互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

第二章　群

在数学中没有几个概念比合成法则更加本质.

——Nicolas Bourbaki

第一节　合成法则

集合 S 上的合成法则就是将 S 中的元素 a，b 结合成另外一个元素，比如说 p. 这个概念的模型是实数的加法和乘法. $n\times n$ 矩阵集合上的乘法是另一个例子.

规范地，合成法则是一个有两个变量的函数或映射：

$$S\times S\to S$$

此处 $S\times S$ 表示集合的积集，它的元素是集合 S 中的元素对.

合成法则作用在元素对 a，b 上所得到的元素通常用类似乘法或加法的记号表示：

$$p=ab,a\times b,a\circ b,a+b$$

或者其他什么符号，具体使用什么符号依所讨论的问题而定. 元素 p 可以叫做 a，b 的积或和，这取决于所采用的记号是乘还是加.

多数情形我们采用乘法记号 ab. 任何采用乘法记号的结果都可以用其他符号(如加法等)改写，结果同样成立. 改写只是个记号变化.

现在就把 ab 看成集合 S 上的某个特定元素，即由 S 中的元素 a，b 应用合成法则得到的. 因此，如果合成法则是矩阵的乘法，且如果 $a=\begin{bmatrix}1&3\\0&2\end{bmatrix}$，$b=\begin{bmatrix}1&0\\2&1\end{bmatrix}$，则 ab 表示矩阵 $\begin{bmatrix}7&3\\4&2\end{bmatrix}$. 一旦计算出积 ab，那么 a，b 就不能从积中复原.

用乘法记号，合成法则的结合律是指：

【2.1.1】　$$(ab)c=a(bc)\qquad(\text{结合律})$$

对于 S 中的任意 a，b，c 成立. 此处 $(ab)c$ 是指先算 a 与 b 的乘积 ab，再计算 ab 与 c 的乘积. 合成法则的交换律是指：

【2.1.2】　$$ab=ba\qquad(\text{交换律})$$

对于 S 中的任意 a，b 成立. 矩阵乘法满足结合律但不满足交换律.

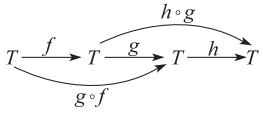
通常用改变 a，b 在加法 $a+b$ 中的顺序来表示交换律，即 $a+b=b+a$ 对任意 a，b 成立. 乘法记号对于交换律没有特别的含义.

结合律比交换律更基础，一个原因是函数的复合满足结合律. 令 T 是一个集合，g 和 f 是 T 到 T 的映射(或者函数)，令 $g\circ f$ 表示复合映射 $t\rightsquigarrow g(f(t))$：先用 f 作用再用 g 作用. 规则

互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

$$g, f \rightsquigarrow g \circ f$$

是映射 $T \to T$ 的集合上的复合运算. 该复合运算满足结合律. 若 f, g 和 h 是 T 到 T 的三个映射, 则 $(h \circ g) \circ f = h \circ (g \circ f)$:



两个复合映射都把元素 t 映射为 $(h(g(f(t))))$.

当 T 只包含两个元素时, 比如 $T=\{a, b\}$, 则存在 T 到 T 的四个映射:

i: 恒等映射, 定义为 $i(a)=a$, $i(b)=b$;

τ: 对换, 定义为 $\tau(a)=b$, $\tau(b)=a$;

α: 常函数, $\alpha(a)=\alpha(b)=a$;

β: 常函数, $\beta(a)=\beta(b)=b$.

映射 $T \to T$ 的集合 $\{i, \tau, \alpha, \beta\}$ 上的合成法则由下面的乘法表给出:

【2.1.3】

	i	τ	α	β
i	i	τ	α	β
τ	τ	i	β	α
α	α	α	α	α
β	β	β	β	β

合成的方式如下:

		f
		⋮
g	…	$g \circ f$

38

因此 $\tau \circ \alpha = \beta$, 而 $\alpha \circ \tau = \alpha$. 函数的复合不满足交换律.

回到一般的合成法则, 假设我们要求一个集合中 n 个元素的乘积 $a_1 a_2 \cdots a_n$=? 有许多种不同的方式计算这个乘积. 例如, 可以先求积 $a_1 a_2$, 然后再和第三个元素 a_3 相乘, 以此类推:

$$((a_1 a_2) a_3) a_4 \cdots$$

也有其他的方法给出按照指定顺序的这些元素的乘积. 但如果乘法运算满足结合律, 则所有计算结果都是 S 中的同一个元素. 这使得我们可以探讨任意元素串的乘积.

【2.1.4】命题 令集合 S 上的合成法则满足结合律. 则有唯一一种方式来定义 S 中任意 n 个元素 a_1, a_2, $\cdots a_n$ 的乘积, 暂时记作 $[a_1 a_2 \cdots a_n]$, 这个乘积具有以下性质:

(i) 一个元素的积是其自身: $[a_1]=a_1$.

(ii) 两个元素的积 $[a_1 a_2]$ 由合成法则给出.

(iii) 对于任意整数 i: $1 \leqslant i < n$, 有 $[a_1 a_2 \cdots a_n] = [a_1 \cdots a_i][a_{i+1} \cdots a_n]$.

互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

方程(iii)右边是先算两个积$[a_1\cdots a_i]$和$[a_{i+1}\cdots a_n]$，然后这两个积再按照合成法则计算其乘积.

证明 对 n 用数学归纳法. (i)和(ii)已经定义了 $n\leqslant 2$ 的乘积. 当 $n=2$ 时(iii)成立. 假设当 $r\leqslant n-1$ 已经定义了 r 个元素的乘积且乘积是唯一的并满足(iii)，然后按照下面的规则定义 n 个元素的乘积：

$$[a_1\cdots a_n]=[a_1\cdots a_{n-1}][a_n]$$

其中右边的项已经定义好了. 如果满足(iii)的乘积存在，那么这个公式给出了积，这正是(iii)中当 $i=n-1$ 的情形. 故若 n 个元素的乘积存在，积就是唯一的. 我们必须检验(iii)对于 $i<n-1$ 成立.

$$\begin{aligned}[a_1\cdots a_n]&=[a_1\cdots a_{n-1}][a_n] && (\text{定义})\\ &=([a_1\cdots a_i][a_{i+1}\cdots a_{n-1}])[a_n] && (\text{归纳假设})\\ &=[a_1\cdots a_i]([a_{i+1}\cdots a_{n-1}][a_n]) && (\text{结合律})\\ &=[a_1\cdots a_i][a_{i+1}\cdots a_n] && (\text{归纳假设})\end{aligned}$$

至此完成了证明. 从现在起，在表示乘积时将省去括号而直接记为 $a_1\cdots a_n$. ■

集合 S 中的元素 e 称为合成法则的恒等元，如果 e 满足

【2.1.5】 $$ea=a \text{ 与 } ae=a, \text{对所有 } a\in S$$

至多有一个恒等元，因为若 e 和 e' 是两个恒等元，则由于 e 是恒等元，故 $ee'=e'$，又有 e' 也是恒等元，故 $e=ee'$. 因此 $e=ee'=e'$.

矩阵乘法和函数的复合都有恒等元，对于 $n\times n$ 矩阵，它是恒等矩阵 I，对于 $T\to T$ 的映射集合，它是恒等映射——将元素映射为自身的映射是恒等映射.

39

注 如果合成法则用乘法表示，则恒等元通常用 1 来表示；如果合成法则用加法表示，则恒等元用 0 来表示. 这些元素与数字 1 和 0 无关，但是在合成法则中起到恒等元的作用.

假设集合 S 上定义了一个满足结合律且有恒等元 1 的合成法则，并记作乘法. S 中的元素 a 是可逆的如果存在另一个元素 b 使得

$$ab=1 \quad 与 \quad ba=1$$

且如果上式成立，则 b 称为 a 的逆. 元素 a 的逆记作 a^{-1}，或当合成法则用加法记时，逆记作 $-a$.

下面不加证明地列出了逆的性质. 除去最后一条性质外，其他性质在矩阵中已经讨论过. 作为最后一个性质的示例，参看练习 1.3.

- 如果 a 有左逆 l 和右逆 r，即 $la=1$ 和 $ar=1$，则 $l=r$，a 是可逆的，且 r 是其逆.
- 如果 a 是可逆的，则其逆是唯一的.
- 乘积的逆按照相反次序：如果 a 和 b 均可逆，则乘积 ab 可逆，且

$$(ab)^{-1}=b^{-1}a^{-1}$$

- 一个元素 a 可以有左逆或右逆，尽管它是不可逆的.

幂记号可以用于满足结合律的运算：当 $n>0$ 时，$a^n=a\cdots a$(n 个因子)，$a^{-n}=a^{-1}\cdots$

互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

a^{-1}，且 $a^0=1$. 通常的幂运算律成立：$a^r a^s=a^{r+s}$，且$(a^r)^s=a^{rs}$. 当合成法则用加法表示时，幂运算记号 a^n 改用记号 $na=a+\cdots+a$.

除非合成法则满足交换律，否则不建议采用分式记号$\frac{a}{b}$，因为不知道这个分式记号所指的是 ba^{-1}还是 $a^{-1}b$，而这二者可以是不同的.

第二节 群与子群

一个群是一个带有下列性质的合成法则的集合 G：

- 合成法则满足结合律：$(ab)c=a(bc)$对 G 中任意 a，b，c 成立.
- G 包含单位元 1，使得对于 G 中任意元素 a 有 $1a=a1=a$.
- G 中任意元素 a 均有逆，即存在元素 b 使得 $ab=ba=1$.

阿贝尔群是合成法则交换的群.

例如，非零实数的集合按照乘法构成的群和实数集合按照加法构成的群都是阿贝尔群. 所有 $n\times n$ 可逆矩阵集合按照矩阵乘法合成法则构成一般线性群，但不是交换群，除非 $n=1$.

当满足复合运算律时，通常把表示该集合的群和该集合用同一个符号表示.

群 G 的阶是其包含的元素个数，通常记作$|G|$：

40 【2.2.1】 $|G|=G$ 的元素个数，G 的阶

如果 G 的阶是有限的，则 G 称为有限群；否则称为无限群. 同样的术语适用于集合. 一个集合 S 的阶$|S|$是 S 中所含的元素个数.

下面列出我们熟悉的一些无限交换群的记号：

【2.2.2】 $\mathbf{Z}^+$：整数集合，加法作为它的复合法则 — 整数加群，

$\mathbf{R}^+$：实数集合，加法作为它的复合法则 — 实数加群，

$\mathbf{R}^\times$：非零实数集合，乘法作为它的复合法则 — 实数乘法群，

$\mathbf{C}^+$，$\mathbf{C}^\times$：类似的群，用复数集合 $\mathbf{C}$ 代替实数集合 $\mathbf{R}$.

注意 也有用 $\mathbf{R}^+$ 来表示正实数集合的. 为了避免混淆，最好用记号$(\mathbf{R},+)$来表示实数加群，即具体地把合成法则表示出来. 但是，我们的记号更紧凑. 此外，用符号 $\mathbf{R}^\times$ 表示非零实数乘法构成的群. 所有实数在乘法下不构成群，因为 0 没有逆.

【2.2.3】命题（消去律） 令 a，b，c 是群 G 中的元素，群 G 的合成法则用乘法表示. 若 $ab=ac$或 $ba=ca$，则 $b=c$. 若 $ab=a$ 或 $ba=a$，则 $b=1$.

证明 $ab=ac$ 两边左乘 a^{-1}得到 $b=c$. 其他证明类似. ■

这个证明中用 a^{-1}左乘很关键. 若元素 a 不可逆，则消去律不一定成立. 例如，

$$\begin{bmatrix}1 & 1\\ & \end{bmatrix}\begin{bmatrix}1 & 1\\ 2 & \end{bmatrix}=\begin{bmatrix}1 & 1\\ & \end{bmatrix}\begin{bmatrix}3 & \\ & 1\end{bmatrix}$$

互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

两个基本的群的例子是由前面讨论过的合成法则——矩阵乘法和函数的合成——通过把不可逆的元素去掉而得到.

注 $n\times n$ 一般线性群是由所有 $n\times n$ 可逆矩阵构成的群. 将它记为

【2.2.4】 $$GL_n=\{n\times n \text{ 可逆矩阵 } A\}$$

如果我们希望指出考虑的是实数矩阵还是复数矩阵，则把它们相应地记为 $GL_n(\mathbf{R})$ 或 $GL_n(\mathbf{C})$.

令 M 表示集合 T 到自身的映射的集合. 映射 $f:T\to T$ 有逆函数当且仅当它是一一映射. 这样的映射也称为 T 的一个置换. 置换的集合在映射合成法则下构成一个群. 如在第一章第五节中一样，置换的合成用乘法表示，即用 qp 表示 $q\circ p$.

注 指标集合{**1**，**2**，…，***n***}的置换群称为对称群，记作 S_n：

【2.2.5】 $$S_n \text{ 是指标 } \mathbf{1},\mathbf{2},\cdots,\boldsymbol{n} \text{ 的置换群}$$ 41

n 个元素的集合共有 $n!$（n 的阶乘$=1\cdot 2\cdot 3\cdot\cdots\cdot n$）个置换，所以对称群 S_n 是阶为 $n!$ 的有限群.

集合{a，b}的置换由恒等置换 i 和对换 τ 构成，形成一个二阶群. 如果用 **1** 代替 a，用 **2** 代替 b，就得到二阶对称群 S_2. 实际上只有一个二阶群 G. 为了说明这一点，注意到群中有一个恒等元 1 和另一个元素 g. 群的乘法表中有 4 个元素 11，1g，g1 和 gg. 除去 gg，其他元素都由恒等元性质得出. 而且由消去律有 $gg\neq g$. 仅有一种可能，就是 $gg=1$. 故乘法表完全确定. 只有一个群运算律.

下面我们描述对称群 S_3. 这个群是六阶群，可以作为按照合成法则构成的最小的非交换群的例子. 后面会经常用到这个群. 为了刻画这个群，选取两个特殊的置换来表示其他的置换. 取循环置换(**1 2 3**)和对换(**1 2**)，并分别用 x 和 y 表示. 容易验证

【2.2.6】 $$x^3=1,y^2=1,yx=x^2y$$

利用消去律，可以看到 6 个元素 1，x，x^2，y，xy，x^2y 是不同的. 所以群 S_3 有 6 个元素：

【2.2.7】 $$S_3=\{1,x,x^2;y,xy,x^2y\}$$

在以后，我们会把(2.2.6)和(2.2.7)作为对称群 S_3 的“一般表示”. 注意 S_3 不满足交换律，因为 $yx\neq xy$.

法则(2.2.6)也可直接验证，对 S_3 的计算有它们就足够了. 不断应用上面的法则，x，y 以及其逆的任意积都等于(2.2.7)中某个元素. 为此，用最后一个法则把所有出现的 y 移到右边，而用前面两个法则使其幂变小. 例如：

【2.2.8】 $x^{-1}y^3x^2y=x^2yx^2y=x^2(yx)xy=x^2(x^2y)xy=xyxy=x(x^2y)y=1$

用这些法则可以写出 S_3 的乘法表. 因此，这些法则称为群的定义关系，我们会在第七章正式学习这一概念.

我们到此为止. S_n 的结构随着 n 的增加变得非常复杂.

