元，$f_{\frac{1}{a},-\frac{b}{a}}$是$f_{a,b}$的逆元. $\langle G, \circ \rangle$是群. 由于运算$\circ$不满足交换律，所以$\langle G, \circ \rangle$是非交换群.

5.3 子群

定义 5.5. $\langle G, * \rangle$是群，H是G的非空子集. 如果

1° $\forall a, b \in H$，$a * b \in H$;

2° $\forall a \in H$，$a^{'} \in H$;

则称$\langle H, * \rangle$是$\langle G, * \rangle$的**子群**，并记为$H \leqslant G$.

定理 5.8. 若$\langle H, * \rangle$是$\langle G, * \rangle$的子群，则$\langle H, * \rangle$也是群.

证明: 从$\langle H, * \rangle$是$\langle G, * \rangle$的子群的定义知运算$*$在集合H中是封闭的. H是G的子集，即H中的每个元素都是G中的元素. 而$\langle G, * \rangle$为群，$*$运算满足结合律，从而$\forall a, b, c \in H \subseteq G$，$(a * b) * c = a * (b * c)$. H是G的非空子集，它至少有一个元素$h \in H$，由子群定义中2°知，$h^{'} \in H$那么$h * h^{'} = e \in H$. 故G中的单位元e在H中并且也是H的单位元. 综上知$\langle H, * \rangle$本身也是群.

由此看出，群G的子群，如果对该群的运算及求逆运算是封闭的，那么该子集对原来群的运算也构成群.

定理 5.9. H是群G的有限非空子集. 如果$\forall a, b \in H$，$a * b \in H$，则$H \leqslant G$.

证明: 任取$a \in H$，$a^2 = a * a \in H$，$a^3 = a^2 * a \in H, \cdots$. 由于$H$是$G$的有限非空子集，$a, a^2, a^3, \cdots$不可能是完全不同的元素，必存在$1 \leq i \leq j$，使得$a^i = a^j = a^i * a^{j-i}$. 用左消去律得到$a^{j-i} = e \in H$，

$$e = a^{j-i} = a * a^{j-i-1},\ j-i-1 \geq 0.$$

$a^{'} = a^{j-i-1} \in H$，这表明H中任意元素a在H中均有逆. 对照定义5.5知$\langle H, * \rangle$是$\langle G, * \rangle$的子群.

例 5.13. $\langle G, \bullet \rangle = \langle \{1, -1, i, -i\}, \bullet \rangle$中，$H = \{-1, 1\} \subset G$. H对复数乘法封闭，$\langle H, \bullet \rangle$是$\langle G, \bullet \rangle$的子群.

例 5.14. 全体非零复数集合C^*，对复数乘法构成群$\langle C^*, \bullet \rangle$. 令

$$H = \{x | x \in C^*, \exists n \in N 使 x^n = 1\},$$

则$H \leqslant C^*$.

证明: 1是群$\langle C^*, \bullet \rangle$的单位元. $1^1 = 1,\ 1 \in H$. H是C^*的非空子集. 若$x, y \in H$，即存在$n, m \in N$，使$x^n = y^m = 1$，而$(x \bullet y)^{mn} = (x^n)^m \bullet (x^m)^n = 1$，故$x \bullet y \in H$. 又若$x \in H$，存在$n \in N, x^n = 1$. 而$(x^{'})^n = (x^n)^{'} = 1^{'} = 1$，故$x^{'} \in H$. 这就证明了$H \leqslant C^*$.

例 5.15. 设$H_1 \subseteq H_2 \subseteq \cdots \subseteq H_n \subseteq \cdots$是由群$G$的子群$H_i$组成的升链. 令$H = \bigcup_i H_i$，则$H \leqslant G$.

证明: H_i是群G的子群. 即$H_i \neq \varnothing$且$H_i \subseteq G$，显然$H = \bigcup_i H_i \neq \varnothing$且$H \subseteq G$. 若$a, b \in H$，存在$i, j, i > j$使$a \in H_i, b \in H_j \subseteq H_i$，由于$H_i \leqslant G$，则$a * b \in H_i \subseteq H$. 又若$a \in H$，存在$i, a \in H_i$. 再由$H_i \leqslant G$，则$a^{'} \in H_i \subseteq H$. 综上知$H \leqslant G$.

例 5.16. $\langle G, * \rangle$为群. S是G的非空子集，令

$$A = \{H | H \leqslant G, 且 S \subseteq H\},$$

即A是G中包含S所有子群构成的集合. 显然$G \in A$，即A是非空的. 定义$K = \bigcap_{H \in A} H$. 证明$K \leqslant G$.

