第 6 章 群

从本章起, 我们将分群、环和域三个部分介绍代数学的基础内容. 群、环和域等代数理论是近世代数的基础, 对当今数学乃至其它学科有非常重要影响, 也推动了数论、几何学的发展. 近世代数学发源于 19 世纪上半叶的方程理论, 主要研究某一方程（组）是否可解, 如何求出方程所有的根, 以及方程的根有何性质等问题. 法国数学家埃瓦里斯特·伽罗瓦（Évariste Galois）在 1832 年运用群的思想彻底解决了用根式求解代数方程的可能性问题. 与此同时, 当代的编码与密码学等信息科学理论的建立与发展也以其为基础.

本章主要介绍群的相关内容, 子群的概念, 循环群与置换群, 陪集与商群的若干性质, 最后介绍重要的同态、同构概念以及同态基本定理.

6.1 群

我们首先来介绍群的定义和基本性质.

群的概念离不开运算, 而运算的实质就是将两个同类型的元素组合在一起形成第三个与它们同样类型的元素. 比如, 我们熟悉的普通加减乘除运算都是将两个数组合后形成第三个数, 还有函数的复合是将两个函数组合后形成第三个函数. 二元运算的定义如下:

集合 G 上的**二元运算**是一个如下的函数

$$*: G\times G\to G.$$

更具体地说, 集合 G 上的二元运算是为每一个 G 上的有序对(a, b)分配一个 G 中的确定元素 $*(a,b)$ 与之对应, 通常我们将 $*(a,b)$ 用更加自然的方式写成 $a*b$, 当然, 我们也可以用“ • ”、“⊙”、“⊕”、“×”、“ ⋆ ”、“+”等符号来表示这样的二元运算. 有时为了简化书写, 在不引起歧义的情况下, 可以用 ab 或 $a+b$ 来表示 $a*b$.

例如, 加法运算是函数$+(a, b) = a+b$, 减法运算是函数$-(a, b) = a-b$, 函数的复合是函数$\circ(f,g)=g\circ f$. 然而, 请注意, 二维及以上向量的点积运算就不是我们这里定义的二元运算, 因为参与点积运算的两个对象是向量, 而计算结果是一个数, 它们属于不同的集合.

定义 6.1.1 G 是一个非空集合, $*$是定义在集合 G 上的一个二元运算. $(G, *)$被称为**半群**, 如果$(G, *)$满足下列条件:

1. 封闭: 对任意 $a, b\in G$, 有 $a* b\in G$;
2. 结合律: 对任意 $a,b,c\in G$, 有

$$a* (b * c) =(a * b) * c$$

例 6.1.1 整数集 $\mathbf{Z}$ 在、有理数集 $\mathbf{Q}$、实数集 $\mathbf{R}$、复数集 $\mathbf{C}$ 在普通加法+下构成半群, $\mathbf{Z}$、$\mathbf{Q}$、$\mathbf{R}$、$\mathbf{C}$ 在普通乘法下也构成半群.

定义 6.1.2 半群$(G, *)$被称为**群**, 如果满足下列条件:

1. 单位元: 存在 $e\in G$, 对任意 $a\in G$ 有 $e * a = a$,并称元素 e 为 G 的**左幺元**,
2. 逆元: 对任意 $a\in G$, 存在 $a'\in G$ 使得 $a' * a =e$,并称元素 a 为 a 的**左逆元.**

例 6.1.2 $\mathbf{Z}$、$\mathbf{Q}$、$\mathbf{R}$、$\mathbf{C}$ 在普通加法+下构成群, $\mathbf{Z}^*=\mathbf{Z}\setminus\{0\}$在普通乘法×下仅构成半群, 而 $\mathbf{Q}^*=\mathbf{Q}\setminus\{0\}$, $\mathbf{R}^*=\mathbf{R}\setminus\{0\}$, $\mathbf{C}^*=\mathbf{C}\setminus\{0\}$在普通乘法×下构成群.

例 6.1.3 实数域 $\mathbf{R}$ 上的所有 n 阶方阵构成的集合对于矩阵加法构成群, 其中幺元为 n 阶

零方阵.

定理 6.1.1 G 是一个群, e 为 G 的**左幺元**, 则有

(1) 对任意 $a\in G$, b 是 a 的左逆元, 则 b 也是 a 的右逆元, 称 b 是 a 的**逆元**.

(2) e 也是 G 的**右幺元**, 即对任意 $a\in G$ 有 $a*e=a$, 故 e 为 G 的**幺元**.

(3) 对任意 $a\in G$, 其逆元唯一.

证 (1) 设 c 是 b 的左逆元, 则有

$$a*b=e*(a*b)=(c*b)*(a*b)=c*(b*a)*b=c*e*b=c*(e*b)=c*b=e.$$

(2) 设 b 是 a 的逆元, 则有

$$a*e=a*(b*a)=(a*b)*a=e*a=a.$$

(3) 设 b,d 是 a 的逆元, 则有

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

定义 6.1.3 群$(G,*)$元素个数$|G|$被称为群的**阶**, 如果$|G|$有限, 则称 G 为有限群.

例 6.1.4 任意整数 n, 定义群$(\mathbf{Z}_n,+)$, 其中 $\mathbf{Z}_n$ 为集合$\{0,1,\ldots,n-1\}$, 运算+为模数 n 加法, 则$(\mathbf{Z}_n,+)$为有限群, 且该群的阶为 n.