一般线性群和对称群如此重要的一个原因，是许多其他群都作为子群包含在它们之中. 群 G 的子集 H 称为一个子群，如果它具有下列性质：

互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

【2.2.9】

- 封闭性：若 $a\in H$ 并且 $b\in H$，则 $ab\in H$.
- 恒等元：$1\in H$.
- 逆元：若 $a\in H$，则 $a^{-1}\in H$.

对这些条件解释如下：第一个条件告诉我们可以用 G 上的合成法则在 H 上定义一个合
42 成法则，称为诱导法则. 第二个和第三个条件指出 H 关于这个诱导法则构成一个群. 注意，(2.2.9)提到了群定义中除了结合律的所有要点. 因为结合律自动地由 G 转移到 H，我们不需要再提及它.

注意

(i) 在数学上，学习每一个术语的定义非常重要. 有直觉是不够的. 例如2×2可逆上三角矩阵的集合 T 是一般的线性群 GL_2 的子群. 只有一种方法证明，就是回到定义. 确实 T 是 GL_2 的子集. 验证任意两个可逆上三角矩阵的乘积还是可逆上三角矩阵，恒等矩阵是上三角的，可逆上三角矩阵的逆矩阵还是上三角的可逆矩阵. 当然这些都容易验证.

(ii) 封闭性作为群的一个公理指的是群 G 中任意两个元素的乘积 ab 仍是群中的元素. 我们把封闭性包含在合成法则中. 这样在群的定义中就不必单独指出运算的封闭性了.

【2.2.10】**例**

(a) 绝对值为 1 的复数的集合——复平面的单位圆上点的集合——是乘法群 $\mathbf{C}^\times$ 的子群，称为圆群.

(b) 所有行列式为 1 的 $n\times n$ 实矩阵构成一般线性群 GL_n 的子群，称为特殊线性群，记为 SL_n：

【2.2.11】 $SL_n(\mathbf{R})$ 是所有行列式为 1 的实 $n\times n$ 矩阵 A 的集合

对于这个特殊线性群，定义(2.2.9)中的性质很容易验证，这里省去验证过程. ■

注 每个群 G 都有两个明显的子群：群 G 自身和由单独一个恒等元构成的平凡子群 $\{1\}$. 一个子群如果不是这两个子群之一，则称为真子群.

第三节 整数加群的子群

这里我们用整数加群 $\mathbf{Z}^+$ 的子群回顾一些基本的数论理论. 首先，列出群运算用加法表示时子群用到的公理：一个用加法表示合成法则的群 G 的子集 S 是一个子群，如果满足下列性质：

【2.3.1】

- 封闭性：如果 a，$b\in S$，则 $a+b\in S$；
- 单位元：$0\in S$；
- 逆元：若 $a\in S$，则 $-a\in S$.

令 a 是异于 0 的整数. 记由所有 a 的倍数构成的 $\mathbf{Z}$ 的子集为 $\mathbf{Z}a$：

【2.3.2】 $$\mathbf{Z}a=\{n\in\mathbf{Z}\mid \text{存在 } k\in\mathbf{Z},\text{使 } n=ka\}$$

43 这是整数加群 $\mathbf{Z}^+$ 的子群. 它的元素也可以描述为被 a 整除的整数.

互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

【2.3.3】定理 令 S 是整数加群 $\mathbf{Z}^+$ 的子群. 则 S 或为平凡子群$\{0\}$，或是有形式 $\mathbf{Z}a$，其中 a 为 S 中最小正整数.

证明 令 S 是 $\mathbf{Z}^+$ 的一个子群. 则 $0\in S$. 如果 0 是 S 中唯一的元素，则 S 为平凡子群. 因而对这一情形结论成立. 否则，S 包含异于 0 的整数 n，且要么 n 是正数，要么 $-n$ 是正数. 由子群的第三个性质知：$-n\in S$. 故 S 含有正整数. 我们必须证明 $S=\mathbf{Z}a$，其中 a 为 S 中最小正整数.

首先证明 $\mathbf{Z}a$ 是 S 的子集，换句话说，$ka\in S$ 对于任意整数 k 成立. 如果 k 是正整数，则 $ka=a+a+\cdots+a$(k 项). 由于 $a\in S$，由子群的封闭性和归纳法知 $ka\in S$. 子群中元素的逆元仍属于 S，因此 $-ka\in S$. 最后，$0a=0\in S$.

其次，证明 S 是 $\mathbf{Z}a$ 的子集，即 S 中任意元素 n 是 a 的整数倍. 用带余除法，记 $n=qa+r$，其中 q，r 都是整数且余数 r 的取值范围为 $0\leqslant r<a$. 由于 $\mathbf{Z}a\subseteq S$，故 $qa\in S$，当然 $n\in S$. 因为 S 是子群，故也有 $r=n-qa\in S$. 现在，根据我们的选取，a 为 S 中最小正整数，而余数 r 满足 $0\leqslant r<a$. 因此，属于 S 的唯一余数是 0. 所以，$r=0$ 且 n 是 a 的整数倍数 qa. ■

这一刻画导致定理 2.3.3 在两个整数 a，b 生成的子群上的一个惊人的应用. 设 a 和 b 都非零整数. 由 a 和 b 的所有整数组合 $ra+sb$ 构成的集合

【2.3.4】
$$S=\mathbf{Z}a+\mathbf{Z}b=\{n\in Z\mid n=ra+sb,\text{其中 } r,s \text{ 是任意整数}\}$$
是 $\mathbf{Z}^+$ 的子群，这时子群被称为由 a，b 生成的子群，因为它是同时包含这两个元素的最小子群. 设 a，b 是不全为零的整数，故 S 不是平凡子群$\{0\}$. 定理 2.3.3 告诉我们存在某个正整数 d，使这个子群具有 $\mathbf{Z}d$ 的形式，它是能被 d 整除的整数的集合. 生成元 d 叫做 a 与 b 的最大公因数，原因在下面命题的(a)和(b)中给出. a 与 b 的最大公约数记作 $\gcd(a,b)$.

【2.3.5】命题 设 a，b 是不全为零的整数，并设 d 是 a 与 b 的最大公约数，且是生成子群 $S=\mathbf{Z}a+\mathbf{Z}b$ 的正整数，则有 $\mathbf{Z}d=\mathbf{Z}a+\mathbf{Z}b$. 则

(a) d 整除 a 与 b.

(b) 若整数 e 整除 a 和 b，则 e 整除 d.

(c) 存在整数 r 和 s，使 d 可以写为 $d=ra+sb$ 的形式.

证明 (c)部分是 d 属于 $\mathbf{Z}a+\mathbf{Z}b$ 的另一种说法. 其次，注意到 a，b 都在子群 $S=\mathbf{Z}d$ 中，因而 d 整除 a 与 b. 最后，若 e 是整除 a 和 b 的整数，则 e 整除整数 a 和 b 的线性组合 $ra+sb$. 由假设，$d=ra+sb$，故 e 整除 d. ■

注意 e 整除 a 和 b，则 e 整除任何具有形式 $ma+nb$ 的整数. 故(c)蕴含(b). 但(b)不蕴含(c). 正如我们将看到的，性质(c)是个功能强大的工具.

反复使用带余除法容易求得最大公约数. 例如，若 $a=314$，$b=136$，则

$$314=2\cdot 136+42,\quad 136=3\cdot 42+10,\quad 42=4\cdot 10+2$$

44

利用这些方程中的第一个，可以证明 314 和 136 的线性组合可以由 136 与 42 的线性组合来表示，反之亦然. 故 $\mathbf{Z}(314)+\mathbf{Z}(136)=\mathbf{Z}(136)+\mathbf{Z}(42)$，因此 $\gcd(314,136)=\gcd(136,42)$. 类似地，$\gcd(136,42)=\gcd(42,10)=\gcd(10,2)=2$. 故 314 与 136 的最大

互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

公约数为 2. 这种求两个整数的最大公约数的迭代法叫做欧几里得算法.

如果给出了整数 a，b，则第二种求这两个数的最大公约数的方法是求得每一个整数的素整数分解，然后将所有公共的素因子收集起来. 命题 2.3.5 中的性质(a)和(b)用这种方法很容易验证. 但是没有定理 2.3.3，性质(c)，即由这种方法确定的最大公约数 d 是 a 和 b 的线性组合这个性质并不是显然的. 这里我们并不做进一步讨论. 在第十二章我们再回来讨论它.

两个非零整数 a 和 b 称为是*互素的*，如果仅有唯一的正整数 1 同时整除这两个数. 这样，它们的最大公约数是 1：$\mathbf{Z}a+\mathbf{Z}b=\mathbf{Z}$.

【2.3.6】推论 *一对整数 a 和 b 互素当且仅当存在整数 r 和 s 使得 $ra+sb=1$.*

【2.3.7】推论 *令 p 是一个素整数. 若 p 整除 a 与 b 的乘积 ab，则 p 整除 a 或者 p 整除 b.*

证明 假设素数 p 整除 ab，但不整除 a. p 仅有的正因子是 1 和 p. 因 p 不整除 a，故 $\gcd(a,\ p)=1$. 因此有整数 r 和 s 使得 $ra+sp=1$. 两边同乘以 b：$rab+spb=b$，注意到 p 整除 rab 和 spb，故 p 整除 b. ■

有一个与整数对 a，b 有关的 $\mathbf{Z}^+$ 的子群，即交集 $\mathbf{Z}a\cap\mathbf{Z}b$，它是包含在 $\mathbf{Z}a$ 和 $\mathbf{Z}b$ 中的整数的集合. 现在假设 a，b 均非零，则 $\mathbf{Z}a\cap\mathbf{Z}b$ 是一个子群. 它不是平凡子群$\{0\}$，因为它包含乘积 ab，而 ab 不是零. 故 $\mathbf{Z}a\cap\mathbf{Z}b$ 对于某个正整数 m 具有形式 $\mathbf{Z}m$. 这个整数 m 称为 a，b 的*最小公倍数*，记作 $\mathrm{lcm}(a,\ b)$，原因由下面的命题给出.

【2.3.8】命题 *令 a 和 b 是非零整数，且 m 是它们的最小公倍数——正整数生成子群 $S=\mathbf{Z}a\cap\mathbf{Z}b$. 故 $\mathbf{Z}m=\mathbf{Z}a\cap\mathbf{Z}b$. 则*

(a) m 被 a 和 b 整除.

(b) 如果 n 被 a 和 b 整除，则 n 被 m 整除.

证明 上述两个断言均得证于事实：一个整数被 a 与 b 整除当且仅当这个整数属于集合 $\mathbf{Z}m=\mathbf{Z}a\cap\mathbf{Z}b$. ■

【2.3.9】推论 *令 $d=\gcd(a,\ b)$和 $m=\mathrm{lcm}(a,\ b)$分别是正整数对 a 与 b 的最大公约数和最小公倍数. 则 $ab=dm$.*

证明 由于 b/d 是一个整数，故 a 整除 ab/d. 类似地，b 整除 ab/d. 故 m 整除 ab/d，且 dm 整除 ab. 其次，记 $d=ra+sb$. 则 $dm=ram+sbm$. 右边两项均能被 ab 整除，所以 ab 整除 dm. 由于 ab 和 dm 都是正数且相互整除，故 $ab=dm$. ■

45

第四节 循 环 群

现在看一个重要的抽象子群的例子，即由 G 中任意一个元素 x 生成的*循环子群*. 我们用乘法的记号，由 x 生成的循环子群 H 是 x 的所有幂的元素的集合：

【2.4.1】
$$H=\{\cdots,x^{-2},x^{-1},x,x^2,\cdots\}$$

它是 G 的包含 x 的最小子群，经常记作$\langle x\rangle$. 但是想正确地解释(2.4.1)，必须记住 x^n 是 G 中某个元素的记号，它是以某种特定方式得到的. 不同的幂可以表示同一个元素. 例如，若群 G 是乘法群 $\mathbf{R}^\times$，且 $x=-1$，则列出的所有元素都等于 1 或 -1，且 H 就是集合$\{1,\ -1\}$.

互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

有两种情形：x 的幂 x^n 都是互不相同的元素，或不是互不相同的元素．我们分析 x 的幂都是互不相同的情形．

【2.4.2】命题 令$\langle x\rangle$是群 G 的由元素 x 生成的循环子群，且令 S 表示满足 $x^k=1$ 的整数 k 的集合．

(a) 集合 S 是整数加群 $\mathbf{Z}^+$ 的子群．

(b) 两个幂 $x^r=x^s$ 对于 $r\geqslant s$ 成立当且仅当 $x^{r-s}=1$，即当且仅当 $r-s\in S$．

(c) 假设 S 是非平凡子群，则 $S=\mathbf{Z}n$ 对某个正整数 n 成立．则幂 1，x，x^2，…，x^{n-1} 是子群$\langle x\rangle$中不同的元素，且$\langle x\rangle$的阶为 n．

证明

(a) 如果 $x^k=1$ 且 $x^l=1$，则有 $x^{k+l}=x^kx^l=1$．这表明若 k，$l\in S$，则 $k+l\in S$．于是子群的第一个性质(2.3.1)成立．因为 $x^0=1$，故 $0\in S$．最后，若 $k\in S$，即 $x^k=1$，则 $x^{-k}=(x^k)^{-1}=1$．从而，$-k\in S$．

(b) 由消去律 2.2.3 可得．

(c) 设 $S\neq\{0\}$．定理 2.3.3 表明 $S=\mathbf{Z}n$，其中 n 为 S 中最小正整数．如果 x^k 是任意幂，用 n 去除 k，记作 $k=qn+r$，$0\leqslant r<n$．则 $x^{qn}=1^q=1$ 且 $x^k=x^{qn}x^r=x^r$．因此 x^k 是 1，x，x^2，…，x^{n-1}之一．从(b)知，这些幂是不同的，因为 x^n 是满足 $x^n=1$ 的最小正整数．■

在这个命题的(c)中描述的群$\langle x\rangle=\{1,x,x^2,\cdots,x^{n-1}\}$称为 n 阶循环群．之所以叫做循环群是因为群中的元素由 x 反复相乘重复得到其中的 n 个元素．

群中的一个元素 x 有阶 n，如果 n 是满足满足 $x^n=1$ 的最小正整数，这等价于说由 x 生成的循环子群$\langle x\rangle$有阶 n．

使用对称群 S_3 通常的记号，元素 x 有阶 3，元素 y 有阶 2．在任何群中，恒等元是唯一阶为 1 的元素．

46

如果对于任意正整数 n 有 $x^n\neq1$，则称 x 是无限阶的．在 $GL_2(\mathbf{R})$中矩阵$\begin{bmatrix}1&1\\0&1\end{bmatrix}$是无限阶的，而$\begin{bmatrix}1&1\\-1&0\end{bmatrix}$是 6 阶的．

当 x 是无限阶时，群$\langle x\rangle$称为无限循环群．对于无限循环群，没什么好讨论的．

【2.4.3】命题 令 x 是群中阶为 n 的元素，且 k 是一个整数，写成 $k=qn+r$，其中 q 和 r 均为整数，且 $0\leqslant r<n$．

- $x^k=x^r$．
- $x^k=1$ 当且仅当 $r=0$．
- 令 $d=\gcd(k,n)$，则 x^k 的阶等于$\dfrac{n}{d}$．

我们也会讲到群 G 中由子集 U 生成的子群，这是指 G 中包含 U 的最小子群，它由 G

互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

中所有可以表成 U 的元素和它们的逆的串的乘积的元素构成. G 的子集 U 称为生成 G，如果 G 中的元素都可表示成这样的积. 例如，在(2.2.7)中，我们看到子集 $U=\{x, y\}$ 生成对称群 S_3. 初等矩阵生成 GL_n(定理 1.2.16). 在这两个例子中，不需要逆. 但情况并非总如此. 一个由 x 生成的无限循环群$\langle x\rangle$就需要用负幂的元素填满.