证明: 任取$H \in A$，H是G的子群，群G的单位元$e \in H$且$H \subseteq G$，所以$e \in \bigcap_{H \in A} H = K$ 且$K \subseteq G$，即K是G的非空子集. 若$a, b \in K$，对任何$H \in A$均有$a, b \in H$，H是G的子群，故$a * b \in H$. 所以$a * b \in K$，又

若$a \in K$，对任何$H \in A$均有$a \in H$，H是G的子群，故$a^{'} \in H$. 所以$a^{'} \in K$，综上知$K \leqslant G$.

A中每个H均满足$S \subseteq H$. 显然$S \subseteq \bigcap_{H \in A} H = K$. 从而$K$是$G$中包含$S$的最小子群. 我们记$\langle S \rangle = K = \bigcap_{H \in A} H$，并称$\langle S \rangle$为$S$生成的子群，如果$S$本身就是$G$的子群，那么$K = \langle S \rangle = S$，否则$S \subseteq \langle S \rangle$.

下面讨论$\langle S \rangle$是哪些元素组成的. 我们先引入集合T.

$$T = \{a_1^{e_1} * a_2^{e_2} * \cdots * a_n^{e_n} \mid a_1, a_2, \cdots, a_n \in S, e_1, e_2, \cdots, e_n = \pm 1, n = 1, 2, \cdots\}.$$

S是非空集合. S中的任意元素a，$a = a^1$，故$a \in T$，也就是说$S \subseteq T$，T是非空集合. 由T的定义知$T \subseteq G$. 若$x = a_{i_1}^{e_{i_1}} * a_{i_2}^{e_{i_2}} * \cdots * a_{i_m}^{e_{i_m}}, y = a_{j_1}^{e_{j_1}} * a_{j_2}^{e_{j_2}} * \cdots * a_{j_n}^{e_{j_n}} \in T$, 那么$x * y = a_{i_1}^{e_{i_1}} * a_{i_2}^{e_{i_2}} * \cdots * a_{i_m}^{e_{i_m}} * a_{j_1}^{e_{j_1}} * a_{j_2}^{e_{j_2}} * \cdots * a_{j_n}^{e_{j_n}} \in T$, $x^{'} = a_{i_1}^{-e_{i_1}} * a_{i_2}^{-e_{i_2}} * \cdots * a_{i_m}^{-e_{i_m}} \in T$, 所以$T$是$G$的包含$S$的子群. 前面已经知道$\langle S \rangle$是$G$中包含$S$的最小子群，于是$\langle S \rangle \subseteq T$.

另一方面，任取$x = a_{i_1}^{e_{i_1}} * a_{i_2}^{e_{i_2}} * \cdots * a_{i_m}^{e_{i_m}} \in T$，其中$a_{i_k} \in S, e_{i_k} = \pm 1, 1 \leq k \leq m$. 由于$\langle S \rangle$是$G$中包含$S$的群，$a_{i_k}^{e_{i_k}} \in \langle S \rangle, 1 \leq k \leq m$，所以$x \in \langle S \rangle$，由此推出$T \subseteq \langle S \rangle$.

综上知$T = \langle S \rangle$.

特别地，当$S = \{a\}$时，$\langle S \rangle = \{a^n | n \in Z\} = \langle a \rangle$. 整数加群$\langle Z, + \rangle$是由整数1生成的群，即$\langle Z, + \rangle = \langle 1 \rangle$. $\langle 2 \rangle = \{2k | k \in Z\}$，$\langle 2, 3 \rangle = \{2a + 3b | a, b \in Z\} = \{k \cdot 1 | k \in Z\} = Z$. 一般地，$\langle m, n \rangle = \{(m, n) \cdot k | k \in Z\}$.

5.4 循环群

有一类群，它的每个元素都可以写成某个固定元素的幂，a^i或a^{-i}，这样的群称之为循环群.

定义 5.6. 在群$\langle G, * \rangle$中，如果存在一个元素$g \in G$，使$G = \{g^n \mid n \in \mathbf{Z}\}$，则称该群为**循环群**，记作$\langle g \rangle$，其中$g$称为循环群的**生成元**.

若群中的运算用“+”表示，循环群$\langle G, + \rangle$写成$\langle g \rangle = \{ng \mid n \in \mathbf{Z}\}$，$g$是该循环群的生成元.

每个循环群都是交换群，这是因为$g^r * g^s = g^{r+s} = g^s * g^r$.

例 5.17. $\langle G,*\rangle=\langle\{1,-1,\mathrm{i},-\mathrm{i}\},\cdot\rangle$是由i生成的四阶循环群.

$$\mathrm{i}^0=1,\mathrm{i}^1=\mathrm{i},\mathrm{i}^2=-1,\mathrm{i}^3=-\mathrm{i},\mathrm{i}^4=1,\cdots$$

所以该群可以写成$\langle\left\{1,\mathrm{i},\mathrm{i}^2,\mathrm{i}^3\right\},\bullet\rangle$.