定义 6.1.4 如果群 G 中的二元运算*还满足交换律, 即对任意 $a,b\in G$ 有 $a*b=b*a$, 我们就称 G 是一个**交换群**或 **Abel 群**, 否则称之为**非交换群**.

例 6.1.5 上面的四个例题均为交换群. 下面给出非交换群的例子.

1. 设 $GL(n,\mathbf{R})$为实数域 R 上的所有 n 阶可逆方阵构成的集合, 我们称之为实数域上的 n 维**一般变换群**. 对于 $GL(n,\mathbf{R})$上的矩阵乘法$\times$ 以及任意元素 A,B, 一般情况下 $A\times B=B\times A$ 不成立, 故 $GL(n,\mathbf{R})$对于矩阵乘法是非交换群, 而例题 6.1.3 中 n 阶方阵对于矩阵加法构成交换群. 同样, 设 $SL(n,\mathbf{R})$为实数域 R 上的所有 n 阶行列式值为 1 的方阵构成的集合, 我们称之为实数域上的 n 维**特殊变换群**, 容易验证 $SL(n,\mathbf{R})$对于矩阵乘法构成非交换群.

2. 在函数的复合运算下, 所有实数域 $\mathbf{R}$ 到 $\mathbf{R}$ 上的可逆函数组成一个群. 其中, 函数的复合满足结合律, 而且两个可逆函数的复合还是可逆函数, 单位元是恒等函数, 任意元素的逆元是其逆函数. 但是, 函数的复合不满足交换律.

为了符号使用的方便, 我们一般用“1”来表示群的单位元, 用 a^{-1} 表示 a 的逆元.

定理 6.1.2 G 是一个群, $a,b\in G$, 则方程 $ax=b$ 和 $ya=b$ 有唯一的解.

证 对 $ax=b$ 两边同时左乘以 a^{-1}, 则 $a^{-1}(ax)=a^{-1}b$, 所以得到解为 $x=a^{-1}b$, a^{-1} 是唯一的, 因此该解是唯一解. 同理, 第二个方程的唯一解为 $y=ba^{-1}$.

定理 6.1.3 对正整数 m 和 n, 群中元素 a 的幂满足:

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

(2) $a^{n+m}=a^na^m$.

(3) $(a^n)^m=a^{nm}$.

证明 略(留给读者作练习).

对于一般整数(不一定是正整数)m 和 n, 上面的定理也是成立的, 虽然很直观, 不过证明略繁琐, 读者直接使用即可.

另外, 当我们不是抽象地讨论一些特定的群时, 我们对群上的运算和元素一般使用自然的表示方法: 但如果我们使用“+”表示运算符, 则用 0 表示单位元, 用$-a$ 表示 a 的逆元; 对正整数 n, 用 na 表示 $\underbrace{a+a+\ldots+a}_{\text{共}n\text{项}}$, 用$-na$ 表示 $\underbrace{-a-a-\ldots-a}_{\text{共}n\text{项}}$, 且 $0a=0$. 此时, 上面定理中的三个表达式需要改写如下,

(1) $n(-a)=-(na)$.

(2) $(n+m)a = na+ma$.

(3) $m(na)=(mn)a$.

定义 6.1.5 在群 G 中，对元素 a 来说，使 $a^n=1$ 的最小正整数 n 称为元素 a 的**阶**，记为 **ord(a)**. 如果不存在这样的正整数，那么我们称 a 为无限阶元素.

例 6.1.6 (1) 在任何群中，ord(1)=1，且只有单位元的阶为 1.

(2) 普通加法下的 $\mathbf{Z}$、$\mathbf{Q}$、$\mathbf{R}$、$\mathbf{C}$ 中，每个非零数都是无限阶的.

(3) 普通乘法下的 $\mathbf{Q}^*$，$\mathbf{R}^*$，$\mathbf{C}^*$ 中，ord(−1)=1，其他不等于 1 和−1 的数都是无限阶的.

定理 6.1.4 群 G 中元素 a 的阶为 k，如果 $a^n=1$，那么 $k|n$.

证明 由带余除法可知，$n= qk+r$，其中 $0\le r<k$. 所以

$$1=a^n= a^{qk+r}=(a^k)^q a^r=a^r,$$

由阶的定义中的“最小”性质可知，只能 $r=0$，即 $k|n$.

定理 6.1.5 有限群 G 中元素 a 的阶必为有限数.

证明 观察如下序列

$$1,\ a,\ a^2,\cdots,\ a^n,\cdots$$

由于以上序列中的元素都属于 G，且 G 是有限群，所以该无限长序列中必然存在重复的元素，设重复的元素为 a^m 和 a^n，其中 $m>n$，即

$$a^m=a^n,$$

所以

$$1= a^m a^{-n}= a^{m-n},$$

其中 $m-n>0$ 说明 a 的阶必为有限数.

下面给出几个稍微复杂一些的群的例子.

例 6.1.7 Klein 四元群为集合 $G=\{a, b, c, e\}$，其上二元运算 $\bullet$ 的定义如表 6.1.1 所示.

表 6.1.1Klein 四元群的定义

$\bullet$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

观察表 6.1.1，$\forall x\in G$，都有 $x\bullet e = e\bullet x = x$，所以 e 是单位元；$\forall x\in G$，都有 $x\bullet x = e$，所以 x 的逆元就是 x 自身. 尽管通过验证$\forall x, y, z\in G$, 都有$(x\bullet y)\bullet z=x\bullet(y\bullet z)$, 我们可以证明$(G, \bullet)$满足结合律，但是这种方法相当繁琐. 我们后面讲到的知识可以用来提供更好的证明方法.