克莱因四元群 V 是由四个矩阵

【2.4.4】
$$\begin{bmatrix}\pm 1 & \\ & \pm 1\end{bmatrix}$$

组成的最简单的非循环群. 任意两个不是恒等元的元素生成 V. 四元数群 H 是 $GL_2(C)$中非循环的小子群的例子. 它由八个矩阵

【2.4.5】
$$H=\{\pm\mathbf{1}, \pm\boldsymbol{i}, \pm\boldsymbol{j}, \pm\boldsymbol{k}\}$$

构成，其中

$$\mathbf{1}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix},\quad \boldsymbol{i}=\begin{bmatrix}\mathrm{i} & 0\\ 0 & -\mathrm{i}\end{bmatrix},\quad \boldsymbol{j}=\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix},\quad \boldsymbol{k}=\begin{bmatrix}0 & \mathrm{i}\\ \mathrm{i} & 0\end{bmatrix}$$

这些矩阵可由物理上的 Pauli 矩阵乘以 i 得到. 元素 $\boldsymbol{i}$, $\boldsymbol{j}$ 生成 H，通过计算可得下列公式：

【2.4.6】
$$\boldsymbol{i}^2=\boldsymbol{j}^2=\boldsymbol{k}^2=-\mathbf{1}, \boldsymbol{ij}=-\boldsymbol{ji}=\boldsymbol{k}, \boldsymbol{jk}=-\boldsymbol{kj}=\boldsymbol{i}, \boldsymbol{ki}=-\boldsymbol{ik}=\boldsymbol{j}$$

第五节 同 态

设 G 和 G'为用乘法记号表示的两个群. 一个同态 $\varphi: G\to G'$是 G 到 G'的映射，使得对于 G 中任意元素 a，b 有

47 【2.5.1】
$$\varphi(ab)=\varphi(a)\varphi(b)$$

这个方程左边的意思是

先在 G 中做 a 与 b 的乘积，然后再用 φ 映射到 G'中的元素，

而方程右边的意思是

先把 a 与 b 分别用 φ 映射到 G'中的元素后，再对 G'中的像做乘积.

直观上，一个同态就是两个群中与合成法则相容的映射，它提供了将两个不同的群联系起来的一种方法.

【2.5.2】**例** 下列映射是同态：

(a) 行列式函数 $\det: GL_n(\mathbf{R})\to\mathbf{R}^\times$ (1.4.10).

(b) 符号同态 $\sigma: S_n\to\{\pm 1\}$将置换映射为相应的正负号(1.5.11).

(c) 幂指数映射 $\exp: \mathbf{R}^+\to\mathbf{R}^\times$定义为 $x\rightsquigarrow \mathrm{e}^x$.

(d) 映射 $\varphi: \mathbf{Z}^+\to G$ 定义为 $\varphi(n)=a^n$，其中 a 为 G 中指定元素.

(e) 绝对值映射 $|\ |: \mathbf{C}^\times\to\mathbf{R}^\times$. ■

在例子(c)和(d)中，定义域中的合成法则用加法记号，值域中的用乘法记号. 同态的条件(2.5.1)必须考虑在内. 同态的条件变为

$$\varphi(a+b)=\varphi(a)\varphi(b)$$

互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

这个公式表明指数映射是一个同态，即 $e^{a+b}=e^a e^b$.

需要提及下面的同态，虽然这些同态不太有趣. 平凡同态 $\varphi:G\to G'$ 将 G 中每一个元素映射为 G' 中的恒等元. 若 H 是 G 的子群，则包含映射 $i:H\to G$ 定义为对于任意的元素 $x\in H$，有 $i(x)=x$，这是一个同态.

【2.5.3】命题 令 $\varphi:G\to G'$ 是群同态.

(a) 如果 a_1，…，a_k 是 G 中的元素，则 $\varphi(a_1\cdots a_k)=\varphi(a_1)\cdots\varphi(a_k)$.

(b) φ 把恒等元映射为恒等元：$\varphi(1_G)=1_{G'}$.

(c) φ 把逆元映射为逆元：$\varphi(a^{-1})=\varphi(a)^{-1}$.

证明 第一个断言由定义和归纳法可得. 其次，由于 $1\cdot 1=1$ 及 φ 是同态，故 $\varphi(1)\cdot\varphi(1)=\varphi(1\cdot 1)=\varphi(1)$，由(2.2.3)两边消去 $\varphi(1)$ 得到 $\varphi(1)=1$. 最后，$\varphi(a^{-1})\cdot\varphi(a)=\varphi(a^{-1}\cdot a)=\varphi(1)=1$. 因此 $\varphi(a^{-1})=\varphi(a)^{-1}$. ■

群同态确定了两个重要的子群：像和核.

注 同态 $\varphi:G\to G'$ 的像常记作 $\mathrm{im}\varphi$，它是 φ 的像的集合：

【2.5.4】
$$\mathrm{im}\varphi=\{x\in G'\mid x=\varphi(a),a\in G\}$$

像的另外一个记号是 $\varphi(G)$.

48

映射 $\mathbf{Z}^+\to G$ 将 n 映射为 a^n，该映射的像是由 a 生成的循环子群.

同态的像是其值域的一个子群. 我们验证封闭性，省略其他性质的验证. 设 x 和 y 是像中的元素，这就是说存在两个元素 a，$b\in G$ 使得 $x=\varphi(a)$，$y=\varphi(b)$. 由于 φ 是同态，$xy=\varphi(a)\varphi(b)=\varphi(ab)$. 所以，$xy=\varphi$(某元素)，它也是像中的元素.

注 同态的核更微妙也更重要. φ 的核记作 $\ker\varphi$，是 G 中所有映射到 G' 恒等元的那些元素的集合：

【2.5.5】
$$\ker\varphi=\{a\in G\mid\varphi(a)=1\}$$

核是 G 的子群，因为若 a 和 b 是核中的元素，则 $\varphi(ab)=\varphi(a)\varphi(b)=1\cdot 1=1$，故 ab 也是核中的元素，等等，其他可类似验证.

行列式同态 $GL_n(\mathbf{R})\to\mathbf{R}^\times$ 的核是一个特殊线性群 $SL_n(\mathbf{R})$(2.2.11). 符号同态 $S_n\to\{\pm 1\}$ 的核称为交错群. 它由所有偶置换组成，记作 A_n：

【2.5.6】 交错群 A_n 是偶置换群

核之所以重要是因为它控制了全部同态. 它不仅告诉我们 G 中哪些元素映射为 G' 中的恒等元，而且告诉我们哪些元素对在 G' 中的像是相同的.

注 如果 H 是 G 的子群，且 a 是 G 中元素，则记号 aH 表示所有乘积 ah，$h\in H$ 的全体：

【2.5.7】
$$aH=\{g\in G\mid g=ah,h\in H\}$$

这个集合称为 H 在 G 中的左陪集，“左”指的是元素 a 出现在左边.

【2.5.8】命题 令 $\varphi:G\to G'$ 是一个群同态，a 和 b 是 G 中元素. 令 K 是 φ 的核. 下列条件是等价的：

- $\varphi(a)=\varphi(b)$，

互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

- $a^{-1}b\in K$，
- $b\in aK$，
- 陪集 bK 与陪集 aK 相等.

证明 若 $\varphi(a)=\varphi(b)$，则 $\varphi(a^{-1}b)=\varphi(a^{-1})\varphi(b)=\varphi(a)^{-1}\varphi(b)=1$. 因此 $a^{-1}b\in K$. 要证明反过来也成立，只需把论证倒过来. 若 $a^{-1}b\in K$，则 $1=\varphi(a^{-1}b)=\varphi(a)^{-1}\varphi(b)$，所以 $\varphi(a)=\varphi(b)$. 这就证明了前两个结论是等价的，从而得证它们与其余的等价. ■

49

【2.5.9】推论 同态 $\varphi:G\to G'$ 是内射的当且仅当它的核 K 是 G 的平凡子群$\{1\}$.

证明 若 $K=\{1\}$，则命题 2.5.8 表明 $\varphi(a)=\varphi(b)$仅当 $a^{-1}b=1$，亦即 $a=b$ 时成立. 反之，若 φ 是内射，则恒等元是 G 中满足 $\varphi(a)=1$ 的唯一元素，故 $K=\{1\}$. ■

同态的核的另一个重要性质在下一个命题中阐述. 如果 a 和 g 是群 G 中的元素，则 gag^{-1}称作由 g 引出的 a 的共轭.

【2.5.10】定义 群 G 的子群 N 是正规子群，如果对于 N 中任意元素 a 和 G 中任意元素 g，共轭 $gag^{-1}\in N$.

【2.5.11】命题 一个同态的核是一个正规子群.

证明 如果 a 是同态 $\varphi:G\to G'$ 的核且 g 是群 G 的任意元素，则 $\varphi(gag^{-1})=\varphi(g)\varphi(a)\varphi(g^{-1})=\varphi(g)1\varphi(g)^{-1}=1$. 因此 gag^{-1} 也属于核. ■

因此，特殊线性群 $SL_n(\mathbf{R})$是一般线性群 $GL_n(\mathbf{R})$的正规子群，交错群 A_n 是对称群 S_n 的正规子群. 交换群的任何子群都是正规的，因为如果 G 是交换群，则 $gag^{-1}=a$ 对于所有的 a 和 g 成立. 但是非交换群的子群未必是正规的. 例如，在对称群 S_3 中，利用(2.2.7)中的表示，2 阶循环子群$\langle y\rangle$不是正规子群，因为 $y\in G$，但是 $xyx^{-1}=x^2y\notin\langle y\rangle$.

注 群 G 的中心(用 Z 表示)是与 G 中每个元素都可以交换的元素的集合：

【2.5.12】
$$Z=\{z\in G\mid zx=xz,\text{对于任意 } x\in G\}$$

Z 是 G 的正规子群. 特殊线性群 $SL_2(\mathbf{R})$的中心由两个矩阵 I，$-I$ 组成. 如果 $n\geqslant 3$，则对称群 S_n 的中心是平凡子群.

【2.5.13】例 对称群间的同态 $\varphi:S_4\to S_3$.

存在三种方式把指标集为$\{\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{4}\}$的集合划分为阶为 2 的子集对，即

【2.5.14】
$$\Pi_1:\{\mathbf{1},\mathbf{2}\}\cup\{\mathbf{3},\mathbf{4}\},\quad \Pi_2:\{\mathbf{1},\mathbf{3}\}\cup\{\mathbf{2},\mathbf{4}\},\quad \Pi_3:\{\mathbf{1},\mathbf{4}\}\cup\{\mathbf{2},\mathbf{3}\}$$

对称群 S_4 的一个元素置换这四个指标，在置换的过程中，也置换这三个划分. 这定义了从 S_4 到集合$\{\Pi_1,\Pi_2,\Pi_3\}$的置换群(即对称群 S_3)的一个映射 φ. 例如，4-循环 $p=(\mathbf{1}\ \mathbf{2}\ \mathbf{3}\ \mathbf{4})$ 在 2 阶子集上的作用如下：

$$\{\mathbf{1},\mathbf{2}\}\rightsquigarrow\{\mathbf{2},\mathbf{3}\}\quad \{\mathbf{1},\mathbf{3}\}\rightsquigarrow\{\mathbf{2},\mathbf{4}\}\quad \{\mathbf{1},\mathbf{4}\}\rightsquigarrow\{\mathbf{1},\mathbf{2}\}$$
$$\{\mathbf{2},\mathbf{3}\}\rightsquigarrow\{\mathbf{3},\mathbf{4}\}\quad \{\mathbf{2},\mathbf{4}\}\rightsquigarrow\{\mathbf{1},\mathbf{3}\}\quad \{\mathbf{3},\mathbf{4}\}\rightsquigarrow\{\mathbf{1},\mathbf{4}\}$$

从上述作用来看，$p=(\mathbf{1}\ \mathbf{2}\ \mathbf{3}\ \mathbf{4})$作用在划分集合$\{\Pi_1,\Pi_2,\Pi_3\}$是$(\Pi_1\Pi_3)$对换，使 Π_2 保持不

50

变而将 Π_1 和 Π_3 互换.

如果 p 和 q 是 S_4 中的元素，则乘积 pq 是置换的复合 $p\circ q$，且 pq 对集合$\{\Pi_1,\Pi_2,$

互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

$\Pi_3\}$的作用是 q 和 p 作用的合成. 因此 $\varphi(pq)=\varphi(p)\varphi(q)$，且 φ 是同态.

这个映射是满射，故其像是整个群 S_3. 它的核能够被计算出来. 它是 S_4 中由恒等元和三个互斥对换的乘积所组成的子群：

【2.5.15】 $$K=\{1,(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}$$ ■

第六节 同 构

一个从群 G 到群 G' 的同构 $\varphi:G\to G'$ 是双射群同态——一个双射，使得 $\varphi(ab)=\varphi(a)\varphi(b)$ 对于所有 a，$b\in G$ 成立.

【2.6.1】例

- 当看成是实数加群 $\mathbf{R}^+$ 到它的像，即正实数乘法群的映射时，指数映射 e^x 是一个同构.
- 若 a 是群 G 中的一个无限阶的元素，则将 $n\rightsquigarrow a^n$ 的映射是整数加群 $\mathbf{Z}^+$ 到群 G 的无限阶循环子群$\langle a\rangle$的同构.
- $n\times n$ 置换矩阵的集合 $\mathcal{P}$ 是 GL_n 的子群，且将置换映射为相应的矩阵(1.5.7)的映射 $S_n\to\mathcal{P}$ 是一个同构. ■

推论 2.5.9 给出了验证一个群同态 $\varphi:G\to G'$ 是同构的方法. 为此，只需验证 $\ker\varphi=\{1\}$，这蕴含了 φ 是单射，且 $\mathrm{im}\varphi=G'$ 蕴含了 φ 是满射.

【2.6.2】**引理** 如果 $\varphi:G\to G'$ 是同构，则其逆映射 $\varphi^{-1}:G'\to G$ 也是同构.

证明 一个双射的逆还是双射. 我们必须证明对于所有 G' 中的元素 x 和 y，有 $\varphi^{-1}(x)\varphi^{-1}(y)=\varphi^{-1}(xy)$. 令 $a=\varphi^{-1}(x)$，$b=\varphi^{-1}(y)$，且 $c=\varphi^{-1}(xy)$. 必须证明的是 $ab=c$. 因为 φ 是双射，故只需证明 $\varphi(ab)=\varphi(c)$就够了. 由于 φ 是同态，故

$$\varphi(ab)=\varphi(a)\varphi(b)=xy=\varphi(c)$$ ■

这个引理表明，当 $\varphi:G\to G'$ 是同构时，可以对这两个群的任何一个进行计算，然后用 φ 和 φ^{-1} 将一个群上的运算转化到另一个群上去. 所以，对群运算律，两个群上的性质是相同的. 为了直观地刻画这个结论，假设一个群的元素被放入没有标签的盒子里，且我们得到了神谕，当给我们两个盒子时，我们知道哪个盒子含有它们的乘积. 我们无法确定盒子里的元素来自 G 还是 G'.