定理 5.10. g是群$\langle G,*\rangle$中的k阶元. 令$H=\{g^r\mid r\in\mathbf{Z}\}$，那么$\langle H,*\rangle$是$\langle G,*\rangle$的一个$k$阶子群.

证明: $\forall r,s\in\mathbf{Z},g^r*g^s=g^{r+s}\in H,\left(g^r\right)'=g^{-r}\in H$. 故$H\leqslant G$. g是G的k阶元，$g^0=e,g^1,\cdots,g^{k-1}$是k个两两互不相同的元素. 对于任意整数t，$t=uk+v$，其中$0\leqslant v<k$，那么

$$g^t=g^{uk+v}=(g^k)^u*g^v=g^v$$
$$H=\{g^r\mid r\in\mathbf{Z}\}=\left\{g^0,g^1,\cdots,g^{k-1}\right\}.$$

$\langle H,*\rangle$是$\langle G,*\rangle$的k阶子群.

特别地，G是n阶群. G的某个元素g是n阶元，那么G必定是由g生成的一个循环群.

定理 5.11. 循环群的每个子群必是循环群.

证明: 令G是由元素a生成的循环群. $G=\langle a\rangle$. H是群G的子群. 如果$H=\{e\}=\langle e\rangle$，显然H是循环群. 如果$H\neq\{e\}$. 那么至少存在一个元素$b\in H$且$b\neq e$. 设m是使$a^m\in H$的最小正整数，任取H中的元素b，b也是群G的元素，则$b=a^n$. 令$n=mu+v$，$0\leqslant v<m$.

$$b=a^n=a^{mu+v}=(a^m)^u*a^v,$$
$$a^v=a^n*(a^m)^{-u}.$$

由于$b=a^n\in H$，$a^m\in H$，而H是群，$(a^m)^{-u}\in H$，从而$a^v\in H$. 假若$v>0$，那么这就与m是使$a^m\in H$的最小正整数相矛盾，故不可. 这说明必须$v=0$，即$b=a^{mu}=(a^m)^u$，也就是说H中的每个元素都可以表示成a^m的方幂. 于是a^m是子群H的生成元，H是循环群.

例 5.18. 模6同余类加群$\langle\mathbf{Z}_6,+\rangle=\langle[1]\rangle$是循环群. $[0]$是1阶元，$\langle[0]\rangle=\{[0]\}$是$\mathbf{Z}_6$的1阶子群，$[3]$是2阶元，$\langle[3]\rangle=\{[0],[3]\}$是$\mathbf{Z}_6$的2阶子群. $[5]$是6阶元，$\langle[5]\rangle=\{[0],[5],[4],[3],[2],[1]\}$是$\mathbf{Z}_6$的6阶子群.

定理 5.12. G是n阶循环群，$G=\langle a\rangle$且$|G|=n$，H是G的一个子群，$H=\langle b\rangle$，且$b=a^s$，则

$$|H|=\frac{n}{(n,s)}.$$

证明： 令H是G的m阶子群，m是使$b^m=e$的最小正整数. $b^m=a^{sm}=e$，而a是n阶元$a^n=e$，故$n\mid ms$. 设$(n,s)=d, n=dn_0, s=ds_0$，且$(n_0,s_0)=1$，于是$n_0\mid ms_0$，进而得到$n_0\mid m$，即$m=n_0\cdot k$. m是满足此式的最小正整数，从而$k=1$. 最后得出

$$m=n_0=\frac{n}{(n,s)}$$

例 5.19. 求模18同余类加群的所有子群.

解： $\langle[1]\rangle=\langle[5]\rangle=\langle[7]\rangle=\langle[11]\rangle=\langle[13]\rangle=\langle[17]\rangle$是$\mathbf{Z}_{18}$的18阶子群.
$\langle[2]\rangle=\langle[4]\rangle=\langle[8]\rangle=\langle[10]\rangle=\langle[14]\rangle=\langle[16]\rangle$是$\mathbf{Z}_{18}$的9阶子群.
$\langle[3]\rangle=\langle[15]\rangle$是$\mathbf{Z}_{18}$的6阶子群.
$\langle[6]\rangle=\langle[12]\rangle$是$\mathbf{Z}_{18}$的3阶子群.
$\langle[9]\rangle$和$\langle[0]\rangle$分别为$\mathbf{Z}_{18}$的2阶和1阶子群.

例 5.20. 在集合$\{1,2,\cdots,p-1\}$上定义运算$*$:

$$a*b=c\Longleftrightarrow a\cdot b\equiv c(\mathrm{mod}\ p),$$

其中p为素数. 若$a\in\{1,2,\cdots,p-1\}$，显然$(a,p)=1$，a的阶为l，那么$l\mid(p-1)$，即a是$x^l\equiv 1(\mathrm{mod}\ p)$的一个解. 于是$\{1,a,a^2,\cdots,a^{l-1}\}$都是$x^l\equiv 1(\mathrm{mod}\ p)$的解，而且是全部解. 它是以$a$为生成元的$l$阶循环群，是$\{1,2,\cdots,p-1\}$的$l$阶子群. 元素$a^k$的阶为$\frac{l}{(k,l)}$.

