CHAPTER 3

第3章 循环群与群的结构

在这一章里，讨论在理论和应用方面都具有重要地位的循环群及它的重要特例剩余类群，并在循环群的基础上进一步深入讨论群的结构。

3.1 循环群

在群里面，希望群的结构尽量简单，然后复杂的群可以分解成简单的群来研究。设 g 是群 G 中的某个元素，则它与自身的反复二元运算和逆元都在群 G 中，由此可以得到最简单的一种群。

定义 3-1 如果一个群 G 里的元素都是某一个元素 g 的幂，则 G 称为循环群，g 称为 G 的一个生成元。由 g 生成的循环群记为 (g)。

无限循环群可表示为：

$$\{\cdots, g^{-2}, g^{-1}, g^0, g^1, g^2, \cdots\} \tag{3-1}$$

其中 $g^0 = e$。

有限 n 阶循环群可表示为：

$$\{g^0, g^1, g^2, \cdots, g^{n-1}\} \tag{3-2}$$

其中 $g^0 = e$。

例 3-1 整数加法群 Z 是一个循环群。1 是生成元，每一个元素都是 1 的“幂”。这里再次说明讨论的群里“乘法”是抽象的，只代表一种代数运算。在整数加群中，“乘法”就是普通加法，那么“幂”就是一个元素的连加，例如

$$1^m = m = \overbrace{1+1+\cdots 1}^{m}$$

$$1^{-m} = -m = \overbrace{(-1)+(-1)+\cdots(-1)}^{m}$$

而且规定

$$0 = 1^0$$

即 0 为 0 个 1 相加。

由上面的例子看到生成元不是唯一的，因为 -1 也可以是生成元。

例 3-2　复数域上的 n 次方程

$$z^n-1=0$$

的根集合

$$\{e^{\frac{2k\pi}{n}i},\quad k=0,1,2,\cdots,n-1\}$$

对复数乘法是一个有限循环群。这个群的生成元是 $e^{\frac{2\pi}{n}i}$。

对于循环群有如下几个性质。

(1) 循环群是交换群。

对于循环群 G 中两个任意元 g^i、g^j，有

$$g^ig^j=g^{i+j}=g^{j+i}=g^jg^i$$

所以循环群一定满足交换律，是交换群(Abel 群)。

(2) 在 n 阶循环群中，有 $g^n=e$。

因为如果 $g^n\neq e$，假设 $g^n=g^i(0<i\leqslant n-1)$，则由消去律得

$$g^{n-i}=e\quad(0<n-i\leqslant n-1)$$

这与 n 阶循环群的定义矛盾。

(3) 由于 n 阶循环群中 $g^n=e$，则可以得到：设 i、j 是任意整数，如果 $i\equiv j(\mathrm{mod}\ n)$，则

$$g^i=g^j$$

g^i 的逆元

$$g^{-i}=g^{n-i}$$

下面利用循环群的概念讨论一般群的**元素的阶**。

设 G 是一个一般群，a 是 G 中的一个元素。可能有下列两种情况。

(1) a 的所有幂两两不相等，于是以 a 为生成元的循环群

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

是无限循环群。如整数加法群。

(2) 存在整数 $i>j$，使

$$a^i=a^j$$

则

$$a^{i-j}=e$$

这表明存在正整数 $k=i-j$，使

$$a^k=e$$

称使上式成立的最小正整数 n 为**元素 a 的阶**。在第(1)种情况下，这样的正整数不存在，称 a 是**无限阶元素**。

设 a 是 n 阶元素，则序列

$$a^0=e,a^1,a^2,\cdots,a^{n-1}$$

两两不等，而且 a 的一切幂都包含在这个序列中。

用反证法证明第一点。如果

$$a^i=a^j,\quad 0\leqslant j<i\leqslant n-1$$

则 $a^{i-j}=e$，而 $0<i-j\leqslant n-1$，这与 a 是 n 阶元素矛盾。

现在证明第二点，即证明对于任意整数 m，a^m 都包含在上面的序列中。m 可表示为：

$$m = qn + r, \quad 0 \leqslant r < n$$

于是

$$a^m = a^{qn+r} = (a^q)^n a^r = a^r$$

因为 a^r 在上面的序列中,则 a^m 也在上面的序列中。

定理 3-1 一个群 G 的任意元素 a 都能生成一个循环群,它是 G 的子群。如果 a 是无限阶元素,则 a 生成无限循环群;如果 a 是 n 阶元素,则 a 生成 n 阶循环群。