有限群 G 中元素的运算关系可以以类似以上列表的形式给出，此表称为 G 的**群表**.

习题 6.1

A 组

1. 试给出若干不是群的半群.
2. 在整数集 $\mathbf{Z}$ 中定义二元运算“$*$”为

(1) $n*m=-n-m,\quad n,m\in\mathbf{Z}$. 证明这个二元运算是交换的, 但不是结合的.

(2) $n*m=n+m-2,\quad n,m\in\mathbf{Z}$. 证明$(\mathbf{Z},*)$是群.

3. 证明: 若 G 为有限集且对运算“$\cdot$”封闭, 满足结合律与消去律, 则$(G,\cdot)$构成一个群. 试问结论对无限集合是否成立.

4. 已知群$(G_1,+_1)$, $(G_2,+_2)$, 构造集合 $G=G_1\times G_2=\{(x,y)|x\in G_1,y\in G_2\}$以及运算+满足

$$(x_1,y_1)+(x_2,y_2)=(x_1+_1x_2,y_1+_2y_2)$$

证明$(G,+)$是群.

B 组

5. 设群 G 中每个非幺元的阶为 2, 证明该群是 Abel 群.

6. 任给集合 S, 定义2^S为所有 S 子集构成的集合, 称之为 S 的幂集. 证明:

(1) $(2^S,\cup)$ 与 $(2^S,\cap)$ 均为半群.

(2) 若对 S 子集定义运算$A\Delta B=(A\backslash B)\cup(B\backslash A)$, 则$(2^S,\Delta)$是群.

7. 设M是幺半群, e是其幺元, 对于元素$a\in M$, 若存在$a^{-1}\in M$ 使得$aa^{-1}=a^{-1}a=e$, 则称 a 可逆, 试证明:

(1) 若$a\in M$ 且$b,c\in M$使得$ab=ca=e$, 则a 可逆且$a^{-1}=b=c$;

(2) $a\in M$ 可逆, 则$a^{-1}=b$ 当且仅当$aba=a,ab^2a=e$;

(3) M 的子集 G 为群的充分必要条件为 G 中的每个元素可逆, 并且对$\forall g_1,g_2\in G$, 有 $g_1g_2^{-1}\in G$;

(4) M 中所有可逆元素构成群.

6.2 子群

我们接下来介绍子群的概念, 并讨论群与子群的相关内容.

定义 6.2.1 $(G,*)$是一个群, 子集$H\subset G$, 如果 H 对于运算*也构成群, 则称 H 是 G 的**子群**, 记为 $\boldsymbol{H\leqslant G}$. 由于$\{1\}$和 G 本身必然是 G 的子群, 所以为了与其他子群进行区分, 我们称$\{1\}$和 G 为**平凡子群**, 否则为**非平凡子群**; 如果子群 $H\neq G$, 我们称 H 为**真子群**, 记为 $\boldsymbol{H<G}$.

例 6.2.1 在普通加法下, $\mathbf{Z}\leq\mathbf{Q}\leq\mathbf{R}\leq\mathbf{C}$.

例 6.2.2 群的子集是群但不是子群的例子:

在普通加法下 $\mathbf{R}$ 是群, 在普通乘法下 $\mathbf{Q^*}$ 是群, $\mathbf{Q^*}$ 明显是 $\mathbf{R}$ 的子集, 但是, $\mathbf{Q^*}$ 不是 $\mathbf{R}$ 的子群. 从这个例子我们看到子群定义中要求子群和群的二元运算具有一致性的重要性.

例 6.2.3 在向量加法下, 一个向量空间的任意子空间是它的子群.

例 6.2.4 $SL(n,\mathbf{R})$为 $GL(n,\mathbf{R})$的子群. 请读者证明这一结论.

定理 6.2.1 G 是一个群, 它的非空子集 H, 则下列条件等价:

1) H 是 G 的子群

2) $1\in H$; $a\in H$, 则$a^{-1}\in H$; $a,b\in H$, 则 $ab\in H$;

3) $a,b\in H$, 则 $ab\in H$, $a^{-1}\in H$;

4) $\forall a,b\in H,\ ab^{-1}\in H$.

证明 1)⇒2). 由 H 对 G 的乘法构成群可知, $a,b\in H$ 则 $ab\in H$. 又 H 有幺元$1'$, 即有 $1'\cdot 1'=1'$. 设$1'$在 G 中的逆元为$1'^{-1}$, 则有

$$1=1'\cdot 1'^{-1}=(1'\cdot 1')\cdot 1'^{-1}=1',$$

故 $1\in H$. 设 a 在 H 中的逆元是a'，于是 $aa'=1'=1$，即$a'=a^{-1}$，故$a^{-1}\in H$. 由此可知 2)成立，而且 H 的幺元是 G 的幺元，且 H 中的逆元与 G 中的逆元一致.

2)⇒3). 显然.

3)⇒4). 若 $a,b\in H$，故 $a,b^{-1}\in H$，进而 $ab^{-1}\in H$.

4)⇒1). 由 H 非空，$\exists a\in H$，因而 $1=aa^{-1}\in H$. 又由 $1,a\in H$ 得$a^{-1}=1a^{-1}\in H$. 又若 $a,b\in H$，由$b^{-1}\in H$ 得 $ab=a(b^{-1})^{-1}\in H$. 由此可知 G 的乘法也是 H 的乘法. 对于 H 而言有幺元 1；对于 $a\in H$ 有逆元；结合律显然成立，故 H 是 G 的子群.