5.5 置换群

定理 5.13. n元集合$A=\{1,2,\cdots,n\}$上的全体置换构成集合S_n，S_n在合成运算之下构成一个群. 称之为n次对称群，其阶数为$n!$.

证明： 集合A上的置换是从A到A的双射. 由于两个双射的合成映射仍是双射. 所以S_n中的置换在合成运算下是封闭的. 并且映射的合成满足结合

律. S_n的单位元是恒同置换$\sigma_I = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$置换$\sigma$的逆元是它的逆置换$\sigma^{-1}$. 根据群的定义知$\langle S_n, \bullet \rangle$是群. n元置换共有$n!$个. 故$|S_n| = n!$.

定义 5.7. 集合A上的双射全体对于映射的合成运算构成群. 该群叫做**对称群**. 对称群的子群为置换群.

由于置换的合成运算不满足交换律，所以置换群通常是非交换群.

例如，$S_2 = \{\sigma_I, (1\ 2)\}, S_3 = \{\sigma_I, (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (1\ 3), (2\ 3)\}$.

例 5.21. 图5.2中的等边三角形经旋转和反射使之三个顶点与原来的顶点重合在一起，一共有六种情况：

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \sigma_1, \qquad \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\ 2),$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3), \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\ 3),$$

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2), \quad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\ 3),$$

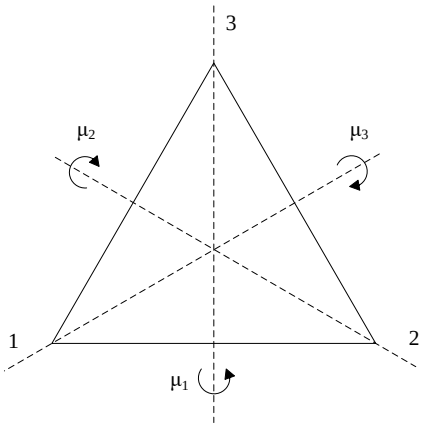

图 5.2: 等边三角形的顶点置换示意图

令ρ_0, ρ_1, ρ_2分别是绕等边三角形中心旋转$0°, 120°, 240°$的结果. μ_1, μ_2, μ_3分别是对三个对称轴反射的结果.

令$D_3=\{\rho_0,\rho_1,\rho_2,\mu_1,\mu_2,\mu_3\}$，$D_3$在合成运算之下形成一个置换群. 它的乘法表如下:

$*$	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_2	μ_3	μ_1
ρ_2	ρ_2	ρ_0	ρ_1	μ_3	μ_1	μ_2
μ_1	μ_1	μ_3	μ_2	ρ_0	ρ_2	ρ_1
μ_2	μ_2	μ_1	μ_3	ρ_1	ρ_0	ρ_2
μ_3	μ_3	μ_2	μ_1	ρ_2	ρ_1	ρ_0

我们注意到$\rho_1\cdot\mu_3=\mu_1,\mu_3\cdot\rho_1=\mu_2$，$D_3$不是交换群，称它为三次二面体. $|D_3|=6$，恰好$D_3=S_3$.

例 5.22. 正方形通过旋转和反射使之顶点与原来顶点重合. 共有如下八种情况:

$$\rho_0=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}=\sigma_1,\qquad \mu_1=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}=(1\ 2)(3\ 4),$$
$$\rho_1=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}=(1\ 2\ 3\ 4),\quad \mu_2=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}=(1\ 4)(2\ 3),$$
$$\rho_2=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}=(1\ 3)(2\ 4),\quad \delta_1=\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}=(1\ 3),$$
$$\rho_3=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}=(1\ 4\ 3\ 2),\quad \delta_2=\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}=(2\ 4).$$

其中$\rho_0,\rho_1,\rho_2,\rho_3$是正方形绕中心旋转$0^\circ,90^\circ,180^\circ,270^\circ$的结果. μ_1,μ_2是关于两个对边中心点连线反射的结果. δ_1,δ_2是关于两条对角线反射的结果*(*图*5.3)*.