证明:设 a 的幂集合为 S。

(1) a 是无限阶元素情形。

对于任意 a^i、$a^j \in S(i,j=0,\pm1,\pm2,\cdots)$,有

$$a^i(a^j)^{-1} = a^{i-j} \in S$$

由 2.2 节中的定理 2-5,S 是 G 的子群。

(2) a 是 n 阶元素情形。

对于任意 a^i、$a^j \in S(i,j=0,\pm1,\pm2,\cdots)$,有

$$a^i a^j = a^{i+j} \in S$$

由 2.2 节中的定理 2-6,S 是 G 的子群。

显然 S 是 a 生成的循环群。定理证毕。

定理 3-2 对于 n 阶元素 a 有:

(1) $a^i = e$,当且仅当 $n \mid i$。

(2) a^k 的阶为 $\dfrac{n}{(k,n)}$。

证明:n 阶元素 a 生成 n 阶循环群

$$\{a^0 = e, a^1, a^2, \cdots, a^{n-1}\}$$

(1) 由于 $n \mid i$,则

$$i \equiv 0 \pmod{n}$$

于是

$$a^i = a^0 = e$$

反之,由

$$i = qn + r, \quad 0 \leqslant r < n$$

得

$$a^i = a^{qn+r} = (a^n)^q a^r = e a^r = a^r = e$$

而 n 是使 $a^k = e$ 的最小正整数,所以 $r=0$,故 $n \mid i$。

(2) 设 $l = \dfrac{n}{(k,n)}$。由于 $(k,n) \mid k$,则

$$n \left| \left(k \frac{n}{(k,n)}\right) = kl \right.$$

于是由(1)有

$$(a^k)^l = a^{kl} = e$$

而如果

$$(a^k)^i = a^{ki} = e$$

则

$$n \mid ki$$

$$\frac{n}{(k,n)} \left| \frac{k}{(k,n)} i \right.$$

因为

$$\left(\frac{n}{(k,n)}, \frac{k}{(k,n)}\right) = 1$$

所以

$$\frac{n}{(k,n)} \left| i \right.$$

故$\frac{n}{(k,n)}$是使

$$(a^k)^i = e$$

成立的最小正整数。证毕。

上面讨论了一般群中元素的阶及其性质，现在再回到循环群上来。

显然无限循环群的元素都是无限阶元素。有限循环群生成元的阶就是群的阶。

推论 3-1　由元素 g 生成的 n 阶循环群 G 中任意元素 $g^k(0<k\leqslant n-1)$ 的阶为 $\frac{n}{(k,n)}$，当 k、n 互素时，g^k 的阶为 n，也是 G 的生成元。

例 3-3　8 阶循环群各个元素的阶分别为：

$$g^0:1;\ g:8;\ g^2:4;\ g^3:8;$$
$$g^4:2;\ g^5:8;\ g^6:4;\ g^7:8$$

其中共有 4 个生成元 g、g^3、g^5、g^7。

整数集合

$$\{0,1,2,\cdots,n-1\}$$

中与 n 互素的数有 $\varphi(n)$ 个（$\varphi(n)$ 是欧拉函数，以后还要深入讨论），因此 n 阶循环群共有 $\varphi(n)$ 个 n 阶元素或 $\varphi(n)$ 个生成元。