两个群 G 和 G' 称为是同构的，如果存在从 G 到 G' 的同构 φ. 我们有时用符号“$\approx$”表示两个群同构：

【2.6.3】 $$G\approx G' \text{ 指的是 } G \text{ 同构于 } G'$$ 51

既然同构的群有相同的性质，因此当非正式地谈到同构的群时，把它们看成是相同的会很方便. 例如，我们经常忽略对称群 S_n 和与之同构的置换矩阵群 $\mathcal{P}$ 之间的差别.

注 与给定的群 G 同构的群形成 G 的同构类.

在同构类中的任何两个群是同构的. 当谈到给群分类时，就是指刻画这些同构类. 对所有群分类太难了，几乎是不可能做到的，但我们将看到每一个阶为素数 p 的群是循环

互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

群. 所以，所有阶为素数 p 的群都是同构的. 阶为 4 的群有两个同构类(2.11.5)，阶为 12 的群有 5 个同构类(7.8.1).

关于同构，一个有趣但容易引起混乱的一点就是存在群 G 到其自身的同构 $\varphi: G \to G$. 这样的同构称为 G 的自同构. 当然，恒等映射是自同构，但几乎总存在其他的自同构. 最重要类型的自同构是共轭：令 g 是群 G 中一个固定的元素. 由 g 得到的共轭是一个群 G 到自身的映射 φ，定义为：

【2.6.4】 $$\varphi(x) = gxg^{-1}$$

这是一个自同构，因为首先它是一个同态：

$$\varphi(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \varphi(x)\varphi(y)$$

其次，这是一个双射. 因为它有逆函数——由 g^{-1} 得到的共轭.

如果群是交换群，则由 g 得到的共轭是恒等映射：$gxg^{-1}=x$. 但任何非交换群有非平凡的共轭，所以就有异于恒等映射的自同构. 例如，在对称群 S_3 中，如以往的表示，由 y 得到的共轭交换 x 和 x^2.

如前所述，元素 gxg^{-1} 称为元素 x 关于 g 的共轭. G 中的两个元素 x，x' 是共轭的，如果 $x'=gxg^{-1}$ 对某个 $g\in G$ 成立. 共轭 gxg^{-1} 的行为与元素 a 自身的行为非常相似，例如它在群中的阶是一样的. 这可由它是元素 x 在一个自同构下的像这一事实得到(参见下面引理 2.6.5 的讨论).

注 有时人们希望确定群 G 中的两个元素 x 和 y 是否共轭，即是否存在一个元素 $g\in G$ 的使得 $y=gxg^{-1}$. 解上面的方程不如解 $yg=gx$ 简单.

注 交换子 $aba^{-1}b^{-1}$ 是与群中元素对 a，b 相关联的另一个元素.

下面的引理通过把一些项从方程的一边移到另一边得到.

【2.6.5】引理 群的两个元素 a，b 可交换，即 $ab=ba$，当且仅当 $aba^{-1}=b$，且结论成立当且仅当 $aba^{-1}b^{-1}=1$.

第七节 等价关系和划分

一个基本的数学构造是从一个集合 S 出发，根据给定的法则等同 S 的元素而得到新的
52 集合. 例如，可以将整数集合分为两类，即偶数和奇数. 所得到的新的集合由两个元素构成，一个元素叫做奇数，一个元素叫做偶数. 或者，可以将平面上的全等三角形视为等价的几何对象. 这个非常一般的过程来自不同的方面，我们现在就讨论这些方面.

注 集合 S 的一个划分 Π 是将 S 分为互不相交的非空的子集：

【2.7.1】 $$S = \text{不相交非空子集的并}$$

奇数集合和偶数集合这两个集合构成所有整数集合的一个划分. 采用通常的记号，集合

【2.7.2】 $$\{1\},\{y,xy,x^2y\},\{x,x^2\}$$

构成对称群 S_3 的一个划分.

注 集合 S 上的等价关系是 S 中某些元素对之间的关系. 我们通常将它们记为 $a\sim b$，

互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

并称为 a 与 b 的一个等价. 一个等价关系需要满足下面的条件:

【2.7.3】

- 传递的: 若 $a\sim b$ 且 $b\sim c$, 则 $a\sim c$.
- 对称的: 若 $a\sim b$, 则 $b\sim a$.
- 自反的: 对所有 a, $a\sim a$.

三角形的全等是平面上三角形的集合 S 上的等价关系的例子. 如果 A, B 和 C 是三角形, 且如果 A 全等于 B, 且 B 全等于 C, 则 A 全等于 C, 等等.

共轭性是群上的一个等价关系. 群中两个元素共轭, $a\sim b$, 如果存在 $g\in G$ 使得 $b=gag^{-1}$. 我们验证传递性: 设 $a\sim b$ 且 $b\sim c$. 这意味着 $b=g_1ag_1^{-1}$ 和 $c=g_2bg_2^{-1}$ 对某个 g_1, $g_2\in G$ 成立. 则 $c=g_2(g_1ag_1^{-1})g_2^{-1}=(g_2g_1)a(g_2g_1)^{-1}$, 故 $a\sim c$.

集合 S 的划分和 S 上的等价关系这两个概念在逻辑上是等价的, 虽然实际上给出的通常只是二者之一.

【2.7.4】**命题** 集合 S 上的一个等价关系确定集合 S 的一个划分, 反之亦然.

证明 给定 S 上的划分 P, 可用下面的规则定义一个等价关系 R: 如果 a 和 b 属于划分的同一个子集, 则 $a\sim b$. 等价关系的三条件显然成立. 反之, 给定等价关系 R, 可以这样定义划分 P: 含 a 的子集是所有满足条件 $a\sim b$ 的元素 b 的集合. 这个子集称为 a 的等价类. 我们用 C_a 表示 a 的等价类:

【2.7.5】
$$C_a=\{b\in S\,|\,a\sim b\}$$

下一个引理完成此命题的证明. ■ 53

【2.7.6】**引理** 给定集合 S 上的等价关系, S 的等价类构成 S 的划分.

证明 这点很重要, 所以我们将仔细验证. 记住记号 C_a 代表以特定方式定义的子集. 划分由这些子集构成, 且一些记号可以描述同一个子集.

自反公理告诉我们 $a\in C_a$. 所以, 类 C_a 是非空的, 并且由于 a 可以是任意元素, 故这些类覆盖 S, 剩下需要证明的划分的性质是等价类间没有重叠部分. 为证明这一点, 先证明:

【2.7.7】
$$\text{如果 } C_a \text{ 和 } C_b \text{ 有一个共同的元素, 则 } C_a=C_b$$

因为 a 和 b 的作用可以互换, 只需证明若 C_a 和 C_b 有一个共同的元素, 比如 d, 则 $C_b\subset C_a$, 即任何属于 C_b 中的元素均属于 C_a. 如果 $x\in C_b$, 则 $b\sim x$. 由于 $d\in C_a$ 和 $d\in C_b$, 故 $a\sim d$, $b\sim d$, 对称性告诉我们 $d\sim b$. 故有 $a\sim d$, $d\sim b$ 和 $b\sim x$. 两次应用传递性得 $a\sim x$, 因此, $x\in C_a$. ■

例如, 群上由 $a\sim b$ 定义的关系(如果 a 和 b 具有相同的阶)是一个等价关系. 对于对称群 S_3 的一个相应划分在(2.7.2)中给出.

如果给定了集合 S 的划分, 我们可以构造一个新的集合 $\overline{S}$, 其元素是等价类或组成划分的子集. 我们想象把这些子集放在不同的堆中, 把这些堆看成是新的集合 $\overline{S}$ 的元素. 建议用一个记号将子集和集合 $\overline{S}$(堆)中的元素区分开来. 如果 U 是一个子集, 则常用 $[U]$ 表示 $\overline{S}$ 中相应的元素. 因此, 如果 S 是整数集合且奇和偶分别表示奇数和偶数子集, 则 $\overline{S}$ 包含两个元素[奇]和[偶].

互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

我们将更广泛地应用这个记号. 当 S 的子集 U 作为 S 的子集的集合中的元素时，记作 $[U]$.

当给出集合 S 上一个等价关系，等价类形成一个划分，我们得到一个新的集合 $\overline{S}$，它的元素是等价类 $[C_a]$. 我们可以用另一种方式看待这个新的集合中的元素，因为这个集合是由元素间的等价关系变化得来的. 如果 a 和 b 属于 S，$a\sim b$ 意味着在 $\overline{S}$ 中 a 和 b 是相等的，因为 $C_a=C_b$. 用这种方式看待新集合的话，两个集合 S 和 $\overline{S}$ 的差别在于在 $\overline{S}$ 中更多的元素被宣布是“相等的”，即等价的. 对我来讲就像在学校里经常把全等三角形看成是一样的.

对于任何等价关系，存在一个自然的满射

【2.7.8】
$$\pi: S \to \overline{S}$$

把 S 中的元素 a 映射为它的等价类：$\pi(a)=[C_a]$. 当我们想把 $\overline{S}$ 看成是由集合 S 中的元素改变等价记号得到的时，$\overline{S}$ 中的元素 $[C_a]$ 用符号 $\overline{a}$ 表示更方便. 则映射 π 变成

54
$$\pi(a) = \overline{a}$$

我们可以在 $\overline{S}$ 中采用 S 中元素的符号，但在元素符号上面加上一横杠提醒我们在 $\overline{S}$ 中采用新规则：

【2.7.9】
$$\text{如果 } a \text{ 与 } b \text{ 属于 } S, \text{则 } \overline{a} = \overline{b} \text{ 意味着 } a \sim b$$

这一横杠符号的缺点是许多符号表示 $\overline{S}$ 中同一元素. 有时这个缺点可通过选取特殊元素(即每个等价类里的代表元)来克服. 例如，偶数与奇数常常用 $\overline{0}$ 与 $\overline{1}$ 表示：

【2.7.10】
$$\{[\text{偶}],[\text{奇}]\} = \{\overline{0},\overline{1}\}$$

虽然堆的图像较为直接，起初很容易掌握，但第二种看待 $\overline{S}$ 的方法更好，因为横杠记号在代数上更容易操作.

由映射定义的等价关系

集合之间的任意映射 $f: S\to T$ 在其定义域 S 上定义了一个等价关系，也就是由规则“如果 $f(a)=f(b)$ 则 $a\sim b$.”给出的等价关系.

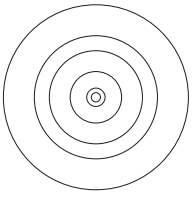
注 T 中元素 t 的原像是由满足 $f(s)=t$ 的所有元素 s 构成的 S 的子集. 用符号表示为

【2.7.11】
$$f^{-1}(t) = \{s \in S \mid f(s) = t\}$$

这是个象征性记号. 请记住只有当 f 是双射时 f^{-1} 才是映射. 原像也叫做映射 f 的纤维，且非空纤维是对于上面定义的等价关系的等价类.

作为映射的像，这里等价类集合 $\overline{S}$ 有另外的体现. 像的元素与非空纤维一一对应，而非空纤维是等价类.

【2.7.12】图



绝对值映射：$\mathbf{C}^\times \to \mathbf{R}^\times$ 的一些纤维

互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

【2.7.13】**例** 如果 G 是有限群，定义映射 $f:G\to\mathbf{N}$ 到自然数{1，2，3，…}的集合，令 $f(a)$表示 G 中元素 a 的阶．这个映射的纤维是同阶元素的集合(例如，见(2.7.2))． ■ 55

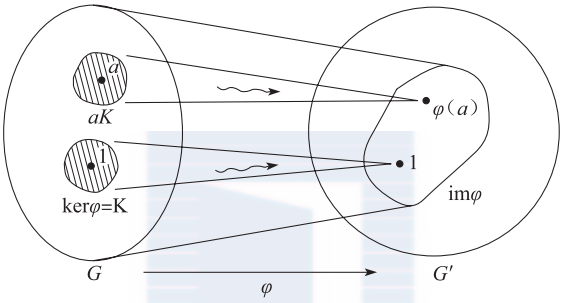
我们回到群同态 $\varphi:G\to G'$．由 φ 定义的群 G 上的等价关系通常用≡表示，而不用～，～指的是同余．

【2.7.14】 $$\text{如果 } \varphi(a)=\varphi(b),\quad \text{则 } a\equiv b$$

我们看到 G 中元素 a 与 b 是同余的，即 $\varphi(a)=\varphi(b)$，当且仅当 b 属于核 K 的陪集 aK(2.5.8)．

【2.7.15】**命题** 令 K 是同态 $\varphi:G\to G'$ 的核．φ 的包含 G 中元素 a 的纤维是核 K 的陪集 aK．这些陪集构成了群 G 的划分，且这个划分对应着 φ 的像的元素．

【2.7.16】图



群同态的图解

第八节 陪 集

如前，如果 H 是群 G 的子群，且 $a\in G$，则子集

【2.8.1】 $$aH=\{ah\mid h\in H\}$$

称为左陪集．子群 H 是一个特殊的左陪集，因为 $H=1H$．

G 中 H 的陪集是关于同余关系

【2.8.2】 $$a\equiv b,\text{如果 } b=ah \text{ 对某个 } h\in H \text{ 成立}$$

的等价类．这很简单，但是让我们验证同余是等价关系．

传递性：假设 $a\equiv b$ 且 $b\equiv c$．这表明对 h，$h'\in H$，有 $b=ah$ 和 $c=bh'$．因此，$c=ahh'$．由于 H 是子群，$hh'\in H$，这样 $a\equiv c$．

对称性：设 $a\equiv b$，则有 $b=ah$．于是 $a=bh^{-1}$ 且 $h^{-1}\in H$，故 $b\equiv a$．

自反性：$a=a1$ 而 $1\in H$，故 $a\equiv a$．

注意，我们用到子群定义的所有性质：封闭性，逆元，恒等元． 56

【2.8.3】**推论** *群 G 的子群 H 的左陪集是群 G 的划分．*

证明 左陪集是同余关系(2.8.2)的等价类． ■

记住符号 aH 定义 G 的某个子集．与任意等价关系一样，若干个记号可以表示同一集合．例如，在对称群 S_3 中，用通常的表示(2.2.6)，元素 y 生成一个阶为 2 的循环子群 $H=\langle y\rangle$．在 G 中有三个关于 H 的左陪集：

互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

【2.8.4】 $H=\{1,y\}=yH$， $xH=\{x,xy\}=xyH$， $x^2H=\{x^2,x^2y\}=x^2yH$
这些集合的确是群的划分.

概括地讲，令 H 是群 G 的子群，a，$b\in G$. 下列结论是等价的：

【2.8.5】

- $b=ah$ 对于某个 $h\in H$，或 $a^{-1}b$ 是 H 的元素成立，
- b 是左陪集 aH 的元素，
- 左陪集 aH 与 bH 是相等的.

一个子群的左陪集的个数叫做这个子群 H 在群 G 中的指标. 指标表示为：

【2.8.6】 $$[G:H]$$

因此子群$\langle y\rangle$在 S_3 中的指标为 3. 当 G 是无限群时，指标也是无限的.