令$D_4=\{\rho_0,\rho_1,\rho_2,\rho_3,\mu_1,\mu_2,\delta_1,\delta_2\}$, D_4在合成运算之下形成一个置换群. 它的乘法表如下:

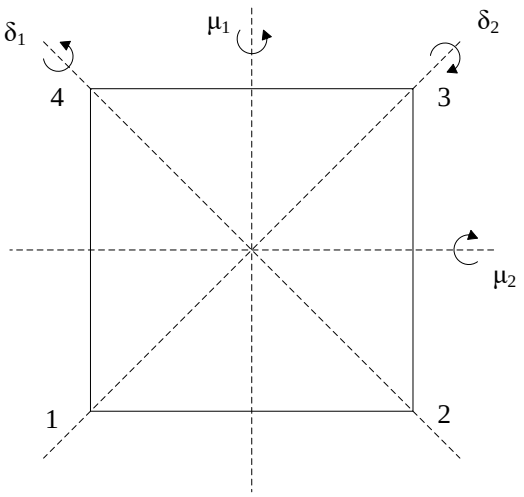

图 5.3: 正方形的顶点置换示意图

$*$	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_1	ρ_1	ρ_2	ρ_3	ρ_0	δ_1	δ_2	μ_2	μ_1
ρ_2	ρ_2	ρ_3	ρ_0	ρ_1	μ_2	μ_1	δ_2	δ_1
ρ_3	ρ_3	ρ_0	ρ_1	ρ_2	δ_2	δ_1	μ_1	μ_2
μ_1	μ_1	δ_2	μ_2	δ_1	ρ_0	ρ_2	ρ_3	ρ_1
μ_2	μ_2	δ_1	μ_1	δ_2	ρ_2	ρ_0	ρ_1	ρ_3
δ_1	δ_1	μ_1	δ_2	μ_2	ρ_1	ρ_3	ρ_0	ρ_2
δ_2	δ_2	μ_2	δ_1	μ_1	ρ_3	ρ_1	ρ_2	ρ_0

D_4称为四次二面体. $|D_4| = 8$. 它是四次对称群S_4的子群.

例 5.23. 证明$S_n = \langle(1\ 2), (1\ 3), \cdots, (1\ n)\rangle$，即对换$(1\ 2)$，$(1\ 3)$，$\cdots$，$(1\ n)$是$S_n$的生成元系.

证明: $\langle(1\ 2), (1\ 3), \cdots, (1\ n)\rangle$是由$(1\ 2)$，$(1\ 3)$，$\cdots$，$(1\ n)$是$S_n$生成的群. 由5.3例5.16知,

$$\langle(1\ 2), (1\ 3), \cdots, (1\ n)\rangle = \{\sigma_1\sigma_2\cdots\sigma_n \mid \sigma_i \in \{(1\ 2), (1\ 3), \cdots, (1\ n)\},$$
$$1 \leqslant i \leqslant n, n = 1, 2, \cdots\}.$$

显然$\langle(1\ 2),(1\ 3),\cdots,(1\ n)\rangle \subseteq S_n$.

下面证明每个n元置换均可以写成$(1\ 2),(1\ 3),\cdots,(1\ n)$这些基本元素的乘积. 对$n$进行归纳证明. 当$n=2$时,

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = (1\ 2)(1\ 2), \qquad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = (1\ 2),$$

该命题成立. 假设$n=k$时命题成立，现设$n=k+1$,

$$\sigma \begin{pmatrix} 1 & 2 & \cdots & k & k+1 \\ \sigma(1) & \sigma(2) & \cdots & \sigma(k) & \sigma(k+1) \end{pmatrix}$$

有如下两种可能:

1° $\sigma(k+1)=k+1$，这时σ本身变成k元置换. 由归纳假设命题成立.

2° $\sigma(k+1)\neq k+1$，必定存在$l, 1\leqslant l\leqslant k, \sigma(l)=k+1$. 用对换$(l\quad k+1)$右乘$\sigma$得到$\sigma_1$,

$$\begin{aligned} &\sigma_1 = \sigma(l\quad k+1) \\ &= \begin{pmatrix} 1 & 2 & \cdots & l-1 & l & l+1 & \cdots & k+1 \\ \sigma(1) & \sigma(2) & \cdots & \sigma(l-1) & k+1 & \sigma(l+1) & \sigma(k+1) & \end{pmatrix} (l\quad k+1) \\ &= \begin{pmatrix} 1 & 2 & \cdots & l-1 & l & l+1 & \cdots & k & k+1 \\ \sigma(1) & \sigma(2) & \cdots & \sigma(l-1) & \sigma(k+1) & \sigma(l+1) & \cdots & \sigma(k) & k+1 \end{pmatrix}, \end{aligned}$$

σ_1变为k元置换. 由归纳假设σ_1可以写成$(1\ 2)$，$(1\ 3)$，$\cdots$，$(1\ k)$的乘积. 而$\sigma=\sigma_1(l\quad k+1)=\sigma_1(1\ l)(1\ k+1)(1\ l)$，故$\sigma$可以写$(1\ 2)$，$(1\ 3)$，$\cdots$，$(1\ k)$，$(1\ k+1)$的乘积. 命题对$n=k+1$也成立.