上述定理可以用于子群的判别.

例 6.2.5 在普通加法下，偶数集合是 $\mathbf{Z}$ 的子群；所有 3 的倍数组成的集合是 $\mathbf{Z}$ 的子群；更一般的，对固定的整数 n，所有 n 的倍数组成的集合是 $\mathbf{Z}$ 的子群. 命题正式陈述如下：

设 $n\in\mathbf{Z}$，令 $n\mathbf{Z}=\{n\times k\mid k\in\mathbf{Z}\}$，则$(n\mathbf{Z},+)$是$(\mathbf{Z},+)$的子群.

证明 显然 $n\mathbf{Z}$ 是 $\mathbf{Z}$ 的一个非空子集，且$\forall a,b\in n\mathbf{Z}$，存在 $i,j\in\mathbf{Z}$ 使得

$$a=n\times i,\quad b=n\times j,$$

因此

$$a-b=n\times i-n\times j=n\times(i-j)\in n\mathbf{Z}.$$

由“子群判别标准”知$(n\mathbf{Z},+)$是$(\mathbf{Z},+)$的子群.

定理 6.2.2 G 是一个有限群，它的非空子集 H 是子群当且仅当子集 H 在 G 的二元运算下是封闭的.

证明 先证必要性. 由子群的定义即可得.

再证充分性. 子集 H 非空，所以存在 $x\in H$，由于子集 H 在 G 的二元运算下是封闭的，所以对任意正整数次幂有 $x^n\in H$. 因为 G 是一个有限群，所以 x 的阶必然有限，即存在正整数 m，使得 $x^m=1$，所以 $1\in H$. $\forall y\in H$，由于 y 的阶必然有限，即存在正整数 k，使得 $y^k=1$，所以由逆元的定义可知，$y^{k-1}=y^{-1}$，因为 $y^{k-1}\in H$，所以 $y^{-1}\in H$. 因此，我们看到 H 满足子群的定义中的所有三个条件.

上面定理中，如果允许 G 是一个无限群，那么结论不一定成立.

例 6.2.6 在普通加法下，$\mathbf{Z}$ 是一个无限群，考虑自然数集合 $\mathbf{N}$，非空且在普通加法下封闭，但是 $\mathbf{N}$ 不是 $\mathbf{Z}$ 的子群.

定义 6.2.2 设两个群满足 $K\leqslant G$，如果对任意 $k\in K$ 和 $g\in G$ 都有 $gkg^{-1}\in K$，则我们称 K 为 G 的**正规子群**，记为 $\boldsymbol{K\lhd G}$.

定理 6.2.3 任意交换群 G 的每个子群 K 都是正规子群.

证明 对任意 $g\in G$，$k\in K$，我们有

$$gkg^{-1}=kgg^{-1}=ke=k,$$

所以 $gkg^{-1}\in K$，由正规子群的定义知 $K\lhd G$. 证毕.

例 6.2.7 设 $n>1$ 是整数，则$(n\mathbf{Z},+)$是$(\mathbf{Z},+)$的正规子群. 因为对任意 $g\in\mathbf{Z}$，$k\in n\mathbf{Z}$，由“+”运算满足交换律，所以我们有，

$$g+k-g=k\in n\mathbf{Z},$$

所以 $n\mathbf{Z}$ 是 $\mathbf{Z}$ 的一个正规子群. 注意，$(n\mathbf{Z},+)=(\langle n\rangle,+)$.

例 6.2.8 $SL(n,\mathbf{R})$为 $GL(n,\mathbf{R})$的正规子群. 请读者证明这一结论.

定理 6.2.4 设群 H 是群 G 的子群，则下列条件等价：

(1) $H\lhd G$；

(2) 对任意 $g\in G$，$gHg^{-1}=H$；

(3) 对任意 $g\in G$，$gH=Hg$；

(4) 对任意 $g_1, g_2 \in G$， $g_1 H g_2 H = g_1 g_2 H$.

证明 (1)$\Rightarrow$(2) 对任意 $g \in G$ 和 $h \in H$，则由 $H \lhd G$ 有 $gHg^{-1} \in H$，又 $h = g^{-1}(gHg^{-1})g \in gHg^{-1}$ 故 $gHg^{-1} = H$；

(2)$\Rightarrow$(3) 对任意 $g \in G$ 和 $h \in H$，有 $gh = ghg^{-1}g \in Hg$， $hg = gg^{-1}hg \in gH$，故 $gH = Hg$；

(3)$\Rightarrow$(4) 对 $g_1, g_2 \in G$ 以及 $h, h_1, h_2 \in H$，由(3)有存在 $h', h_1' \in H$ 使得 $h_1 g_2 = g_2 h_1'$，$g_2 h = h' g_2$. 于是 $g_1 h_1 g_2 h_2 = g_1 g_2' h_1 h_2$ g_1， $g_1 g_2 h = g_1 h' g_2 \cdot 1 \in g_1 H \cdot g_2 H$，故 $g_1 H g_2 H = g_1 g_2 H$；

(4)$\Rightarrow$(1) 对任意 $g \in G$ 和 $h \in H$，有 $ghg^{-1} \in gHg^{-1}H = gg^{-1}H = H$，则 $H \lhd G$.