【2.8.7】**引理** *群 G 的子群 H 的所有左陪集 aH 有相同的阶.*

证明 存在一个由子群 H 到陪集 aH 的映射：$h\to aH$ 将 h 映射为 ah，即 $h\rightsquigarrow ah$. 这个映射是双射，因为它的逆是由 a^{-1} 所诱导的乘法映射. ■

因为所有陪集有相同的阶，而这些陪集是群的一个划分，所以我们得到重要的计数公式：

【2.8.8】 $$|G|=|H|[G:H]$$

$$(G\text{ 的阶数})=(H\text{ 的阶数})(\text{陪集个数})$$

其中，如通常一样，$|G|$表示 G 的阶. 如果某项为无穷，等式的意义是显然的. 对于 S_3 的子群$\langle y\rangle$，这个公式成为 $6=2\cdot 3$.

从计数公式得到(2.8.8)右边两项一定整除左边. 下面是这些结果中的一个，称为拉格朗日定理：

【2.8.9】**定理**(拉格朗日定理) *设 G 是有限群且 H 是 G 的子群. H 的阶整除 G 的阶.*

57 【2.8.10】**推论** *有限群的元素的阶数整除群的阶数.*

证明 一个群 G 的元素 a 的阶等于由 a 生成的循环子群$\langle a\rangle$的阶(命题 2.4.2). ■

【2.8.11】**推论** *设群 G 的阶为 p 且 p 是素数. 设 $a\in G$ 是任意元，但不是恒等元. 则 G 是由 a 生成的循环群$\langle a\rangle$.*

证明 元素 $a\neq 1$ 的阶大于 1 且它整除 $|G|=p$. 所以，a 的阶等于 p. 这也是由 a 生成的循环子群$\langle a\rangle$的阶. 因为 G 的阶为 p，所以$\langle a\rangle=G$. ■

这一推论对所有素数阶 p 的群作了分类. 它们构成一个同构类，即 p 阶循环群类.

当给定同态 $\varphi:G\to G'$时，计数公式也可以应用. 正如我们在(2.7.15)中所看到的，$\ker\varphi$ 的左陪集是映射 φ 的纤维，它们与像中的元素一一对应.

【2.8.12】 $$[G:\ker\varphi]=|\mathrm{im}\varphi|$$

【2.8.13】**推论** *设 $\varphi:G\to G'$：是有限群的一个同态. 则*

- $|G|=|\ker\varphi|\cdot|\mathrm{im}\varphi|$，
- $|\ker\varphi|$ 整除 $|G|$，
- $|\mathrm{im}\varphi|$ 整除 $|G|$ 和 $|G'|$.

互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

证明 第一个公式由(2.8.8)和(2.8.12)合起来得到，而且它蕴含着$|\ker\varphi|$和$|\mathrm{im}\varphi|$整除$|G|$. 因为$\mathrm{im}\varphi$是G'的子群，由拉格朗日定理可知，$|\mathrm{im}\varphi|$也整除$|G'|$. ■

例如，符号同态$\sigma:S_n\to\{\pm1\}$(2.5.2)(b)是满射，所以它的像的阶为2. 它的核即交错群A_n)有阶$\frac{1}{2}n!$. S_n的一半元素是偶置换，一半元素是奇置换.

当给出一串子群时，计数公式2.8.8有类似的结论.

【2.8.14】命题(指标的乘法性质) 令$G\supset H\supset K$是群G的子群，则$[G:K]=[G:H][H:K]$.

证明 我们假设右边两个指标都是有限的，比如，令$[G:H]=m$和$[H:K]=n$. 当其中一个指标无限时，推理是类似的. 我们列出H在G中的m个陪集，每个陪集选出代表元，比如g_1H，…，g_mH. 则$g_1H\cup\cdots\cup g_mH$是G的一个划分. 同样选出K在H中的所有陪集的代表元，得到H的一个划分$H=h_1H\cup\cdots\cup h_nK$. 由于用$g_i$乘的运算是可逆的，因此$g_iH=g_ih_1K\cup\cdots\cup g_ih_nK$是陪集$g_iH$的一个划分. 将这些划分组合起来，就构成了由$mn$个陪集$g_ih_jK$组成的$G$的一个划分. ■

右陪集

让我们回到陪集的定义. 这里使用的是左陪集aH，也可以定义子群H的右陪集并且 58
重复上面的讨论. 群G的子群H的右陪集是集合

【2.8.15】
$$Ha=\{ha\,|\,h\in H\}$$

它们是关系(右同余)

$$a\equiv b,\text{如果存在 } h\in H,\text{使 } b=ha$$

的等价类. 右陪集和左陪集不一定相同，但它们也构成群的一个划分. 例如，S_3的子群$\langle y\rangle$的右陪集是

【2.8.16】
$$H=\{1,y\}=Hy,\quad Hx=\{x,x^2y\}=Hx^2y,\quad Hx^2=\{x^2,xy\}=Hxy$$

这和划分(2.8.4)中的左陪集不同. 然而，如果一个子群是正规子群，那么它的左陪集和右陪集就是相同的.

【2.8.17】命题 令H是群G的子群. 下列条件是等价的：

(i) H是正规子群：对于所有$h\in H$和$g\in G$有$ghg^{-1}\in H$.

(ii) 对于所有$g\in G$，$gHg^{-1}=H$.

(iii) 对于所有$g\in G$，左陪集gH等于右陪集Hg.

(iv) H在G中的每一个左陪集都是右陪集.

证明 记号gHg^{-1}代表所有元素ghg^{-1}所成的集合，其中$h\in H$.

假设H是正规子群. 故(i)成立，且蕴含$gHg^{-1}\subset H$对于所有$g\in G$成立. 用g^{-1}代替g也可证$g^{-1}Hg\subset H$. 在这个包含关系两边左乘g且右乘g^{-1}可得$H\subset gHg^{-1}$. 因此，$gHg^{-1}=H$. 这就证明了(i)蕴含(ii). 显然，(ii)蕴含(i). 其次，若$gHg^{-1}=H$，两边右乘g，得$gH=Hg$. 这证明了(ii)蕴含(iii). 类似可证明(iii)蕴含(ii). 由于(iii)蕴含(iv)是

互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

显然的，因此只需验证(iv)蕴含(iii).

那么在什么情况下左陪集和右陪集相等？我们回忆一下右陪集全体是群 G 的一个划分，且注意到左陪集 gH 与右陪集 Hg 有一个共同的元素，即 $g=g\cdot 1=1\cdot g$. 所以，如果左陪集 gH 等于某个右陪集，那么这个右陪集一定是 Hg. ■

【2.8.18】命题

(a) 如果 H 是群 G 的子群且 g 是 G 中一个元素，则集合 gHg^{-1} 也是一个子群.

(b) 如果群 G 只有一个 r 阶子群 H，则这个子群是正规的.

证明 (a) 由 g 导出的共轭是群 G 的一个自同态(参见(2.6.4))，且 gHg^{-1} 是 H 的同态像. (b)参见(2.8.17)：gHg^{-1} 是阶为 r 的子群. ■

注意 如果 H 是有限群 G 的子群，则用右陪集和左陪集的计数公式是一样的，所以左陪集的个数与右陪集的个数相等. 这对于 G 是无限群的情形也是成立的，虽然不能通过计数来证明(参见练习 M.8).

59

第九节 模 算 术

这一节包含对数论里一个重要概念——整数的同余——的一个简短的讨论. 如果你以前没有遇到过这个概念，则需要了解关于同余的更多知识. 例如，参看[Stark]. 整个这一节都对一个固定的正整数 n 进行讨论.

注 两个整数 a 和 b 说是模 n 同余的，即

【2.9.1】
$$a\equiv b(\bmod n)$$

如果 n 整除 $b-a$，或如果对于某个整数 k，有 $b=a+nk$. 例如，$2\equiv 17(\bmod 5)$.

容易验证同余是等价关系，所以可以考虑等价类，称为同余类. 我们用画横杠的符号 $\bar{a}$ 来表示整数 a 模 n 的同余类. 这个同余类是整数集合：

【2.9.2】
$$\bar{a}=\{\cdots,a-n,a,a+n,a+2n,\cdots\}$$

如果 a 和 b 是整数，方程 $\bar{a}=\bar{b}$ 意味着 $a\equiv b(\bmod n)$，或 n 整除 $b-a$. 同余类 $\bar{0}$：

$$\bar{0}=\mathbf{Z}n=\{\cdots,-n,0,n,2n,\cdots\}=\{kn\,|\,k\in\mathbf{Z}\}$$

是整数加群 $\mathbf{Z}^+$ 的一个子群. 其他同余类是这个子群的陪集. 请注意 $\mathbf{Z}n$ 不是右陪集——它是 $\mathbf{Z}^+$ 的一个子群. 和子群 H 的陪集记号 aH 类似，但用加法记号表示合成法则，$a+H=\{a+h\,|\,h\in H\}$. 为简化符号，将子群 $\mathbf{Z}n$ 记为 H. 则 H 的陪集(同余类)是集合

【2.9.3】
$$a+H=\{a+kn\,|\,k\in\mathbf{Z}\}$$

n 个整数 0，1，…，$n-1$ 是这 n 个同余类的代表元.

【2.9.4】命题 有 n 个模 n 的同余类，即 $\bar{0}$，$\bar{1}$，…，$\overline{n-1}$. $\mathbf{Z}n$ 在 $\mathbf{Z}$ 中的指标 $[\mathbf{Z}:\mathbf{Z}n]$ 是 n.

令 $\bar{a}$ 和 $\bar{b}$ 表示整数 a，b 的同余类. 它们的和定义为 $a+b$ 的同余类，它们的积是 ab 的同余类. 换句话说，由定义，

【2.9.5】
$$\bar{a}+\bar{b}=\overline{a+b}\quad,\quad \bar{a}\bar{b}=\overline{ab}$$

这个定义需要证明其合理性，因为同一个同余类可以用多个不同的整数表示. 任何与 a 模

互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

n 同余的整数 a' 代表同一个类. 故最好是当 $a'\equiv a$，$b'\equiv b$ 时，$a'+b'\equiv a+b$ 和 $a'b'\equiv ab$ 都成立. 幸运的是，情况的确如此.

【2.9.6】引理 如果 $a'\equiv a(\mathrm{mod}\ n)$，$b'\equiv b(\mathrm{mod}\ n)$，则 $a'+b'\equiv a+b(\mathrm{mod}\ n)$，$a'b'\equiv ab(\mathrm{mod}\ n)$.

60

证明 假设 $a'\equiv a(\mathrm{mod}\ n)$，$b'\equiv b(\mathrm{mod}\ n)$，所以 $a'=a+rn$，且 $b'=b+sn$，其中 r，s 为整数. 这样，$a'+b'=a+b+(r+s)n$. 这表明 $a'+b'\equiv(a+b)(\mathrm{mod}\ n)$. 同理，$a'b'=(a+rn)(b+sn)=ab+(as+rb+rns)n$，故 $a'b'\equiv ab(\mathrm{mod}\ n)$. ■

同余类对于加法和乘法的结合律、交换律和分配律成立因为这些运算律对于整数的加法和乘法成立. 例如，分配律证明如下：

$$\begin{aligned}\bar{a}(\bar{b}+\bar{c}) &= \bar{a}\overline{(b+c)} = \overline{a(b+c)} && \text{（同余类加法和乘法的定义）}\\ &= \overline{ab+ac} && \text{（整数的分配律）}\\ &= \overline{ab}+\overline{ac} = \bar{a}\bar{b}+\bar{a}\bar{c} && \text{（同余类加法和乘法的定义）}\end{aligned}$$

其他运算律的证明是类似的，在此省略.

模 n 同余类的集合通常记作 $\mathbf{Z}/\mathbf{Z}n$，$\mathbf{Z}/n\mathbf{Z}$ 或 $\mathbf{Z}/(n)$. 加、减和乘可以通过取用 n 去除整数所得的余数而直接得到. 这就是公式(2.9.5)的含义. 这里两个公式表明，将整数 a 变到其同余类 $\bar{a}$ 的映射

【2.9.7】
$$\mathbf{Z}\to\mathbf{Z}/\mathbf{Z}n$$

与加法和乘法相容. 因而计算可在整数中进行，而在最后搬回到 $\mathbf{Z}/\mathbf{Z}n$ 上. 然而，如果使用较小的数字，则运算比较简单. 可通过在做了部分运算后取余数，从而保持运算中的数字都很小.

于是，如果 $n=29$，从而 $\mathbf{Z}/\mathbf{Z}n=\{\bar{0},\bar{1},\cdots,\overline{28}\}$，则 $(\overline{35})(\overline{17}+\bar{7})$ 可以按 $(\overline{35})\cdot(\overline{24})=\bar{6}\cdot(-\bar{5})=-\overline{30}=-\bar{1}$ 的顺序计算.

从长远考虑，数字上面加横杠是很烦人的，因而常被省去，但要记住下面的规则：

【2.9.8】 在 $\mathbf{Z}/\mathbf{Z}n$ 中说 $a=b$ 是指 $a\equiv b(\mathrm{mod}\ n)$

模一个素数的同余有特殊的性质，将在下一章的开头讨论.

第十节 对 应 定 理

令 $\varphi:G\to\mathcal{G}'$ 是群同态，而 H 是 G 的子群. 则可以限制 φ 到 H 得到一个同态

【2.10.1】
$$\varphi|_H:H\to\mathcal{G}$$

这是指取相同的映射 φ 但将其定义域限制到 H. 故由定义，对所有 $h\in H$ 有 $[\varphi|_H](h)=\varphi(h)$. (为清楚起见，我们给符号 $\varphi|_H$ 加了括号)因为 φ 是同态，所以它的限制也是同态，且 $\varphi|_H$ 的核是 $\ker\varphi$ 与 H 的交：

【2.10.2】
$$\ker(\varphi|H)=(\ker\varphi)\cap H$$

61

由核的定义这是明显的. $\varphi|_H$ 的像与 H 在映射 φ 下的像 $\varphi(H)$ 是一样的.

计数公式也可以帮助描述这个限制. 根据推论(2.8.13)，像的阶既整除 $|H|$，也整除

互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

$|\mathcal{G}|$. 如果$|H|$|和$|\mathcal{G}|$没有公因子，则 $\varphi(H)=\{1\}$，因而可得 $H\subset\ker\varphi$.

【2.10.3】例 符号同态 $\sigma:S_n\to\{\pm1\}$的像的阶为 2. 如果对称群 S_n 的子群 H 为奇数阶，则它包含在 σ 的核——由偶置换构成的交错群 A_n 中. 当 H 是由一个在群中阶为奇数的置换 q 生成的循环子群时，也是这样的. 每一个奇数阶的置换(例如奇数阶循环群)为偶置换. 另一方面，我们不能对偶数阶的置换得出任何结论. 它们可以是奇的，也可以是偶的. ■

【2.10.4】命题 令 $\varphi:G\to\mathcal{G}$是一个群同态且其核为 K，令$\mathcal{H}$是$\mathcal{G}$的子群. 记逆像 $\varphi^{-1}(\mathcal{H})$为 H. 则 H 是 G 的子群且 $H\supset K$. 如果$\mathcal{H}$是$\mathcal{G}$的正规子群，则 H 是 G 的正规子群. 如果 φ 是满射，且 H 是 G 的正规子群，则$\mathcal{H}$是$\mathcal{G}$的正规子群.