定理 3-3

（1）循环群的子群是循环群，它或者仅由单位元构成，或者由子群中具有最小正指数的元素生成，即生成元为具有最小正指数的元素。

（2）无限循环群的子群除 $\{e\}$ 外都是无限循环群。

（3）有限 n 阶循环群的子群的阶是 n 的正因子，且对 n 的每一个正因子 q，有且仅有一个 q 阶子群。

证明：　设 H 是循环群 (g) 的一个子群。

（1）假设 $H=\{e\}$，H 自然是循环群。假设 $H\neq\{e\}$，则有 $i\neq 0$ 使 $g^i\in H$，又因为 $g^{-i}=(g^i)^{-1}\in H$，所以可以假定 $i>0$，说明有正指数存在。

设 s 是 H 中的最小正指数，即 s 是使 $g^s\in H$ 的最小正整数，现在证明

$$H = (g^s)$$

对于任意 $g^m\in H$，有

$$m = qs + t,\quad 0\leqslant t < s$$

由于 $g^{qs}=(g^s)^q\in H$（子群 H 的封闭性，q 个 g^s 连乘也属于 H），所以

$$g^t = g^m(g^{qs})^{-1} \in H$$

(g^{qs}存在逆元,且由于封闭性,g^m、$(g^{qs})^{-1}$乘积属于H)由于s是使$g^s \in H$的最小正整数,因此得

$$t = 0$$

$$g^m = (g^s)^q$$

H的任意元素都是g^s的幂,则$H=(g^s)$。

(2) 当(g)是无限循环群时,如果$n \neq m$,则$g^n \neq g^m$,于是

$$g^{ms}(m = 0, \pm 1, \pm 2, \cdots)$$

两两不同,H是无限循环群。

(3) 假设(g)是n阶循环群,由于

$$n = qs + t, \quad 0 \leqslant t < s$$

则

$$e = g^n = g^{qs+t}$$

于是

$$g^t = (g^{qs})^{-1} \in H$$

s的最小性使得$t=0$,所以

$$n = qs$$

H可表示为

$$H = \{e, g^s, \cdots, g^{(q-1)s}\}$$

当$s=n$时

$$H = \{e\}$$

上面不仅证明了H的阶q是n的正因子,而且给出n的正因子q阶子群。当q跑遍n的所有正因子时,s也跑遍n的正因子,所以对于n的每一个正因子q,都有而且仅有一个q阶循环子群。

例 3-4 8阶循环群G的真子群。

8的所有正因子为2、4,相应的子群分别为

$$\{e, g^2, g^4, g^6\}$$

$$\{e, g^4\}$$

3.2 剩余类群

现在讨论一类特别重要的循环群——**剩余类群**。

根据同余的概念,可以将全体整数Z进行分类。设m是正整数,把模m同余的整数归为一类,即可表示为

$$a = qm + r, \quad 0 \leqslant r < m, \quad q = 0, \pm 1, \pm 2, \cdots$$

的整数为一类,称为**剩余类**,剩余类中的每个数都称为该类的**剩余**或**代表**,r称为该类的**最小非负剩余**。

例 3-5 $m=8$,$r=5$的剩余类为

$$5, \quad \pm 1 \times 8 + 5, \quad \pm 2 \times 8 + 5, \quad \pm 3 \times 8 + 5, \quad \cdots$$

这样可以将全体整数按模m分成m个剩余类:

$$\bar{0},\quad \bar{1},\quad \bar{2},\quad \cdots,\quad \overline{m-1}$$

这 m 个剩余类可分别表示为：

$$\bar{0}=\{0,\pm m,\pm 2m,\pm 3m,\cdots\}$$
$$\bar{1}=\{1,1\pm m,1\pm 2m,1\pm 3m,\cdots\}$$
$$\bar{2}=\{2,2\pm m,2\pm 2m,2\pm 3m,\cdots\}$$
$$\cdots$$
$$\overline{m-1}=\{(m-1),(m-1)\pm m,(m-1)\pm 2m,(m-1)\pm 3m,\cdots\}$$

这 m 个剩余类称为**模 m 剩余类**。

例 3-6　模 8 的剩余类为

$$\bar{0}=\{0,\pm 8,\pm 2\times 8,\pm 3\times 8,\cdots\}$$
$$\bar{1}=\{1,1\pm 8,1\pm 2\times 8,1\pm 3\times 8,\cdots\}$$
$$\bar{2}=\{2,2\pm 8,2\pm 2\times 8,2\pm 3\times 8,\cdots\}$$
$$\cdots$$
$$\bar{7}=\{7,7\pm 8,7\pm 2\times 8,7\pm 3\times 8,\cdots\}$$