习题 6.2

A 组

1. 设$(G, \bullet)$是一个群, H 是 G 的一个有限子集, 证明$(H, \bullet)$构成$(G, \bullet)$的子群的充要条件是：对任意 $a, b \in H$ 有 $a \bullet b \in H$. .
2. 设 H 是 $\mathbf{Z}$ 的子群, 则存在整数 n 使得 $H = n\mathbf{Z}$.
3. 证明群 G 不能写为两个真子群的并.

B 组

4. 定义 $SO_n(\mathbf{R}) = \{A \in GL_n(\mathbf{R}) \mid AA^T = I_n, \det(A) = 1\}$，证明 $SO_n(\mathbf{R})$ 是 $GL_n(\mathbf{R})$ 的子群.
5. 设 H, K 是群 G 的两个正规子群, 且 $H \cap K = \{1\}$, 求证: $hk = kh$, $\forall h \in H, k \in K$.
6. 对于群$(G, \bullet)$和其中幺元 e，定义其中的**扭元**为满足存在 $n \in \mathbf{Z}^+, g^n = e$ 的元素 g，定义纽元集合为 $G_{tor} = \{g \in G \mid \exists n \in \mathbf{Z}^+, g^n = e\}$，证明： G_{tor} 是 G 的正规子群.

6.3 循环群

循环群，作为一类特殊的群，具有特殊的代数结构. 循环群广泛存在于代数、数论中, 在编码、密码学中也有重要的应用. 我们下面来介绍这一类群.

定义 6.3.1 G 是一个群，且 $a \in G$，令集合

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

则我们称集合$\langle a \rangle$为**由元素 a 生成的 G 的循环子群**.

定理 6.3.1 $\langle a \rangle$是一个群，且是 G 的子群.

证明 由循环子群的定义可知, $1 = a^0 \in \langle a \rangle$; $(a^n)^{-1} = a^{-n} \in \langle a \rangle$; $a^n a^m = a^{n+m} \in \langle a \rangle$且结合律

显然成立，满足群的定义中的条件，所以$<a>$是一个群．又由于$<a>$显然是 G 的子集，所以$<a>$是 G 的子群．

定义 6.3.2　G 是一个群，如果存在 $a\in G$ 使得，

$$G=<a>,$$

则我们称 G 为**循环群**，而且称 a 为 G 的**生成元**．

由前面的定义和定理显然可知任何群的循环子群必定是循环群．另外，一个循环群可以有不只一个生成元，例如，如果集合

$$G=<a>=\{a^n \mid n\in \mathbf{Z}\},$$

则因为

$$\{a^n \mid n\in \mathbf{Z}\}=\{(a^{-1})^n \mid n\in \mathbf{Z}\}=<a^{-1}>,$$

所以有 $G=<a^{-1}>$.

例 6.3.1　$(\mathbf{Z},+)$是交换群，任取 $a\in\mathbf{Z}$，则$<a>=\{n\times a \mid n\in\mathbf{Z}\}$，则$(<a>,+)$是$(\mathbf{Z},+)$的循环子群．当 $a=0$ 时，这个子群仅由一个元素 0 组成；当 $a=1$ 时$<1>=\mathbf{Z}$，所以$(\mathbf{Z},+)$是循环群，1 是$\mathbf{Z}$的生成元．当然也有当 $a=-1$ 时$<-1>=\mathbf{Z}$，所以-1 也是$\mathbf{Z}$的生成元．当 $a=2$ 或者-2 时$<2>=<-2>=$ 偶数集合，所以 2 和-2 都是偶数集合的生成元．注意，奇数集合不是 $\mathbf{Z}$ 的循环子群，其实奇数集合根本不是群，因为不含单位元 1.

例 6.3.2　集合$\mathbf{Z}_6=\{0,1,\ldots,5\}$，1 是$\mathbf{Z}_6$的生成元，另一个明显的生成元是 5．它的子集$\{0,3\}$是一个循环子群，该子群的生成元只有一个是 3．它的另一个子集$\{0,2,4\}$也是一个循环子群，该子群的生成元是 2 和 4.

例 6.3.3　集合$\mathbf{Z}_5^*=\{1,2,\ldots,4\}$，即从$\mathbf{Z}_5$里去掉元素 0，则 2 和 3 是它的生成元．该集合的子集$\{1,4\}$是$(\mathbf{Z}_5^*,\cdot)$的一个循环子群，生成元是 4．我们可以举出很多这样的例子，详细内容，读者可以参考前面数论中有关原根的部分.

定理 6.3.2　如果 $G=<a>$是一个循环群，且$|G|=n$，则当且仅当$(k,n)=1$ 时，a^k 是 G 的生成元.

证明　先证必要性．如果 a^k 是 G 的生成元，则 $a\in<a^k>$，即存在整数 s，使得$(a^k)^s=a$．两边同时乘以 a^{-1} 得到 $a^{ks-1}=1$．由定理 6.1.4 可知，$n\mid ks-1$，即存在整数 t 使得 $tn=ks-1$，所以 $tn=ks-1$，就是 $ks-tn=1$，由之前数论的相关结论可知$(k,n)=1$.

再证充分性．如果$(k,n)=1$，则存在整数 s 和 t，使得 $ks+tn=1$．则 $a=a^{ks+tn}=a^{ks}(a^n)^t=a^{ks}(1)^t=a^{ks}$，所以 $a\in<a^k>$，因此 $G=<a>\le<a^k>$，但是由于明显有$<a^k>\le G$，所以 $G=<a^k>$，即 a^k 是 G 的生成元.

我们马上可以得到如下的推论.

推论　n 阶循环群共有 $\varphi(n)$ 个生成元.