例如，令 φ 表示行列式同态 $GL_n(\mathbf{R})\to\mathbf{R}^\times$. 正实数集合是 $\mathbf{R}^\times$ 的子群. 它是正规子群因为 $\mathbf{R}^\times$ 是交换的. 它的逆像——具有正的行列式值的可逆矩阵的集合——是 $GL_n(\mathbf{R})$的正规子群.

证明 证明是简单的，但必须记住，φ^{-1} 不是映射. 由定义，$\varphi^{-1}(\mathcal{H})=\{x\in G|\varphi(x)\in\mathcal{H}\}$. 首先，如果 $x\in K$，则 $\varphi(x)=1\in\mathcal{H}$，故 $x\in H$. 因此 $H\supset K$. 下面验证子群的条件.

封闭性：设 x，$y\in H$. 则 $\varphi(x)$，$\varphi(y)\in\mathcal{H}$. 由于$\mathcal{H}$是子群，故 $\varphi(x)\varphi(y)\in\mathcal{H}$. 由于 φ 是同态，故 $\varphi(x)\varphi(y)=\varphi(xy)$. 因而 $\varphi(xy)\in\mathcal{H}$，且 $xy\in H$.

有恒等元：$1\in H$ 因为 $\varphi(1)=1\in\mathcal{H}$.

逆元：令 $x\in H$，则 $\varphi(x)\in\mathcal{H}$. 由于$\mathcal{H}$是子群，故 $\varphi(x)^{-1}\in\mathcal{H}$. 由于 φ 是同态，故 $\varphi(x)^{-1}=\varphi(x^{-1})\in\mathcal{H}$，且 $x^{-1}\in H$.

假设$\mathcal{H}$是正规子群. 令 $x\in H$，$g\in G$. 则 $\varphi(gxg^{-1})=\varphi(g)\varphi(x)\varphi(g)^{-1}$是 $\varphi(x)$的共轭，而 $\varphi(x)\in\mathcal{H}$. 因为$\mathcal{H}$是正规子群，故 $\varphi(gxg^{-1})\in\mathcal{H}$，因此 $gxg^{-1}\in H$.

假设 φ 是满射，且 H 是 G 的正规子群. 令 $a\in\mathcal{H}$且 $b\in\mathcal{G}$. 存在元素 $x\in H$，$y\in G$ 使得 $\varphi(x)=a$，$\varphi(y)=b$. 由于 H 是正规子群，$yxy^{-1}\in H$，因此 $\varphi(yxy^{-1})=bab^{-1}\in\mathcal{H}$. ■

【2.10.5】定理(对应定理) 令 $\varphi:G\to\mathcal{G}$是一个群满同态且其核为 K. 存在$\mathcal{G}$的子群到 G 的包含 K 的子群之间的双射：

62

$$\{G\text{ 的含有 }K\text{ 的子群}\}\leftrightarrow\{\mathcal{G}\text{的子群}\}$$

这个对应定义如下：

$$G\text{ 的含有 }K\text{ 的子群 }H\rightsquigarrow\text{像 }\varphi(H)\text{是}\mathcal{G}\text{的子群}$$

$$\mathcal{G}\text{的一个子群}\mathcal{H}\rightsquigarrow\text{其逆像 }\varphi^{-1}(\mathcal{H})\text{是 }G\text{ 的子群}$$

如果 H 和$\mathcal{H}$是对应的子群，则 H 是 G 的正规子群当且仅当$\mathcal{H}$是$\mathcal{G}$的正规子群.

如果 H 和$\mathcal{H}$是对应的子群，则 $|H|=|\mathcal{H}||K|$.

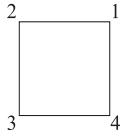
【2.10.6】例 回到在例 2.5.13 中定义的同态 $\varphi:S_4\to S_3$ 和它的核 K(2.5.15).

群 S_3 有 6 个子群，其中 4 个真子群. 用通常的表示，有一个 3 阶真子群，即循环群 $\langle x\rangle$，有 3 个 2 阶子群，包括$\langle y\rangle$. 对应定理告诉我们存在 4 个 S_4 的包含 K 的真子群. 由于 $|K|=4$，因此有一个 12 阶子群和 3 个 8 阶子群.

我们知道有一个 12 阶子群，即交错群 A_4. 这是对应于 S_3 的循环群$\langle x\rangle$的子群.

互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

8 阶子群可利用正方形的对称性来解释. 正方形四个顶点的标号如下图所示，通过$\frac{\pi}{2}$角度逆时针旋转对应 4-循环(**1 2 3 4**). 关于通过顶点 1 的对角线反射得到对换(**2 4**). 这两个置换生成一个 8 阶子群. 其他的 8 阶子群可以通过给正方形的顶点以另外的方式标号得到.



S_4 中也有不含 K 的一些子群. 对应定理对此没有给出讨论. ■

对应定理的证明 令 H 是 G 的含 K 的子群，$\mathcal{H}$是$\mathcal{G}$的子群. 我们必须验证下面几点：

- $\varphi(H)$是 G'的子群.
- $\varphi^{-1}(\mathcal{H})$是 G 的含 K 的子群.
- $\mathcal{H}$是$\mathcal{G}$的正规子群当且仅当 $\varphi^{-1}(\mathcal{H})$是 G 的正规子群.
- (对应的双射性)$\varphi(\varphi^{-1}(\mathcal{H}))=\mathcal{H}$且 $\varphi^{-1}(\varphi(H))=H$.
- $|\varphi^{-1}(\mathcal{H})|=|\mathcal{H}||K|$.

由于 $\varphi(H)$是同态 $\varphi|_H$ 的像，故它是$\mathcal{G}$的子群. 第二、第三条来自命题 2.10.4.

关于第四条，等式 $\varphi(\varphi^{-1}(\mathcal{H}))=\mathcal{H}$对应任意集合上的满射 $\varphi:S\to S'$和任意子集$\mathcal{H}\subset S'$成立. 而且 $H\subset\varphi^{-1}(\varphi(H))$对于任何映射和任何子集 $H\subset S$ 成立. 我们省略这些事实的验 63
证，只验证 $H\supset\varphi^{-1}(\varphi(H))$. 令 $x\in\varphi^{-1}(\varphi(H))$. 我们必须证明 $x\in H$. 由逆像的定义，$\varphi(x)\in\varphi(H)$，比如 $\varphi(x)=\varphi(a)$，$a\in H$. 则 $a^{-1}x\in K$(2.5.8)，且由于 $H\supset K$，故 $a^{-1}x\in H$. 由于 $a\in H$，$a^{-1}x\in H$，故 $x\in H$.

我们把最后一条的证明留作练习. ■

第十一节 积 群

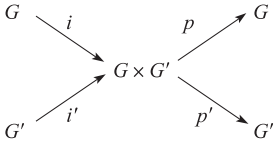
设 G，G'为两个群. 积集 $G\times G'=\{(a,a')\mid a\in G,a'\in G'\}$可按分量乘积构成一个群，即按如下规则

【2.11.1】
$$(a,a')\cdot(b,b')=(ab,a'b')$$

定义元素对的乘积. 元素对(1，1)是恒等元，而(a,a')的逆元是(a^{-1},a'^{-1}). $G\times G'$上的结合律由 G 和G'上的结合律得到.

这样得到的群称为 G 和G'的积，记为 $G\times G'$. 积群以简单的方式与其因子群 G 和G'相联系，我们可用由 $i(x)=(x,1)$，$i'(x')=(1,x')$，$p(x,x')=x$，$p'(x,x')=x'$定义的同态的语言加以总结：

【2.11.2】图



互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

单同态 i，i'可用来将 G 和 G'等同于它们的像，$G\times G'$的子群 $G\times 1$，$1\times G'$. 映射 p，p'是满射，p 的核是 $1\times G'$，而 p'的核是 $G\times 1$. 这两个映射是投影.

显然，大家都期望把一个给定的群 G 分解成积，也就是说找到两个群 H 和 H'，使 G 同构于它们的积 $H\times H'$. 群 H 和 H'较简单，而且 $H\times H'$与其因子的关系也容易理解. 可是，给定的群是积的情形非常稀少，但的确偶有发生.

例如，令人惊叹的是 6 阶循环群可以被分解：一个 6 阶循环群 C_6 同构于 2 阶和 3 阶的循环群的积 $C_2\times C_3$. 要说明这点，令 $C_2=\langle y\rangle$，$C_3=\langle z\rangle$，且 $y^2=1$，$z^3=1$，令 x 表示积群$C_2\times C_3$中的元素(y, z). 使得 $x^k=(y^k, z^k)$成为恒等元$(1, 1)$的最小正整数是 $k=6$. 故 x 的阶是 6. 由于 $C_2\times C_3$ 的阶也是 6，故 $C_2\times C_3=\langle x\rangle$. x 的方幂按照顺序为：

$$(1,1),(y,z),(1,z^2),(y,1)(1,z),(y,z^2)$$

只要两个整数 r 和 s 没有公因子，同样的论证就可用于 rs 阶循环群.

64 **【2.11.3】命题** 令整数 r 和 s 互素. rs 阶循环群同构于 r 阶循环群和 s 阶循环群的积.

另一方面，4 阶循环群不同构于两个 2 阶循环群的积. $C_2\times C_2$ 中每个元素的阶或为 1 或为 2，而 4 阶循环群中有两个元素阶为 4.

下面的命题刻画了群的积.

【2.11.4】命题 令 H 和 K 是群 G 的子群，令 $f:H\times K\to G$ 是乘法映射，定义为 $f(h, k)=hk$. 它的像是集合 $HK=\{hk\mid h\in H, k\in K\}$.

(a) f 是单射的当且仅当 $H\cap K=\{1\}$.

(b) f 是积群 $H\times K$ 到群 G 的同态当且仅当 K 的元素与 H 的元素可交换：$hk=kh$.

(c) 如果 H 是 G 的正规子群，则 HK 是 G 的子群.

(d) f 是积群 $H\times K$ 到群 G 的同构当且仅当 $H\cap K=\{1\}$，$HK=G$，且 H 和 K 都是 G 的正规子群.

注意到乘法映射可以是双射尽管它可能不是群同态这点是重要的. 这种情况会发生，例如，当 $G=S_3$ 时，用通常的记号，$H=\langle x\rangle$，$K=\langle y\rangle$.

证明

(a) 如果 $H\cap K$ 包含一个元素 $x\neq 1$，则 $x^{-1}\in H$，且 $f(x^{-1}, x)=1=f(1, 1)$，所以 f 不是单射. 假设 $H\cap K=\{1\}$. 令(h_1, k_1)和(h_2, k_2)是 $H\times K$ 中的元素使得 $h_1k_1=h_2k_2$. 在方程两边左乘 h_1^{-1}且右乘 k_2^{-1}，得到 $k_1k_2^{-1}=h_1^{-1}h_2$. 左边是 K 中元素，右边是 H 中元素. 由于 $H\cap K=\{1\}$，故 $k_1k_2^{-1}=h_1^{-1}h_2=1$，于是，$k_1=k_2$，$h_1=h_2$，且$(h_1, k_1)=(h_2, k_2)$.

(b) 令(h_1, k_1)和(h_2, k_2)是积群 $H\times K$ 中的元素. 这些元素在 $H\times K$ 中的积为(h_1h_2, k_1k_2)，且 $f(h_1h_2, k_1k_2)=h_1h_2k_1k_2$，而 $f(h_1, k_1)f(h_2, k_2)=h_1k_1h_2k_2$. 这些元素是相等的当且仅当 $h_2k_1=k_1h_2$.

(c) 假设 H 是正规子群. 我们注意 KH 是左陪集 kH 的并，其中 $k\in K$，而 HK 是所有右陪集 Hk 的并，其中 $k\in K$. 由于 H 是正规子群，$kH=Hk$，所以 $HK=KH$. HK 对

互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

于乘法的封闭性得证，因为 $HKHK=HHKK=HK$. 还有，$(hk)^{-1}=k^{-1}h^{-1}$ 属于 $KH=HK$. 这证明了 HK 的逆元是封闭的.

(d) 假设 H 和 K 满足所给条件. 则 f 既是单射又是满射，所以是双射. 由(b)，f 是同构当且仅当对所有 $h\in H$，$k\in K$，有 $hk=kh$. 考虑交换子 $(hkh^{-1})k^{-1}=h(kh^{-1}k^{-1})$. 由于 K 是正规子群，故左边属于 K，又由于 H 是正规子群，故右边属于 H. 因为 $H\cap K=\{1\}$，故 $hkh^{-1}k^{-1}=1$，$hk=kh$. 反过来，如果 f 是同构，可以验证同构群 $H\times K$ 而不是 G 中列出的这些条件. ■

我们用这个命题对阶为 4 的群进行分类.

【2.11.5】命题 *存在两个 4 阶群的同构类. 一类是 4 阶循环群 C_4，一类是克莱因四元群，它同构于阶为 2 的两个群的积 $C_2\times C_2$.* 65

证明 令 G 是 4 阶群，故 G 的每个元素的阶都整除 4. 于是，考虑两种情形：

情形 1：G 有一个元素的阶为 4. 则 G 是 4 阶循环群.

情形 2：G 中每个除了单位元以外的元素的阶均为 2.

在此情形，对 G 中任意元素 x 有 $x=x^{-1}$. 令 x 和 y 是 G 中两个元素. 则 xy 的阶为 2，故 $xyx^{-1}y^{-1}=(xy)(xy)=1$. 这证明了 x 和 y 可交换(2.6.5)，且既然是群中任意元素，因此 G 是交换群. 故任意子群都是正规子群. 选取 G 中不同元素 x 和 y，令 H 和 K 是由 x 和 y 生成的 2 阶循环子群. 命题 2.11.4(d)表明 G 同构于积群 $H\times K$. ■

第十二节 商 群

在这一节我们将在群 G 的正规子群 N 的陪集的集合上定义合成法则. 这个运算法则使得正规子群的陪集成为一个群，称为商群.

整数模 n 的同余类的加法就是商结构的一个例子. 另一个熟悉的例子是角度的加法. 每个实数代表一个角，任意两个实数代表同一个角当且仅当它们相差 2π 的整数倍. 所有 2π 的整数倍的实数构成实数加群 $\mathbf{R}^+$ 的一个子群 N，角对应着 N 在 G 中的陪集 $\theta+N$. 角的群是元素是陪集的商群.

正规子群 N 在 G 中的陪集的集合通常用 G/N 表示.

【2.12.1】 G/N 是正规子群 N 在 G 中的陪集的集合

当把陪集 C 看成陪集集合中的元素时，用括号 $[C]$ 表示. 如果 $C=aN$，也可用加横杠的方式 $\bar{a}$ 表示元素 $[C]$，而陪集的集合记作 $\overline{G}$：

$$\overline{G}=G/N$$

【2.12.2】定理 *令 N 是 G 的正规子群，令 $\overline{G}$ 表示 N 在 G 中的陪集的集合. 存在 $\overline{G}$ 上的一个合成法则使其成为一个群，使得定义为 $\pi(a)=\bar{a}$ 的映射 $\pi:G\to\overline{G}$ 是一个核为 N 的满同态.*

注 映射 π 经常称为 G 到 $\overline{G}$ 的典范映射. “典范”是指这是仅有的一个有理由讨论的映射.

下一个推论非常简单，但很重要，值得单独列出来.