设 $\bar{i}$ 和 $\bar{j}$ 是两个模 m 的剩余类，定义剩余类的加法如下：

$$\bar{i}+\bar{j}=\overline{(i+j)(\mathrm{mod}\ m)}$$

例 3-7　对于模 8 的剩余类，$\bar{1}+\bar{2}=\bar{3}$，$\bar{7}+\bar{2}=\bar{1}$。

定理 3-4　模 m 的全体剩余类集合对于剩余类加法构成 m 阶循环群。

证明：封闭性和结合律显然满足。$\bar{0}$ 是单位元，$\bar{i}$ 的逆元是

$$-\bar{i}=\overline{m-i}$$

故剩余类集合是一个群。该群是一个循环群，生成元是 $\bar{1}$。注意对于加法，元素的“幂”就是元素的连加。

介绍了剩余类群后，有下面的重要定理。

定理 3-5　任意无限循环群与整数加群 Z 同构，任意有限 n 阶循环群与 n 阶剩余类加群同构。

证明：设(g)为任意循环群。

如果(g)是无限循环群，做整数加群 Z 到(g)的映射如下：对于任意 $k\in Z$，有

$$f(k)=g^k$$

这是一个一一映射，而且对于 k、$h\in Z$，有

$$f(k)f(h)=g^kg^h=g^{k+h}=f(k+h)$$

故 f 是 Z 到(g)的同构映射，(g)与 Z 同构。

如果(g)是 n 阶循环群，做模 n 剩余类加群 Z_n到(g)的映射：对于任意$\bar{k}\in Z_n$，有

$$f(\bar{k})=g^k$$

这显然是一一映射，而且对于$\bar{k}$、$\bar{h}\in Z_n$，有

$$f(\bar{k})f(\bar{h})=g^kg^h=g^{k+h}=f(\overline{k+h})$$

故 f 是 Z_n 到(g)的同构映射，(g)与 Z_n 同构。

定理 3-5 隐含表明了任意无限循环群互相同构，任意同阶有限循环群互相同构。

定理3-5的意义在于通过了解整数加群和剩余类加群,就了解了一切无限循环群和有限循环群的构造。

3.3 子群的陪集

讨论子群陪集的目的是利用子群对群进行划分,并且进一步认识子群的特性。

在给出陪集的定义之前,先证明一个引理。

引理3-1 设G是一个群。

(1) 对于任意$a\in G$,集合

$$aG = \{ah \mid h \in G\} = G$$

(2) $GG=\{ah|h\in G,a\in G\}=G$。

证明:

(1) a、h都是G的元素,由G的封闭性,有

$$ah \in G$$

则对于任意$b\in aG$,总有$b\in G$,于是

$$aG \subseteq G$$

对于任意$b\in G$,有

$$b = eb = (aa^{-1})b = a(a^{-1}b)$$

由于

$$a^{-1}b \in G$$

所以

$$b = a(a^{-1}b) \in aG$$

于是

$$G \subseteq aG$$

故

$$G = aG$$

(2) $GG=\bigcup\limits_{a\in G}aG=\bigcup G=G$。

例3-8 对于整数加群Z有

$$a + Z = Z, \quad (a \in Z)$$

实际上,$a+Z$只是Z在数轴上做平移,如图3-1所示。

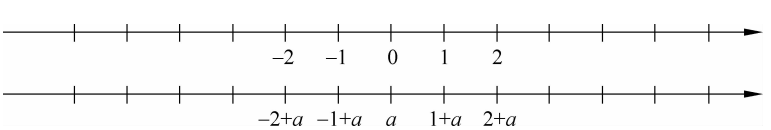

图3-1 整数加群示意图

由于Z对乘法不是群,所以不能保证

$$aZ = Z, \quad (a \in Z)$$

例如$2Z=\{0,\pm2,\pm4,\cdots\}\neq Z$。

定义3-2 设H是群G的一个子群。对于任意$a\in G$,集合

$$aH = \{ah \mid h \in H\}$$

称为 H 的一个**左陪集**，记为 aH。

同样定义右陪集

$$Ha = \{ha \mid h \in H\}$$

对于交换群（Abel 群），左陪集和右陪集是一致的，可以称为**陪集**。

由于当 $a \in H$ 时有

$$aH = H$$

则 H 也是自己的一个左陪集。同理 H 也是自己的右陪集。

左陪集可由 aH 中的任意一个元素唯一确定。假设 $b \in aH$，即

$$b = ah(h \in H)$$

则

$$bH = ahH = a(hH) = aH$$

同理右陪集可由 Ha 中的任意一个元素唯一确定。

例 3-9　设 m 是一个正整数，M 表示所有 m 的倍数组成的集合，即

$$M = \{mt \mid t = 0, \pm 1, \pm 2, \pm 3, \cdots\}$$
$$= \{0, \pm m, \pm 2m, \pm 3m, \cdots\}$$

M 的另一种表示为

$$M = \{mt \mid t \in Z\}$$

显然 M 是整数加群 Z 的子群。

设 $\overline{i}$ 为模 m 的一个剩余类，即

$$\overline{i} = \{i + mt \mid t \in Z\}$$

于是有

$$\overline{i} = i + M$$

可见 $\overline{i}$ 是 M 的一个陪集。由 Z 可以按模 m 分成 m 个剩余类，则 Z 可以按 M 分成 m 个陪集：

$$M, 1 + M, 2 + M, \cdots, (m-1) + M$$

定理 3-6　设 H 是群 G 的一个子群。H 的任意两个左（右）陪集或者相等或者无公共元素。群 G 可以表示成若干互不相交的左（右）陪集的并集。

证明：设 aH、bH 是两个左陪集。如果它们有公共元素，即存在 h_1、$h_2 \in H$ 使

$$ah_1 = bh_2$$

于是 $a = bh_2h_1^{-1} = bh_3$，其中 $h_3 = h_2h_1^{-1} \in H$。由

$$ah = bh_3h \in bH$$

可知

$$aH \subset bH$$

同样可证 $bH \subset aH$。于是有

$$aH = bH$$

这就证明两个左陪集或者相等或者无公共元素。

G 中的任何元素都在 H 的一个左陪集中。否则假设 c 不在 H 的任何左陪集中，可以做左陪集 cH，由于单位元 $e \in H$，所以

$$ce = c \in cH$$

c 在一个左陪集中。

于是得到,G 为 H 的所有左陪集的并集,即

$$G = \bigcup_{a \in G} aH$$

去掉那些相等的左陪集,则 G 为 H 的互相不相交的左陪集的并集。

对于右陪集可以做同样的证明。定理证毕。

定理 3-6 表明群 G 的一个子群 H 的左(右)陪集是对 G 的一个划分。

下面讨论两个问题:

(1) 陪集元素数目是多少?

(2) 陪集也可以成为子群吗?

这里只对左陪集讨论这些问题,对右陪集结论是一样的。

做一个 H 到它的一个左陪集 aH 的一个映射 f:对于任意 $h \in H$,

$$f(h) = ah$$

f 是一一映射。首先它是单射,否则如果对于不同的 h 和 h' 有

$$ah = ah'$$

在 G 中应用消去律得 $h = h'$,与 $h \neq h'$ 矛盾。

由于 f 是单射,所以 h 遍历 H 时,ah 遍历 aH,则 f 又是满射,所以 f 是一一映射。这表明对于有限子群 H,每个左(右)陪集内元素数目都等于 H 的阶;而对于无限子群 H,H 中的元素与陪集中的元素一一对应。

由于子群 H 的陪集互不相交,由于 $e \in H$,则 H 的其他陪集中不含单位元 e,所以它们不可能是群。故 H 的陪集除 H 外对于 G 的运算都不是群。