例 6.3.4　考虑集合$\mathbf{Z}_{12}=\{0,1,\cdots,11\}$，注意到$\varphi(12)=4$，所以共有 4 个生成元，最明显的一个是 1．与 12 互素的 4 个 k 为 1, 5, 7, 11．所以其他 3 个生成元为 5, 7, 11.

定理 6.3.3　如果 $G=<a>$是一个循环群，且 $S\le G$，则 S 必定是循环群，且如果 k 是使得 $a^k\in S$ 的最小正整数，则 a^k 是 S 的生成元.

证明　当 $S=\{1\}$时，命题显然成立．下面设 $S\ne\{1\}$．因为 $G=<a>$且 $S\le G$，所以 S 中的元素必然是 a 的幂．如果 $a^k\in S$，那么由于 S 是群，则 $a^{-k}\in S$，因此 S 中必然存在 a 的正整数次幂．设 k 是使得 $a^k\in S$ 的最小正整数，则对任意 $a^m\in S$，因为 $m=tk+r$，其中 $0\le r<k$，则因为 S 是群，所以 $a^{-k}\in S$，所以 $a^r=a^m(a^{-k})^t$，所以 $a^r\in S$，注意到 r 是非负数和 k 是使得 $a^k\in S$ 的最小正整数，我们可知 $r=0$，即 $k\mid m$，由 a^m 的任意性可知 S 中的元素都是 a^k 的幂，且由 S 是群，可知 a^k 的任意幂都在 S 中，所以

$$S=\{(a^k)^n \mid n\in \mathbf{Z}\},$$

即 S 必定是循环群，它的生成元是 a^k.

定理 6.3.4 G 是有限群，且 $a\in G$，则 $\mathrm{ord}(a)=|\langle a\rangle|$.

证明 因为 G 是有限群，所以 $\mathrm{ord}(a)$一定为有限数．令 $k=\mathrm{ord}(a)$，则 1，a，a^2，$\cdots$，a^{k-1} 这 k 个元素必然互不相同．因为，假设存在重复，既存在 $0\leqslant i<j\leqslant k-1$ 使得 $a^i=a^j$，则 $a^{j-i}=1$，其中 $j-i$ 显然是小于 k 的正整数，这与 $k=\mathrm{ord}(a)$的“最小”性质矛盾.

如果令集合 $H=\{1,a,a^2,\cdots,a^{k-1}\}$，则$|H|=k$. 很明显，$H\subseteq\langle a\rangle$. 对任意 $a^i\in\langle a\rangle$，由带余除法得到 $i=qk+r$，其中 $0\leqslant r<k$，则 $a^i=a^{qk+r}=a^{qk}a^r=(a^k)^q a^r=a^r\in H$，所以$\langle a\rangle\subseteq H$，所以$\langle a\rangle=H$. 所以$|\langle a\rangle|=|H|=k=\mathrm{ord}(a)$.

定理 6.3.5 $G=\langle a\rangle$是有限循环群，且$|G|=n$，则对任意整除 n 的正整数 d，一定存在一个唯一的阶为 d 的循环子群，该循环子群为$\langle a^{n/d}\rangle$.

证明 因$(a^{n/d})^d=a^n=1$，所以 $\mathrm{ord}(a^{n/d})\mid d$. 又因为$(a^{n/d})^{\mathrm{ord}(a^{n/d})}=1$，故 $n\mid(n/d)\mathrm{ord}(a^{n/d})$，所以必然有 $\mathrm{ord}(a^{n/d})/d$ 为整数，即 $d\mid\mathrm{ord}(a^{n/d})$．因此 $d=\mathrm{ord}(a^{n/d})$．由定理 6.3.4 可知

$$|\langle a^{n/d}\rangle|=\mathrm{ord}(a^{n/d})=d,$$

即存在性得证.

下面证明唯一性．令 H 是 G 的一个阶为 d 的循环子群，则 H 必然是循环子群，当然可以写成如下形式 $H=\langle x\rangle$．因为 $x\in G$，所以必然存在整数 m 使得 $x=a^m$，所以$(a^m)^d=1$，所以 $n\mid md$，所以存在整数 k 使得 $md=nk$. 因此，$x=(a^{n/d})^k$，所以 $H=\langle x\rangle\subseteq\langle a^{n/d}\rangle$，由于这两个子群的阶相同，所以必然有 $H=\langle a^{n/d}\rangle$.

接下来我们讨论由给定的子群构造新的子群的问题.

定理 6.3.6 $(G,\bullet)$是群，$\{(H_i,\bullet)\mid i\in I\}$是$(G,\bullet)$的一族子群，其中 I 是某个指标集合，则$(\cap_{i\in I}H_i,\bullet)$是$(G,\bullet)$的一个子群．也就是说，子群的交集还是子群.

证明 对任意 $i\in I$，因为 H_i 是子群，所以 $1\in H_i$，所以 $1\in\cap_{i\in I}H_i$，即$\cap_{i\in I}H_i\neq\varnothing$；对任意 $a,b\in\cap_{i\in I}H_i$，都有 $a,b\in H_i$ $(i\in I)$，即 a,b 属于这一族子群中的每一个子群，由定理 6.2.1 知 $a\bullet b^{-1}\in H_i(i\in I)$. 所以有 $a\bullet b^{-1}\in\cap_{i\in I}H_i$．由定理 6.2.1 知$(\cap_{i\in I}H_i,\bullet)$是$(G,\bullet)$的一个子群．证毕.