例如

$$\begin{aligned} S_2 &= \{\sigma_I,(1\ 2\ 3),(1\ 3\ 2),(1\ 2),(1\ 3),(2\ 3)\} \\ &= \{(1\ 2)(1\ 2),(1\ 3)(1\ 2),(1\ 2)(1\ 3),(1\ 2),(1\ 3),(1\ 2)(1\ 3)(1\ 2)\} \end{aligned}$$

5.6 群的同构

本节讨论两个群之间的关系.

我们在习题中曾经讨论过$\langle S,*\rangle$，其中$S=\{\alpha,\beta,\gamma,\delta\}$，乘法表为

$*$	α	β	γ	δ
α	β	δ	α	γ
β	δ	γ	β	α
γ	α	β	γ	δ
δ	γ	α	δ	β

$\langle S, * \rangle$是群，把该表的行与列适当地调换次序得到

$*$	γ	α	β	δ
γ	γ	α	β	δ
α	α	β	δ	γ
β	β	δ	γ	α
δ	δ	γ	α	β

再与5.2节的C_4的乘法表比较，只要把$\gamma, \alpha, \beta, \delta$分别换名为$e, a, b, c$，它们是完全相同的. 也就是说群$S$和群$C_4$的元素之间的有一种一一对应关系. 我们研究群时并不关心元素本身是什么，关心的是元素与元素间的关系. 所以，从这个意义上群S与群C_4是一回事.

为了刻画上述思想，我们引出同构的概念.

定义 5.8. $\langle G_1, * \rangle$与$\langle G_2, \bullet \rangle$是两个群，如果存在着从集合$G_1$到集合$G_2$的双射$\varphi$，对于任何$a, b \in G_1$，

$$\varphi(a * b) = \varphi(a) \bullet \varphi(b).$$

则称G_1与G_2同构，记作$G_1 \cong G_2$. 双射φ称作**同构映射**.

φ作为同构映射，除了要求它是双射外，还要求它保持运算. 即$\forall a, b \in G_1$，$\varphi(a * b) = \varphi(a) \bullet \varphi(b)$. 形象地说，同构映射$\varphi$满足如图5.4所示交换图表.

如果群G_1与群G_2同构，那么两个群的单位元之间以及元素和它的逆元之间有什么联系呢? 这是下面定理要讨论的内容.

定理 5.14. φ是从群G_1到群G_2的同构映射，e_1和e_2分别是群G_1和G_2的单位元，必有$\varphi(e_1) = e_2$，并且对任何G_1中的元素a，$\varphi(a') = \varphi'(a)$.

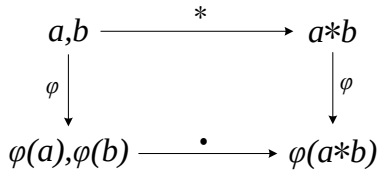

图 5.4: 同构映射φ的交换图表

证明： e_1和e_2分别是群G_1和G_2的单位元. 对任意G_1中的元素a,

$$\varphi(a) = \varphi(e_1 * a) = \varphi(e_1) \bullet \varphi(a).$$

等式两边同时右乘$\varphi^{'}(a)$得到

$$e_2 = \varphi(a) \bullet \varphi^{'}(a) = \varphi(e_1) \bullet \varphi(a) \bullet \varphi^{'}(a) = \varphi(e_1),$$

即群G_1的单位元e_1的同构映射像是G_2的单位元e_2.

又对于G_1的任意元素a,

$$\varphi^{'}(a) = \varphi^{'}(a) \bullet e_2 = \varphi^{'}(a) \bullet \varphi(e_1) = \varphi^{'}(a) \bullet \varphi(a) \bullet \varphi(a^{'}) = \varphi(a^{'}),$$

即G_1任意元素a的逆元的像等于该元素同构映射像的逆元.

例 5.24. 证明正实数乘群与实数加群同构.

证明： $\langle \mathbf{R}^+, \bullet \rangle$与$\langle \mathbf{R}, + \rangle$分别为正实数乘群与实数加群. $\varphi : \mathbf{R} \to \mathbf{R}^+$, $\varphi(x) = \mathrm{e}^x$. 显然$\varphi$是双射. 对任意$x, y \in \mathbf{R}$,

$$\varphi(x + y) = \mathrm{e}^{x+y} = \mathrm{e}^x \bullet \mathrm{e}^y = \varphi(x) \bullet \varphi(y),$$

故φ为同构映射. 从而$\langle \mathbf{R}^+, \bullet \rangle \cong \langle \mathbf{R}, + \rangle$.

这里要指出的是并非每个从G_1到G_2的双射都是同构映射. 例如：$\psi : \mathbf{R} \to \mathbf{R}^+, \psi(x) = \mathrm{e}^{x-1}$，显然$\psi$是双射. 但是对任意$x, y \in \mathbf{R}$,

$$\psi(x + y) = \mathrm{e}^{x+y-1}$$
$$\phi(x) \bullet \psi(y) = \mathrm{e}^{x-1} \bullet \mathrm{e}^{y-1} = \mathrm{e}^{x+y-2}$$

故ψ不是从$\mathbf{R}$到$\mathbf{R}^+$的同构映射.