下面利用上述结论考察有限群。

假设群 G 的阶是 n,H 是 G 的 m 阶子群:

$$H = \{g_1, g_2, \cdots, g_m\}$$

做 H 的左陪集,设互不相交的左陪集共有 j 个,j 称为**子群 H 在群 G 中的指数**。把这 j 个陪集排列如下:

$$\begin{array}{lccccc}
a_1H(a_1 = e): & g_1 & g_2 & \cdots & g_m \\
a_2H: & a_2g_1 & a_2g_2 & \cdots & a_2g_m \\
\cdots & & & & \\
a_jH: & a_jg_1 & a_jg_2 & \cdots & a_jg_m
\end{array}$$

这称为**左陪集阵列**。

显然有

$$n = jm$$

也就是

$$|G| = j\,|H|$$

由此得到著名的**拉格朗日(Lagrange)定理**。

推论 3-2(拉格朗日定理) 设 G 是一个有限群,H 是一个子群,则 H 的阶是 G 的阶的因子。

推论 3-2 是显然的,它是一个非常重要的结果,是子群的一个重要特性。

在 3.1 节中曾指出，在群 G 中，任意一个元素 a 的全体幂的集合

$$\{a^m \mid m \in Z\}$$

构成 G 的一个子群，而且是循环群。这个子群的阶就是 a 的阶。于是有下面的结论。

推论 3-3　设 G 是一个有限群，G 中的每一个元素的阶一定是 G 的阶的因子。设 G 的阶为 n，则对任意 $a \in G$，有

$$a^n = e$$

证明：只需证第二点。对于任意 $a \in G$，设 a 的阶为 m。由于 m 是 n 的因子，则存在整数 q 有

$$n = mq$$

于是

$$a^n = a^{mq} = (a^m)^q = e$$

推论 3-4　阶为素数的群一定为循环群。

证明：　设群 G 的阶为素数，即 $|G|$ 是素数。

当 $|G|>1$ 时，取 $a \in G$ 且 $a \neq e$，则 a 生成一个循环子群 H，且 $|H| \neq 1$。由于 $|H|$ 是 $|G|$ 的因子，而当 $|G|$ 是素数时，它只有 1 和 $|G|$ 两个因子，故

$$|H| = |G|$$

这表明 $H=G$，G 是一个循环群。

结合陪集的知识，再介绍一个重要的定理——同构基本定理。

定理 3-7　f 是群 G 到群 G' 的满同态映射，则

$$G/\ker(f) \cong G' \tag{3-3}$$

证明：由 2.3 节的定理 2-8 知道 $\ker(f)$ 是 G 的子群，因此可以得到 G 关于 $\ker(f)$ 的陪集构成的集合 $G/\ker(f)=\{g\ker(f): g \in G\}$。构造从 $G/\ker(f)$ 到 G' 的映射 φ：

$$\varphi(g\ker(f)) = f(g)$$

需要证明映射 φ 是一一映射且保持运算。

(1) 映射 φ 是满射。

这是因为 f 是群 G 到群 G' 的满同态映射，所以在 G' 任意元素 g' 都存在 $g \in G$ 满足 $f(g)=g'$。

同样地，映射 φ 是单射。

这是因为如果存在 $g\ker(f) \neq h\ker(f)$，但是 $\varphi(g\ker(f))=\varphi(h\ker(f))$，那么有 $f(g)=f(h)$，$gh^{-1} \in \ker(f)$。

所以有 $gh^{-1} \in \ker(f)$，则 $g\ker(f)=h\ker(f)$。

这与 $g\ker(f) \neq h\ker(f)$ 矛盾。

所以映射 φ 是一一映射。

(2) 下面证明映射 φ 是保持运算的。

设 $g\ker(f)$、$h\ker(f) \in G/\ker(f)$，则 $\varphi(g\ker(f))=f(g)$，$\varphi(h\ker(f))=f(h)$。

那么由于 f 是群 G 到群 G' 的同态映射，得

$$\varphi(g\ker(f))\varphi(h\ker(f)) = f(g)f(h) = f(gh) = \varphi((g\ker(f))(h\ker(f)))$$