设$(G,\bullet)$为群，S 是 G 的子集，则 S 对运算“$\bullet$”不一定封闭，即使 S 对运算“$\bullet$”封闭，S 也不一定是 G 的子群，那么给定子集 S 时，我们如何由 S 得到一个子群呢？

定义 6.3.3 设$(G,\bullet)$为群，S 是 G 的子集，设$(H_i\mid i\in I,\bullet)$是$(G,\bullet)$的所有包含集合 S 的子群，即 $S\subseteq H_i(i\in I)$，则$(\cap_{i\in I}H_i,\bullet)$叫作**由集合 S 生成的子群**，记为$(\langle S\rangle,\bullet)$，$S$ 中的元素叫子群$(\langle S\rangle,\bullet)$的**生成元**.

容易证明，

$$\langle S\rangle=\{b_{k_1}\square b_{k_2}\square\cdots\square b_{k_r}\mid b_{k_j}\in S\text{ 或 }b_{k_j}^{-1}\in S,j=1,\cdots,r,r\in\mathbf{N}\}.$$

特别是当 S 由一个元素 a 组成时，

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

当$(X,\bullet)$为交换群，且 S 由有限个元素 $a_1,a_2,\cdots,a_m$ 组成时，

$$\langle S\rangle=\langle a_1,a_2,\cdots,a_m\rangle=\{a_1^{n_1}\bullet\cdots\bullet a_m^{n_m}\mid n_1,\cdots,n_m\in\mathbf{Z}\}.$$

例 6.3.5 $(G,\bullet)$为群，$S=\varnothing$ 是 G 的子集，求$\langle\varnothing\rangle$.

解 因为$\varnothing$包含于 G 的任意子群 H，所以$\langle\varnothing\rangle$是 G 的所有子群的交集，而$\{1\}$是一个子群且包含于 G 的任意子群 H，所以 G 的所有子群的交集就是$\{1\}$，从而$\langle\varnothing\rangle=\{1\}$.

例 6.3.6 循环群 $G=\langle a\rangle$是由子集$\{\ a\ \}$生成的，我们在书写时使用记号$\langle a\rangle$，而不使用记号$\langle\{\ a\ \}\rangle$.

定义 6.3.4 设$(G,\ \bullet)$为群，如果存在 G 的子集 S，使得 $G=\langle S\rangle$，且对 S 的任一真子集 S'，必有 $G\neq\langle S'\rangle$，那么 S 称为群$(G,\ \bullet)$的**极小生成集**，也称为群$(G,\ \bullet)$的一组**基**. 当 S 是有限集时就说$(G,\ \bullet)$是**有限生成群**.

例 6.3.7 对任一$a\in\mathbf{Z}$，令$\langle a\rangle=\{n\times a\mid n\in\mathbf{Z}\}$，我们知道$(\langle a\rangle,+)$是$(\mathbf{Z},+)$的子群. 当$a=1$时$\langle 1\rangle=\mathbf{Z}$，所以$(\mathbf{Z},+)$是循环群，1 是它的生成元. 此外，$\{2,3\}$是它的一个极小生成集，即$\mathbf{Z}=\langle 1\rangle=\langle\{2,3\}\rangle$，且明显$\mathbf{Z}\neq\langle 2\rangle$=偶数集合以及$\mathbf{Z}\neq\langle 3\rangle=3$ 的倍数集合. 参见如下定理.

定理 6.3.7 设$a,b\in\mathbf{Z}$，$A=\langle a\rangle$，$B=\langle b\rangle$，$C=\{\ sa+tb\mid s,t\in\mathbf{Z}\ \}$，则

(1) $C=\langle d\rangle$，其中 $d=(a,\ b)$；

(2) $A\cap B=\langle m\rangle$，其中 $m=[a,\ b]$.

证明 (1) 由集合 C 的元素的形式，我们易知 C 是 $\mathbf{Z}$ 的子群，且 $C=\langle\{\ a,\ b\ \}\rangle$. 由于 $\mathbf{Z}$ 是循环群，所以根据定理 6.3.3 可知，它的子群 C 也是循环群，即存在某个正整数 d，使得 $C=\langle d\rangle$，其中 $d=C$ 中的最小正整数. 因为(a,b)是 a,b 的线性组合，所以$(a,b)\in C$，且其他 C 中的元素因为都是 a,b 的线性组合，所以必然都是$(a,\ b)$的倍数，因此(a,b)是 C 中的最小正整数. 所以 $d=(a,\ b)$，即 $C=\langle(a,\ b)\rangle$.

(2) 因为 A 中的元素一定是 a 的倍数且 B 中的元素一定是 b 的倍数，所以 $A\cap B$ 中的元素一定是 a 和 b 的公倍数. 反过来，a 和 b 的任意公倍数一定属于 $A\cap B$. 因为 A 和 B 都是 $\mathbf{Z}$ 的子群，所以由定理 6.3.6 可知，$A\cap B$ 也一定是 $\mathbf{Z}$ 的子群，又由于 $\mathbf{Z}$ 是循环群，所以根据定理 6.3.3 可知，$A\cap B$ 也是循环群，即存在某个正整数 m，使得 $A\cap B=\langle m\rangle$，其中 $m=A\cap B$ 中的最小正整数. 显然，$A\cap B$ 中的最小正整数为$[a,\ b]$，所以 $A\cap B=\langle[a,\ b]\rangle$.

习题 6.3

A 组

1. 证明群中元素与其逆元具有相同的阶.
2. 有限群$(G,\bullet)$中的任何元素 a 的阶可整除$|G|$.
3. p 是素数,证明$(\mathbf{Z}_p,+)$有 p-1 个生成元.