例 5.25. 在同构的意义下循环群$G = \langle a\rangle$只有两类：若a是无限阶元，则$G \cong \langle \mathbf{Z}, +\rangle$. 若$a$是$n$阶元，则$G \cong \mathbf{Z}_n$.

证明： 若循环群$G = \langle a\rangle$的生成元a是无限阶元，对任何$m_1 \neq m_2$均有$a^{m_1} \neq a^{m_2}$. f 是从G到整数集合$\mathbf{Z}$的映射，$f : G \to \mathbf{Z}, f(a^m) = m$. 显然$f$是双射. 对任意$a^{m_1}, a^{m_2} \in G$，

$$f(a^{m_1} * a^{m_2}) = f(a^{m_1+m_2}) = m_1 + m_2 = f(a^{m_1}) + f(a^{m_2}).$$

f是同构映射，故$G \cong \langle \mathbf{Z}, +\rangle$.

若生成元a是n阶元，则$G = \left\{a^0, a^1, a^2, \cdots, a^{n-1}\right\}$. f是从G到模n同余类集合$\mathbf{Z}_n$的映射，$f : G \to \mathbf{Z}_n, f(a^i) = [i]$. 显然$f$是双射. 对任意$a^i, a^j \in G$，

$$f(a^i * a^j) = f(a^{i+j}) = [i + j] = [i] + [j] = f(a^i) + f(a^j).$$

f是同构映射，故$G \cong \langle \mathbf{Z}_n, +\rangle$.

例 5.26. 任意一个群都与一个置换群同构.

证明： 对于任意群$\langle G, *\rangle$构造一个新的集合

$$G^{'} = \{f_a \mid a \in G, f_a : G \to G, f_a(x) = a * x\}.$$

容易证明f_a是G上的双射，$G^{'}$上的运算$\cdot$是映射的合成运算.

$$(f_a \bullet f_b)(x) = f_a(b * x) = (a * b) * x = f_{a*b}(x),$$

即$f_a \bullet f_b = f_{a*b}$. 该运算在$G^{'}$中封闭且满足结合律. f_e是$G^{'}$的单位元，$f_{a'}$是f_a的逆元，从而$\langle G^{'}, \bullet\rangle$是置换群.

在群G与$G^{'}$之间定义映射$h : G \to G^{'}, h(a) = f_a$，显然$h$是双射. 对任意$a, b \in G$，

$$h(a * b) = f_{a*b} = f_a \bullet f_b = h(a) \bullet h(b),$$

故h是同构映射. 从而$G \cong G^{'}$.

例 5.27. 求出与n阶循环群同构的置换群.

解： 令$G=\langle a\rangle$是循环群，$f:G\to G'$是同构映射. 任取$x\in G'$，必存在$g=a^i\in G$使

$$x=f(g)=f(a^i)=(f(a))^i.$$

这说明G'是以$f(a)$为生成元的循环群. 现G是n阶循环群，$G=\{a^0,a^1,\cdots,,a^{n-1}\}$，从例5.26可知$G'=\{f_{a^0},f_{a^1},\cdots,f_{a^{n-1}}\}$. 也是$n$阶循环群. 其生成元是$f_a$，它对应$G$上长为$n$的轮换$(a^0\ a^1\ \cdots\ a^{n-1})$. 令$G''=\langle(a^0\ a^1\ \cdots\ a^{n-1})\rangle$，则$G\cong G''$.

定理 5.15. $\langle G,*\rangle$为群，另有一个集合G'，是G'上的运算. 如果存在从G到G'上的双射f，对G中的任意元素a,b有$f(a*b)=f(a)\bullet f(b)$. 那么$\langle G',\bullet\rangle$也是群，并且$G\cong G'$.

证明： 任取$x,y\in G'$，f是从G到G'的满射，存在$a,b\in G$使得$f(a)=x$. $f(b)=y$. 由于f保持运算，

$$x\bullet y=f(a)\bullet f(b)=f(a*b)\in G',$$

可知运算$\bullet$在G'中是封闭的，任取$x,y,z\in G'$. 对于满射f在G中有原像. $f(a)=x$，$f(b)=y$，$f(c)=z$，

$$\begin{aligned}(x\bullet y)\bullet z&=(f(a)\bullet f(b))\bullet f(c)=f((a*b)*c)\\&=f(a*(b*c))=f(a)\bullet(f(b)\bullet f(c))=x\bullet(y\cdot z),\end{aligned}$$

即G'中运算$\bullet$满足结合律. 容易看出$f(e)$是G'的单位元. 任取$x\in G',a\in G$是它的原像，易知$f(a')\in G'$是x的逆元.