由(1)、(2)得到 $G/\ker(f)\cong G'$。

3.4 正规子群与商群

前面介绍了陪集的概念,希望在陪集组成的集合上定义二元运算,使之构成群,但并不是任何子群都能达到此目的。

定义 3-3 设 H 是群 G 的子群。如果 H 的每一个左陪集也是右陪集,即对于任意 $a\in G$,总有

$$aH = Ha \tag{3-4}$$

则称 H 为 G 的**正规子群**,或**不变子群**。

显然阿贝尔(Abel)群的所有子群是正规子群,但是反之不一定成立。

对于一般群和其子群,有下述定理。

定理 3-8 设 H 是群 G 的子群。则下面 4 个命题是等价的。

(1) H 是群的正规子群。

(2) 对于任意 $a\in G$,总有

$$aHa^{-1} = H$$

(3) 对于任意 $a\in G$ 及任意 $h\in H$,总有

$$aha^{-1} \in H$$

(4) 对于任意 $a\in G$,总有

$$aHa^{-1} \subseteq H$$

证明:通过证明(1)⇒(2)⇒(3)⇒(4)⇒(1),从而证明 4 个命题等价。

(1)⇒(2):如果 H 是正规子群,则

$$aHa^{-1} = (aH)a^{-1} = (Ha)a^{-1} = H(aa^{-1}) = He = H$$

(2)⇒(3):显然。

(3)⇒(4):也是显然。

(4)⇒(1):由 $aHa^{-1}\subseteq H$,得 $aH\subseteq Ha$;又由 $a^{-1}Ha\subseteq H$(注意对于任意 $a\in G$,有 $aHa^{-1}\subseteq H$,而 $a^{-1}\in G$,所以 $a^{-1}Ha\subseteq H$),得 $Ha\subseteq aH$。故

$$Ha = aH$$

定理证毕。

定理 3-8 表明,子群是正规子群的充分必要条件是(2)或者(3)或者(4)。

由 3.2 节的例 3-5 知道,正整数 m 的所有倍数的集合 M 是整数加群 Z 的子群,由于 Z 是阿贝尔(Abel)群,所以 M 是正规子群。现在指出,M 的全部陪集即模 m 剩余类集合

$$\{\overline{0},\overline{1},\overline{2},\cdots,\overline{m-1}\}$$

之所以构成一个群,正是因为 M 是 Z 的正规子群。下面探讨一般情形。

先在群中定义子集合的运算。

定义 3-4 设 A、B 是群 G 中的两个子集合,定义**子集合 *A* 和 *B* 的乘积**为

$$AB = \{ab \mid a \in A, b \in B\} \tag{3-5}$$

即为 A 中元素和 B 中元素相乘得到的集合。

显然子集乘积满足结合律:

$$(AB)C = A(BC)$$

如果 A 是一个子群，$b\in G$，令 $B=\{b\}$，则 A 的左陪集 bA 可表示为 BA。因此就定义了陪集的乘法。

在这个定义基础上有下面的定理。

定理 3-9　设 H 是群 G 的一个子群，H 是正规子群的充分必要条件是任意两个左(右)陪集的乘积仍然是一个左(右)陪集。

证明：如果 H 是正规子群，aH 和 bH 是 H 的两个左陪集，则

$$(aH)(bH)=a(Hb)H=a(bH)H=abH$$

反之，如果$(aH)(bH)$是一陪集，假设

$$(aH)(bH)=cH$$

因为 $e\in H\Rightarrow a\in aH$ 和 $b\in bH$，则

$$ab\in(aH)(bH)=cH$$

由于陪集可由其中任一元素确定，于是有

$$(aH)(bH)=cH=abH$$

两边同乘 a^{-1}，得

$$HbH=bH$$

由于 $e\in H$，则

$$Hb=Hb\{e\}\subseteq HbH$$

于是

$$Hb\subseteq bH$$

实际上对于任意 $b\in G$ 都有

$$HbH=bH$$

则有

$$Hb^{-1}H=b^{-1}H$$

由 $e\in H$，则

$$Hb^{-1}\subseteq Hb^{-1}H=b^{-1}H$$

两边分别左乘和右乘 b，得

$$bH\subseteq Hb$$

综合之，得

$$bH=Hb$$

H 是一个正规子群。定理证毕。

现在可以解决一个正规子群的陪集是否成为一个群的问题。

定理 3-10　如果 H 是群 G 的正规子群，则 H 的全体陪集

$$\{aH\mid a\in G\}$$

对于群子集的乘法构成群。这个群称为 ***G* 对正规子群 *H* 的商群**，记为 G/H。

证明：显然运算满足结合律。由于定理 3-9，封闭性满足。

$eH=H$ 是单位元，因为对于任意 $a\in G$，都有

$$H(aH)=H(Ha)=(HH)a=Ha=aH$$

每个 aH 都具有逆元 $a^{-1}H$，因为

$$(a^{-1}H)(aH)=a^{-1}(Ha)H=a^{-1}(aH)H=(a^{-1}a)HH=H$$

故全体陪集是一个群。

如果 G 是有限群,则 $|G/H|$ 是 H 在 G 中的指数,于是有

$$|G/H| = \frac{|G|}{|H|}$$

这就是为什么 $|G/H|$ 称为商群的原因。

做一个从 G 到 G/H 的映射:f:对于任意 $a \in G$,

$$f(a) = aH$$

f 是一个满射,而且保持运算,即对于任意 a、$b \in G$,总有

$$f(ab) = (ab)H = (aH)(bH) = f(a)f(b)$$

所以 f 是 G 到 G/H 的满同态,称为**自然同态**。于是发现,任何群都与它的商群同态。

习题 3

题 3-1 在 G 到 G' 的一个同态映射之下:$a \to a'$,a 和 a' 的阶是否一定相同?

题 3-2 证明:

(1) 在一个有限群里,阶大于 2 的元素的个数一定是偶数。

(2) 假设 G 是一个阶为偶数的有限群,则 G 中阶为 2 的元素个数一定为奇数。

题 3-3 求三次对称群 S_3 的所有元素的阶。

题 3-4 求出三次对称群 S_3 的所有元素生成的循环子群。

题 3-5 假设 a 生成一个阶为 n 的循环群 G。证明:如果 $(m,n)=1$,a^m 也生成 G。

题 3-6 假设 G 是循环群,并且 G 与 G' 满同态。证明 G' 也是循环群。

题 3-7 假设 G 是无限阶循环群,G' 是任意循环群。证明 G 与 G' 同态。(提示:将 G' 分为无限循环群和有限循环群分别证明)

题 3-8 分别求出 13、16 阶循环群各个元素的阶,指出其中的生成元。

题 3-9 分别求 15、20 阶循环群的真子群。

题 3-10 参考第 2 章题 2-4,建立模 8 剩余类群的运算表。

题 3-11 证明:设 p 是一个素数,任意两个 p 阶群都同构。

题 3-12 证明:设 p 是一个素数,则阶是 p^m 的群一定有一个阶为 p 的子群。

题 3-13 a、b 是一个群 G 的元素,并且 $ab=ba$;又假设 a 的阶为 m,b 的阶为 n,且 $(m,n)=1$。证明 ab 的阶是 mn。

题 3-14 四次对称群 S_4 的一个 4 阶子群如下:

$$H = \{(1),(12)(34),(13)(24),(14)(23)\}$$

求出 H 的全部左陪集。

题 3-15 证明:两个正规子群的交还是正规子群。

题 3-16 证明:指数是 2 的子群一定是正规子群。

题 3-17 假设 H 是 G 的子群,N 是 G 的正规子群,证明 HN 是 G 的子群。

题 3-18 基于加法和加法群对第 2 章和本章内容进行归纳总结。加法群中的单位元用 0 表示,元素 a 的逆元用 $-a$ 表示。(通过该练习可以加深巩固对群论的熟悉和理解,建议初学的读者完成好该练习)