【2.12.3】推论 *令 N 是群 G 的正规子群，令 $\overline{G}$ 表示 N 在 G 中的陪集的集合. 令 $\pi:G\to\overline{G}$ 是*

互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

典范同态. 令 a_1，…，a_k 是 G 中的元素使得积 $a_1\cdots a_k\in N$. 则 $\overline{a_1}\cdots\overline{a_k}=\overline{1}$.

66 **证明** 令 $p=a_1\cdots a_k$. 则 $p\in N$，故 $\pi(p)=\overline{p}=\overline{1}$. 由于 π 是同态，故 $\overline{a_1}\cdots\overline{a_k}=\overline{p}$. ■

定理 2.12.2 的证明 有下面几件事必须要做.

- 在 $\overline{G}$ 上定义合成法则.
- 证明 $\overline{G}$ 在此合成法则下成为一个群.
- 证明典范映射 π 是满同态.
- 证明 π 的核是 N.

我们采用下面的记号：如果 A 和 B 是群 G 的子集，则 AB 表示积 ab 的集合：

【2.12.4】 $$AB=\{x\in G\mid \text{存在 } a\in A, b\in B \text{ 使得 } x=ab\}$$

我们称此为集合的积，虽然在某些场合“集合的积”指的是元素对的集合 $A\times B$.

【2.12.5】**引理** 设 N 是群 G 的一个正规子群，则 N 的两个陪集 aN，bN 的积 $(aN)(bN)$ 仍是一个陪集，且 $(aN)(bN)=abN$.

我们注意集合 $(aN)(bN)$ 包含群 G 中所有形如 $anbn'$ 的元素，其中 n，$n'\in N$.

证明 因为 N 是子群，故 $NN=N$. 由于 N 是正规子群，故左右陪集相等：$Nb=bN$ (2.8.17). 于是由下面的形式推导证明了引理：

$$(aN)(bN)=a(Nb)N=a(bN)=abNN=abN$$ ■

这个引理使我们能够在 $\overline{G}=G/N$ 上定义乘法. 用(2.7.8)的括号记号，定义如下：如果 C_1 和 C_2 是两个陪集，则 $[C_1][C_2]=[C_1C_2]$，其中 C_1C_2 是积集. 这个引理表明积集是另一个陪集. 为计算积陪集 $[C_1][C_2]$，取任意元素 $a\in C_1$ 和 $b\in C_2$，使得 $C_1=aN$ 且 $C_2=bN$. 于是，$C_1C_2=abN$ 是含有元素 ab 的陪集. 故有非常自然的公式

【2.12.6】 $$[aN][bN]=[abN] \quad 或 \quad \overline{a}\,\overline{b}=\overline{ab}$$

这样，由映射 π 在(2.12.2)中的定义，

【2.12.7】 $$\pi(a)\pi(b)=\overline{a}\,\overline{b}=\overline{ab}=\pi(ab)$$

一旦我们证明了 $\overline{G}$ 是个群，则 π 是同态的事实就可从(2.12.7)得出. 由于典范映射 π 是满射(2.7.8)，因此下面的引理证明 $\overline{G}$ 是一个群.

【2.12.8】**引理** 令 G 是个群，且令 Y 是一个带有合成法则的集合，合成法则都用乘法记号表示. 令 $\varphi:G\to Y$ 是一个具有同态性质的满射，即对于所有 a，$b\in G$，均有 $\varphi(ab)=$

67 $\varphi(a)\varphi(b)$. 则 Y 是一个群，且 φ 是同态.

证明 利用满射 φ 把群 G 所满足的公理推广到 Y 上. 下面是结合律的证明：令 y_1，y_2，$y_3\in Y$. 由于 φ 是满射，故 $y_i=\varphi(x_i)$，$x_i\in G$，$i=1$，2，3. 则

$$(y_1y_2)y_3=(\varphi(x_1)\varphi(x_2)\varphi(x_3))=\varphi(x_1x_2)\varphi(x_3)=\varphi((x_1x_2)x_3)$$

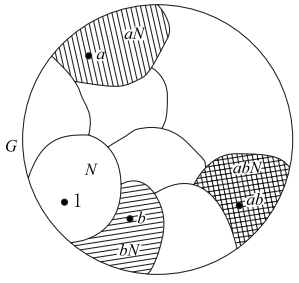
$$\overset{*}{=}\varphi(x_1(x_2x_3))=\varphi(x_1)\varphi(x_2x_3)=\varphi(x_1)(\varphi(x_2)\varphi(x_3))=y_1(y_2y_3)$$

等式中用 $*$ 号标记的部分是群 G 的结合律. 其他部分可由 φ 的同态性质得到. 群的其他公理的验证类似可得. ■

互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

剩下的唯一需要验证的是同态 π 的核为子群 N. $\pi(a)=\pi(1)$ 当且仅当 $\bar{a}=\bar{1}$，或 $[aN]=[1N]$，此式成立当且仅当 $a\in N$. ■

【2.12.9】图

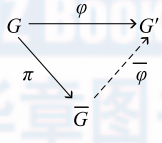


陪集乘法的简略图解

注意 在引理 2.12.5 中假设 N 是群 G 的正规子群是至关重要的. 如果 H 不是正规的，则存在 H 在 G 中的左陪集 C_1 和 C_2 使得积集 C_1C_2 不在一个左陪集内. 回到 S_3 的子群 $H=\langle y\rangle$，积集 $(1H)(xH)$ 包含 4 个元素：$\{1,\ y\}\{x,\ xy\}=\{x,\ xy,\ x^2y,\ x^2\}$. 这不是一个陪集. 子群 H 不是正规的.

下面的定理将商群的构造与一般的群同态联系起来，这个定理提供了确定(等同)商群的基本方法.

【2.12.10】**定理**(第一同构定理) 设 $\varphi:G\to G'$ 是一个满群同态，其核 $N=\ker\varphi$，则商群 $\overline{G}=G/N$ 与像 G' 同构. 准确地说，令 $\pi:G\to\overline{G}$ 是典范映射，则存在唯一一个同构映射 $\overline{\varphi}:\overline{G}\to G'$ 使得 $\varphi=\overline{\varphi}\circ\pi$.



68

证明 $\overline{G}$ 的元素是 N 的陪集，也是映射 φ 的纤维(2.7.15). 映射 $\overline{\varphi}$ 将非空纤维映射到纤维的像：$\overline{\varphi}(\overline{x})=\varphi(x)$. 对于任何集合间的满射 $\varphi:G\to G'$，可以形成纤维的集合 $\overline{G}$，然后可得到如上的图，其中 $\overline{\varphi}$ 是双射，它将一个纤维映射到它的像. 当 φ 是群同态时，$\overline{\varphi}$ 是同构，这是因为 $\overline{\varphi}(\overline{ab})=\varphi(ab)=\varphi(a)\varphi(b)=\overline{\varphi}(\overline{a})\overline{\varphi}(\overline{b})$. ■

【2.12.11】**推论** 令 $\varphi:G\to G'$ 是一个群同态，其核为 N，像为 H'. 商群 $\overline{G}=G/N$ 同构于 H'.

两个例子：绝对值映射 $\mathbf{C}^\times\to\mathbf{R}^\times$ 的像是正实数，其核是单位圆 U. 这个定理断言商群 $\mathbf{C}^\times/U$ 同构于正实数的乘法群. 另外，行列式是一个满同态 $GL_n(\mathbf{R})\to\mathbf{R}^\times$，其核为特殊线性群 $SL_n(\mathbf{R})$. 因而商群 $GL_n(\mathbf{R})/SL_n(\mathbf{R})$ 同构于 $\mathbf{R}^\times$.

还有第二、第三同构定理，虽然这些定理不如第一同构定理重要.

练　　习

第一节　合成法则

1.1 令 S 是一个集合. 证明：对于任意 $a,b\in S$，由 $ab=a$ 定义的合成法则是结合的. 对怎样的集合这

互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

个合成法则有恒等元？

1.2 证明在本节最后列出的逆的性质.

1.3 令 $\mathbf{N}$ 表示自然数集合$\{1, 2, 3, \cdots\}$，且令 $s:\mathbf{N}\to\mathbf{N}$ 是平移映射，定义为 $s(n)=n+1$. 证明 s 没有右逆，但有无穷多个左逆.

第二节 群与子群

2.1 作出对称群 S_3 的乘法表.

2.2 令 S 是具有恒等元和合成法则满足结合律的集合. 证明 S 的所有具有逆元的集合构成一个群.

2.3 令 x，y，z 和 w 是群 G 中的元素.

(a) 已知 $xyz^{-1}w=1$，求 y.

69 (b) 设 $xyz=1$，是否可据此得出 $yzx=1$ 或 $yxz=1$？

2.4 在下列何种情形下 H 是 G 的子群？

(a) $G=GL_n(\mathbf{C})$，$H=GL_n(\mathbf{R})$.

(b) $G=\mathbf{R}^\times$，$H=\{1, -1\}$.

(c) $G=\mathbf{R}^+$，H 是正整数集合.

(d) $G=\mathbf{R}^\times$，H 是正实数集合.

(e) $G=GL_2(\mathbf{R})$和 H 是所有形如$\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$的矩阵的集合，其中 $a\neq 0$.

2.5 在子群的定义中，子群 H 的恒等元要求是群 G 的恒等元. 可以只要求子群 H 有恒等元，不必要求此恒等元为群 G 的恒等元. 证明：如果 H 有恒等元，则这个恒等元是群 G 的恒等元. 类似地证明子群 H 中的逆元也是其在群 G 中的逆元.

2.6 令 G 是一个群. 定义一个反群 G°有下面的合成法则 $a*b$：基础集合还是集合 G，但合成法则是 $a*b=ba$. 证明 G°是一个群.

第三节 整数加群的子群

3.1 令 $a=123$ 且 $b=321$. 求 $d=\gcd(a, b)$，并把 d 表示成 $ra+bs$ 的形式.

3.2 证明：如果正整数 a，b 的和是一个素数 p，则 $\gcd(a, b)=1$.

3.3 (a) 定义集合$\{a_1, a_2, \cdots, a_n\}$的最大公约数. 证明它是整数 a_1，a_2，$\cdots$，a_n 的组合.

(b) 如果$\{a_1, a_2, \cdots, a_n\}$的最大公约数是 d，则$\{a_1/d, a_2/d, \cdots, a_n/d\}$的最大公约数是 1.

第四节 循环群

4.1 令 a 和 b 是群 G 的元素. 设 a 的阶为 7 且 $a^3b=ba^3$. 证明 $ab=ba$.

4.2 一个 n 次单位根是一个复数 z 满足 $z^n=1$.

(a) 证明单位元的 n 次方根构成 $\mathbf{C}^\times$ 的 n 阶循环子群.

(b) 确定所有单位元的 n 次方根的积.

4.3 令 a 和 b 是群 G 的元素. 证明 ab 和 ba 有相同的阶.

4.4 刻画所有没有真子群的群.

4.5 证明循环群的任意子群还是循环群. 通过研究指数并应用对 $\mathbf{Z}^+$ 的子群的描述来加以证明.

4.6 (a) 令 G 是 6 阶循环群. G 有多少生成元？对 5 阶和 8 阶循环群讨论同样的问题.

(b) 讨论任意阶循环群的生成元的个数.

4.7 令 x 和 y 是群 G 的元素. 设 x，y 和 xy 的阶均为 2. 证明集合 $H=\{1, x, y, xy\}$是 G 的子群，且

70 阶为 4.

互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

4.8 (a) 证明(1.2.4)中第一、第三型初等矩阵生成 $GL_n(\mathbf{R})$.

(b) 证明(1.2.4)中第一型初等矩阵生成 $SL_n(\mathbf{R})$. 先对 2×2 矩阵证明此结论.

4.9 对称群 S_4 有多少个 2 阶的元素?

4.10 举例说明群中有限阶元素的积未必是有限阶的. 如果是交换群呢?

4.11 (a) 采用行约简的方法证明对换生成对称群 S_n.

(b) 对于 $n\geqslant 3$, 证明 3-循环生成交错群 A_n.

第五节 同态

5.1 设 $\varphi: G\to G'$ 是群的满同态. 证明: 若 G 是循环群, 则 G' 也是循环群; 若 G 是阿贝尔群, 则 G' 也是阿贝尔群.

5.2 设 H 和 K 是群 G 的子群, 则 $H\cap K$ 是 H 的子群, 且如果 K 是 G 的正规子群, 则 $H\cap K$ 是 H 的正规子群.

5.3 令 U 是 2×2 可逆上三角矩阵 $A=\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ 的群, 且 $\varphi: U\to \mathbf{R}^\times$ 满足 $A\rightsquigarrow a^2$. 证明 φ 是同态, 并求此同态的核和像.

5.4 令 $f: \mathbf{R}^+\to \mathbf{C}^\times$ 满足 $f(x)=\mathrm{e}^{\mathrm{i}x}$. 证明 f 是同态, 并求此同态的核和像.

5.5 证明: 形如 $M=\begin{bmatrix} A & B \\ 0 & D \end{bmatrix}$ 的 $n\times n$ 分块矩阵构成 $GL_n(\mathbf{R})$ 的一个子群 H, 其中 $A\in GL_r(\mathbf{R})$, $D\in GL_{n-r}(\mathbf{R})$; 且映射 $\varphi: H\to GL_r(\mathbf{R})$ 满足 $M\rightsquigarrow A$ 是一个同态. 同态的核是什么?

5.6 确定 $GL_n(\mathbf{R})$ 的中心.

提示: 要求可逆矩阵 A 使得其与任何可逆矩阵 B 可换. 不要用一般矩阵尝试, 要用初等矩阵尝试.

第六节 同构

6.1 令 G' 是形如 $\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$ 的实矩阵群. 映射 $\mathbf{R}^+\to G'$ 将 $x\to \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$ 是同构映射吗?

6.2 刻画所有同态 φ: $\mathbf{Z}^+\to\mathbf{Z}^+$. 确定哪些是单射, 哪些是满射, 哪些是同构.

6.3 证明: 函数 $f=\dfrac{1}{x}$, $g=\dfrac{x-1}{x}$ 生成一个函数群, 合成法则是函数的合成, 它同构于对称群 S_3.

6.4 证明: 在群中, 积 ab 和 ba 是共轭元.

6.5 确定两个矩阵 $A=\begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix}$ 与 $B=\begin{bmatrix} 1 & 1 \\ -2 & 4 \end{bmatrix}$ 在一般线性群 $GL_2(\mathbf{R})$ 中是否为共轭元. 71

6.6 矩阵 $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ 和 $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ 是否为 $GL_2(\mathbf{R})$ 中的共轭元? 是否为 $SL_2(\mathbf{R})$ 中的共轭元?

6.7 令 H 是 G 的子群, 并设 $g\in G$. 共轭子群 gHg^{-1} 定义为所有共轭 ghg^{-1} 的集合, 其中 $h\in H$. 证明 gHg^{-1} 是 G 的子群.

6.8 证明映射 $A\rightsquigarrow (A^{\mathrm{t}})^{-1}$ 是 $GL_2(\mathbf{R})$ 的自同构.

6.9 证明群 G 和它的反群 G^o(练习 2.6)同构.

6.10 确定下列群的自同构群.

(a) 10 阶循环群, (b)对称群 S_3.

6.11 令 a 是群 G 的元素. 证明: 如果集合 $\{1, a\}$ 是 G 的正规子群, 则 a 属于 G 的中心.

互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

第七节 等价关系和划分

7.1 令 G 是一个群，证明：对于某个 $g\in G$ 使得 $b=gag^{-1}$ 的关系 $a\sim b$ 是一个等价关系.