综上知$\langle G',\bullet\rangle$是群. f就是从G到G'的同构映射，从而$G\cong G'$.

习题

1. 如下代数系统$\langle S,*\rangle$哪些是群? 如果是群，它是否是交换群? 指出它的单位元以及如何计算其逆元.

(1) $S=\{z|z\in\mathbf{C},|z|=1\}$，其中$\mathbf{C}$是复数集合，$*$是普通的复数加法.

(2) $S=\{a+b\sqrt{2}\mid a,b\in\mathbf{Q}\}$，其中$\mathbf{Q}$是有理数集合. $*$是普通的加法.

(3)

$$S=\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}-1&0\\0&-1\end{pmatrix},\begin{pmatrix}1&0\\0&-1\end{pmatrix},\begin{pmatrix}-1&0\\0&1\end{pmatrix}\right\}$$

$*$是矩阵乘法.

(4) $S=\{\alpha,\beta,\gamma,\delta\}$

$*$	α	β	γ	δ
α	β	δ	α	γ
β	δ	γ	β	α
γ	α	β	γ	δ
δ	γ	α	δ	β

(5) $S=\mathbf{R}-\{0\}$是非零实数集合，在S 上定义运算$*$:

$$x*y=\begin{cases}x\cdot y & x>0,\\ x/y & x<0.\end{cases}$$

(6) p为素数，$S=\{1,2,\cdots,p-1\}$. 在S上定义运算$*$:

$$a*b=c\Longleftrightarrow a\cdot b\equiv c(\mathrm{mod}\ p).$$

2. 令$S=\mathbf{R}-\{-1\}$，在S上定义运算$*$:

$$a*b=a+b+ab$$

(1) 证明$\langle S,*\rangle$是群;

(2) 在S中求解方程$2*x*3=7$.

3. 在群G中，如果对G有任意元素a均有$a^2=e$，证明G必是交换群.

4. G是交换群当且仅当对G中任意元素$a,b,(a*b)^2=a^2*b^2$.

5. g是群G中的任意元素，那么，

(1) g与它的逆元$g^{'}$同阶;

(2) $(g^k)^{'}=(g^{'})^k$，k是非负整数.

6. a与b是群G中的两个任意元素. 证明$a*b$与$b*a$是同阶的.

7. 如果群G中只有一个2阶元a，那么a与G中任意元素都是可交换的，即$\forall x \in G, a * x = x * a$.

8. G是群，G中的元素个数为偶数，证明：存在$a \in G, a$是2阶元.

9. H是群G的非空子集. $\langle H, * \rangle$是$\langle G, * \rangle$的子群当且仅当$\forall a, b \in H, a * b' \in H$.

10. G是群.

$$H = \{a \mid a \in G, \forall g \in G, a * g = g * a\},$$

称为群G的中心. 证明：$\langle H, * \rangle$是$\langle G, * \rangle$的子群.

11. H, K是群G的子群. 证明$H \cap K$也是G的子群. $H \bigcup K$是G的子群吗? 证明你的结论.

12. 找出K_4群的所有子群.

13. 令$G = \{f_{a,b} \mid f_{a,b} : \mathbf{Q} \to \mathbf{Q}, f(x) = ax + b, a \neq 0, a, b \in \mathbf{Q}\}$, G对合成运算构成群. 证明$H = \{f_{1,b} \mid b \in \mathbf{Q}\}$是$G$的子群.

14. 指出下列群中哪个是循环群? 对循环群写出它的全部生成元.

(1) $G_1 = \langle \mathbf{Q}, + \rangle$;

(2) $G_2 = \langle 6Z, + \rangle$;

(3) $G_3 = \langle \{6^n \mid n \in \mathbf{Z}\}, \bullet \rangle$.

15. G是6阶循环群，找出G的全部生成元并列出G的所有子群.

16. 证明：只有一个生成元的循环群至多含有两个元素.

17. 如果n阶群G的某个元素g是n阶的，那么G是由g生成的循环群.

18. G是n阶循环群，d是n的因子，G存在且仅存在一个d阶子群.

19. 找出S_3的所有子群.

20. A_4是全体4元偶置换构成的群，请列出它的全部元素.

21. $S_n (n \geqslant 2)$的每个子群或者全部由偶置换构成，或者其中奇、偶置换各占一半.

22. 证明：整数加群与偶数加群同构.

23. 证明：群的同构关系是一种等价关系.

24. 找出所有与K_4群同构的S_n的子群.

25. 证明：无限循环群的子群，除$\{e\}$以外都是无限循环群.

26. 在群$\langle G, * \rangle$中定义新的二元运算$\bullet$，

$$a \bullet b = b * a.$$

证明：$\langle G, \bullet \rangle$是群，并且$\langle G, * \rangle$与$\langle G, \bullet \rangle$同构.