7.2 集合 S 上等价关系由 $S\times S$ 的满足 $a\sim b$ 的对(a,b)所组成的集合 R 来确定. 将等价关系的公理用子集 R 来表示.

7.3 用练习 7.2 中的记号，两个等价关系 R 和 R' 的交 $R\cap R'$ 是否是等价关系？$R\cup R'$ 是否是等价关系？

7.4 设 R 是实数集合上的一个等价关系. R 可视为(x,y)平面的子集. 用练习 7.2 中的记号，解释自反性和对称性的几何意义.

7.5 用练习 7.2 中的记号，下面(x,y)平面的子集 R 定义了实数集合 $\mathbf{R}$ 上的一个关系. 确定哪个关系满足公理(2.7.3).

(a) $R=\{(s,s)\mid s\in\mathbf{R}\}$.

(b) $R=$空集.

(c) $R=$轨迹$\{xy+1=0\}$.

(d) $R=$轨迹$\{x^2y-xy^2-x+y=0\}$.

7.6 5 个元素的集合上可以定义多少种等价关系？

第八节 陪集

8.1 令 H 是交错群 A_4 的一个由置换(**1 2 3**)生成的循环子群. 具体写出 H 的所有左陪集和右陪集.

8.2 在实向量加群 $\mathbf{R}^m$ 中，令 W 是齐次线性方程组 $AX=0$ 的解集合. 证明非齐次线性方程组 $AX=B$ 的解集合或为空集或为 W 的一个(加法)陪集.

8.3 阶为某个素数 p 的方幂的群含有阶为 p 的元素吗？

8.4 阶为 35 的群是否含有阶为 5 的元素？是否含有阶为 7 的元素？

8.5 一个有限群包含阶为 10 的元素 x，也包含阶为 6 的元素 y，对该群 G 的阶有什么结论？

72 8.6 令 $\varphi:G\to G'$ 是群同态. 假设 $|G|=18$，$|G'|=15$，且 φ 不是平凡同态. 同态核的阶是多少？

8.7 22 阶群 G 包含元素 x 和 y，其中 $x\neq1$，y 不是 x 的幂. 证明由这些元素生成的子群是整个群 G.

8.8 令 G 是一个 25 阶群. 证明 G 至少有一个 5 阶子群，且如果它只有一个 5 阶子群，则此群是循环群.

8.9 令 G 是一个有限群. 在什么情况下由 $\varphi(x)=x^2$ 定义的映射 $\varphi:G\to G$ 是群 G 的自同构？

8.10 证明指标为 2 的任意子群为正规子群. 举例说明指标为 3 的子群未必是正规子群.

8.11 令 G 和 H 是 $GL_2(\mathbf{R})$的以下形式的子群：

$$G=\left\{\begin{bmatrix}x & y\\ 0 & 1\end{bmatrix}\right\},H=\left\{\begin{bmatrix}x & 0\\ 0 & 1\end{bmatrix}\right\}$$

其中 x 和 y 是实数，且 $x>0$. 群 G 中的元素可由右半平面的点来表示. 简要证明半平面可以分划为 H 的左陪集和右陪集.

8.12 令 S 是群 G 的包含恒等元 1 的子集，且使得左陪集 $aS(a\in G)$划分群 G. 证明 S 是 G 子群.

8.13 令 S 是一个带有合成法则的集合. S 的一个划分 $\Pi_1\cup\Pi_2\cup\cdots$是与合成法则相容的，对于所有 i 和 j，积集

$$\Pi_i\Pi_j=\{xy\mid x\in\Pi_i,y\in\Pi_j\}$$

包含在划分的某个单个子集 Π_k 中.

(a) 整数集合 $\mathbf{Z}$ 可以划分为三个子集[正整数]，[负整数]，[{0}]. 讨论合成法则 $+$，$\times$ 与这个划分的相容程度.

互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

(b) 刻画与加法相容的所有整数集合的划分.

第九节 模算术

9.1 对于怎样的整数 n 使得 2 在 $\mathbf{Z}/\mathbf{Z}n$ 中有乘法逆元?

9.2 a^2 模 4 的可能值是什么? 模 8 呢?

9.3 证明每个整数 a 模 9 同余于其十进制各位数之和.

9.4 解同余方程 $2x\equiv 5$ 模 9 和模 6.

9.5 确定使同余方程 $2x-y\equiv 1$, $4x+3y\equiv 2 \pmod n$ 有解的整数 n.

9.6 证明中国剩余定理: 设 a, b, u, v 为整数, 且设 a, b 的最大公约数是 1, 则存在整数 x 使 $x\equiv u \pmod a$ 且 $x\equiv b \pmod b$.

提示: 先讨论 $u=0$, $v=1$ 的情形.

9.7 确定每一个矩阵 $A=\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$ 和 $B=\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}$ 的阶, 其中矩阵元素是模 3 同余的. 73

第十节 对应定理

10.1 描述如何从循环分解中区分一个置换是奇还是偶的.

10.2 令 H 和 K 是群 G 的子群.

(a) 证明 H 和 K 的两个陪集的交集 $xH\cap yK$ 或为空集或为子群 $H\cap K$ 的一个陪集;

(b) 如果 H 和 K 在 G 中的指标是有限的, 则 $H\cap K$ 在 G 中的指标也是有限的.

10.3 令 G 和 G' 是分别由 x 和 y 生成的 12 阶和 6 阶循环群, 令 $\varphi: G\to G'$ 是由 $\varphi(x^i)=y^i$ 定义的映射. 具体列出在对应定理中提到的对应.

10.4 用对应定理中的记号, 令 H 和 H' 是对应子群. 证明 $[G:H]=[G':H']$.

10.5 参照在例 2.5.13 中的同态 $S_4\to S_3$, 确定 S_4 的包含核 K 的 6 个子群.

第十一节 积群

11.1 令 x 是群 G 中阶为 r 的元素, y 是群 G' 中阶为 s 的元素, 元 (x, y) 在积群 $G\times G'$ 中的阶是多少?

11.2 用对称群 S_3 的通常记号, 当 H 和 K 是子群 $\langle y\rangle$ 和 $\langle x\rangle$ 时, 命题 2.11.4 告诉我们什么?

11.3 证明两个无限循环群的积不是无限循环群.

11.4 在下面每一种情形中, 确定 G 是否同构于积群 $H\times K$.

(a) $G=\mathbf{R}^\times$, $H=\{\pm 1\}$, $K=\{$正实数$\}$.

(b) $G=\{2\times 2$ 可逆上三角矩阵$\}$, $H=\{$可逆对角矩阵$\}$, $K=\{$对角线元素为 1 的上三角矩阵$\}$.

(c) $G=\mathbf{C}^\times$, $H=\{$单位圆$\}$, $K=\{$正实数$\}$.

11.5 令 G_1 和 G_2 是群, 且 Z_i 是 G_i 的中心. 证明积群 $G_1\times G_2$ 的中心为 $Z_1\times Z_2$.

11.6 令 G 是一个分别包含阶为 3 和阶为 5 的正规子群的群. 证明 G 包含一个阶为 15 的元素.

11.7 令 H 是 G 的子群, 令 $\varphi: G\to H$ 是一个同态, 其在 H 上的限制为恒等映射, 令 N 是其核. 关于乘积映射 $H\times N\to G$ 有何结论?

11.8 令 G, G' 和 H 是群. 建立从 H 到积群的同态 $\Phi: H\to G\times G'$ 以及由同态 $\varphi: H\to G$ 和 $\varphi': H\to G'$ 构成的对 (φ, φ').

11.9 令 H 和 K 是 G 的子群. 证明集合的积 HK 是 G 的子群当且仅当 $HK=KH$.

第十二节 商群

12.1 证明: 如果子群 H 不是群 G 的正规子群, 则存在左陪集 aH 与 bH, 它们的积不是陪集. 74

互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

12.2 在一般线性群 $GL_3(\mathbf{R})$ 中，考虑形如

$$H=\begin{bmatrix}1 & * & * \\ & 1 & * \\ & & 1\end{bmatrix} \quad 和 \quad K=\begin{bmatrix}1 & 0 & * \\ & 1 & 0 \\ & & 1\end{bmatrix}$$

的子集，其中 $*$ 代表任意实数. 证明 H 是 GL_3 的子群，K 是 H 的正规子群，确定商群 H/K. 确定 H 的中心.

12.3 令 P 是群 G 的划分且具有如下性质：对于划分中任意两个元素对 A，B，集合的积 AB 完全包含在划分的另一个元素 C 中. 令 N 是划分 P 的一个元素且包含 1. 证明 N 是 G 的正规子群且 P 是其陪集的集合.

12.4 令 $H=\{\pm 1, \pm i\}$ 是群 $G=\mathbf{C}^{\times}$ 中的四次单位根组成的子群. 明确写出 H 在 G 中的陪集. G/H 与 G 同构吗？

12.5 令 G 是上三角实矩阵 $\begin{bmatrix}a & b \\ 0 & d\end{bmatrix}$ 所组成的群，其中 $a\neq 0$，$d\neq 0$，对于下列子集 S，确定其是否为子群，是否为正规子群. 如果 S 是正规子群，确定商群 G/S.

(i) S 是定义中满足 $b=0$ 的子集.

(ii) S 是定义中满足 $d=1$ 的子集.

(iii) S 是定义中满足 $a=d$ 的子集.

杂题

M.1 描述一个整数矩阵 A 当其逆矩阵也是整数矩阵时其第一列列向量 $(a, c)^t$ 是什么.

M.2 (a) 每个偶数阶群都包含一个阶为 2 的元素.

(b) 每个 21 阶群都包含一个阶为 3 的元素.

M.3 分析下列三种情况，对 6 阶群进行分类：

(i) G 包含一个阶为 6 的元素.

(ii) G 包含一个阶为 3 的元素，但不包含一个阶为 6 的元素.

(iii) G 的所有元素的阶为 1 或 2.

M.4 一个半群 S 是一个带有满足结合律的合成法则且有恒等元的集合. 元素不要求有逆元，且消去律不必成立. 一个半群 S 称为是由元素 s 生成的，如果 s 的非负幂的集合 $\{1, s, s^2, \cdots\}$ 等于 S. 对一个生成元的半群进行分类.

M.5 令 S 是一个满足削去律 2.2.3 的有限半群(见练习 M.4)，证明 S 是群.

*M.6 令 $a=(a_1, \cdots, a_k)$ 和 $b=(b_1, \cdots, b_k)$ 是 k 维空间 $\mathbf{R}^k$ 中的点. 从 a 到 b 的一条路是一个在 $\mathbf{R}^k$ 的区间 $[0, 1]$ 上取值的连续函数，即函数 $X:[0, 1]\to\mathbf{R}^k$，使 $t\rightsquigarrow X(t)=(x_1(t), \cdots, x_k(t))$，满足条件 $X(0)=a$ 和 $X(1)=b$. 若 S 是 $\mathbf{R}^k$ 的子集且 a，$b\in S$，定义 $a\sim b$，如果 a，b 可由一条完全在 S 中的路连起来.

75

(a) 证明 $\sim$ 是 S 上的一个等价关系. 注意你构造的路在集合 S 中.

(b) $\mathbf{R}^k$ 的子集 S 称为路连通的，如果对任意两点 a，$b\in S$，有 $a\sim b$ 成立. 证明 S 的任意子集可划分为路连通子集，而且不同子集中的两个点不能由 S 中的路连接.

(c) $\mathbf{R}^2$ 中的下列轨道中哪些是路连通的？$\{x^2+y^2=1\}$，$\{xy=0\}$，$\{xy=1\}$.

*M.7 $n\times n$ 矩阵集合可以等同于空间 $\mathbf{R}^{n\times n}$. 设 G 是 $GL_n(\mathbf{R})$ 的子群. 用练习 M.6 的记号，证明：

互动出版网 China-Pub.com 专业图书网上第一专营店 www.china-pub.com 独家提供样章

(a) 如果 A，B，C，$D\in G$，且如果 G 中有 A 到 B 的路和 C 到 D 的路，则 G 中有一条 AC 到 BD 的路.

(b) 可以连到恒等矩阵 I 的矩阵集合构成 G 的一个正规子群(称为 G 的连通分支).

*M. 8 (a) 群 $SL_n(\mathbf{R})$由第一型的初等矩阵生成(见练习 4.8). 用这一事实证明这个群是路连通的.

(b) 证明 $GL_n(\mathbf{R})$是两个路连通子集的并，并描述它们.

M. 9 (双陪集)令 H 和 K 是群 G 的子群，令 g 是 G 的元素. 集合

$$HgK=\{x\in G\,|\,x=hgk,\quad h\in H,k\in K\}$$

称为双陪集. 双陪集是群 G 的划分吗?

M. 10 令 H 是群 G 的子群. 证明双陪集(参见练习 M. 9)

$$HgH=\{h_1gh_2\,|\,h_1,h_2\in H\}$$

是左陪集 gH 当且仅当 H 是正规的.

*M. 11 大多数可逆矩阵可以写成一个下三角矩阵 L 和一个上三角矩阵 U 且 U 的主对角线元素为 1 的矩阵乘积 $A=LU$.

(a) 当矩阵 A 已知，如何求 L 和 U.

(b) 证明分解的唯一性，即存在至多一种方式将矩阵 A 表示成这样的乘积.

(c) 证明每个可逆矩阵可以写成乘积 LPU 的形式，其中 L 和 U 同上，P 是置换矩阵.

(d) 刻画双陪集 LgU(参见练习 M. 9).

M. 12 (邮票问题)令 a 和 b 是互素的正整数.

(a) 证明每个充分大的正整数 n 可写成 $ra+sb$ 的形式，其中 r，s 为正整数.

(b) 确定不具有这种形式的最大整数.

M. 13 (一个游戏)初始位置为点(1，1)，一个点(a，b)只允许移动到点($a+b$，b)或(a，$a+b$). 这样从始点移动一步后的位置是(2，1)或(1，2). 确定能到达的点.

M. 14 (生成 $SL_2(\mathbf{Z})$)证明两个矩阵

$$E=\begin{bmatrix}1&1\\0&1\end{bmatrix},E'=\begin{bmatrix}1&0\\1&1\end{bmatrix}$$

76

生成所有行列式为 1 的整数矩阵的群 $SL_2(\mathbf{Z})$. 记住它们生成的子群由四个元素 E，E'，E^{-1}，E'^{-1}的积构成.

提示：不要直接将矩阵写成生成元的乘积. 用行约简.

M. 15 (初等矩阵生成的半群)确定矩阵 A 的半群 S(见练习 M. 4)，其中矩阵 A 是由下面两个矩阵作为项的任意长度的矩阵乘积：

$$\begin{bmatrix}1&1\\0&1\end{bmatrix}\quad 或\quad \begin{bmatrix}1&0\\1&1\end{bmatrix}$$

证明 S 中每个元素恰有一种方式可以表示为乘积的形式.

M. 16 (同音群：一个数学娱乐)由定义，英语单词是同音的，如果它们的音标在字典里是相同的. 同音群$\mathcal{H}$由字母表的字母生成，并服从下面的关系：发音相同的英文单词看做群中相同的元素，例如 $be=bee$，且由于$\mathcal{H}$是群，我们可以消去 be 得到 $e=1$. 试着确定群$\mathcal{H}$.

77