B 组

4. n 是任意整数素数,试通过其标准分解式,给出$(\mathbf{Z}_p,+)$所有生成元,并求出其个数.
5. n 是正整数,试求出$(\mathbf{Z}_p,+)$的所有生成元.
6. 群 G 只有有限个子群,证明 G 为有限群.
7. 设 G 是 Abel 群, H,K 是其子群, 阶分别为 r , s, 试证：

   (1) 若$(r\ ,\ s)=1$, 则 G 有阶为 rs 的循环子群;

   (2) G 包含一个阶为 gcd$(r\ ,\ s)$的循环子群.

6.4 置换群

置换群是一类重要的群，它们的元素是置换作用．在后面的伽罗瓦理论中，我们将看到置换群的重要应用．此外，置换群在几何学、编码理论中也有重要的应用．实际上密码学上任何分组加密方法都可以看作将所有可能的明文进行置换得到所有可能的密文．置换群不仅被人们看作一种需要加以深入研究的群，而且置换群还是最能说明群的各种概念的例子．本节对置换群进行简要的讨论．

定义 6.4.1 给定非空集合 X，我们将任意一个双射 $\alpha: X\to X$ 称作集合 X 的一个**置换**.

由上面的定义可知，置换实际上就是双射函数，如果我们把函数的复合“∘”看作一种置换间的二元运算，那么由非空集合 X 的所有置换组成的集合就是一个群，我们将这个群用符号记为$(S_X, \circ)$，因为

(1) 封闭性：任意选择两个置换 $\alpha: X\to X$ 和 $\beta: X\to X$，因为它们都是双射，所以复合函数 $\alpha\circ\beta: X\to X$ 也是双射，即置换，因此“∘”是 S_X 上的（封闭的）二元运算；

(2) 结合律：由于一般的函数的复合是满足结合性质的，所以“∘”满足结合律；

(3) 单位元：我们定义恒等置换 $1_X: X\to X$ 为，对任意 $x\in X$，$1_X(x)=x$，则对任意置换 α，

$$\alpha\circ 1_X = 1_X\circ\alpha=\alpha,$$

所以 1_X 是单位元;

(4) 逆元：对任意置换 $\alpha: X\to X$，因为是双射，所以存在双射的逆函数 $\alpha^{-1}: X\to X$，满足

$$\alpha\circ\alpha^{-1}=\alpha^{-1}\circ\alpha=1_X,$$

所以置换 α^{-1} 是 α 的逆元.

综上所述，$(S_X, \circ)$满足所有的群条件，所以的确是一个群.

定义 6.4.2 我们将上述的群$(S_X, \circ)$称为集合 X 上的**全变换群**或**对称群**．当 $X=\{1, 2, \cdots, n\}$ 时，我们称 S_X 为 ***n* 次全变换群(对称群)**，记作 S_n.

我们可以用如下的两行记号来表达 S_n 中的置换 α:

$$\alpha=\begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{pmatrix}$$

例 6.4.1 考虑 S_n 的一个重要子群 A_n，首先考虑 n 个变量的多项式

$$A=\prod_{1\le i<j\le n}(x_i-x_j)$$

对于 $\alpha\in S_n$，令

$$A_\alpha=\prod_{1\le i<j\le n}(x_{\alpha(i)}-x_{\alpha(j)})$$

我们先说明$A_\alpha=\pm A$，注意到A中没有重因式，现需说明A_α中仍然没有重因式．设有$\{\alpha(i),\alpha(j)\}=\{\alpha(k),\alpha(l)\}$，则有如下两种可能：

1) $\alpha(i)=\alpha(k),\alpha(j)=\alpha(l)$，则有 $i=k, j=l$

2) $\alpha(i)=\alpha(l),\alpha(j)=\alpha(k)$，则有 $i=l, j=k$

因而有$\{i,j\}==\{k,l\}$，故$A_\alpha=\pm A$.

若$A_\alpha=A$，则称A_α为偶置换，并记$sgn(\alpha)$=1；若$A_\alpha=-A$，则称A_α为奇置换，记$sgn(\alpha)$= -1，称$sgn(\alpha)$为 α 的符号，故有A_α=$sgn(\alpha)A$.

令 A_n 为 S_n 的所有偶置换的集合，即$A_n=\{\alpha\in S_n|sgn(\alpha)=1\}$

则可以证明A_n是 S_n 的子群，并称之为 ***n* 次交错群.**

利用排列组合的知识我们很容易得到 S_n 的元素数量是 $n!$. 下面我们讨论如何用另一种方式表达这么多的置换.

定义 6.4.3 设 $\alpha\in S_n$，$A=\{i_1, i_2, \cdots, i_r\}\subseteq\{1, 2, \cdots, n\}$，$B=\{1, 2, \cdots, n\}-A$，如果置换 α 满足，

(1) 对 A 中的元素有 $\alpha(i_1)=i_2$，$\alpha(i_2)=i_3, \cdots, \alpha(i_{r-1})=i_r$，$\alpha(i_r)=i_1$；

(2) 对任意 $i\in B$ 有，$\alpha(i)=i$；

则我们称置换 α 为一个 ***r* −轮换**，记为 $\alpha=(i_1, i_2, \cdots, i_r)$. 我们也把 2−轮换称为**对换**.

例 6.4.2 一个 3−轮换为 $\alpha=(2, 1, 3)\in S_5$，它的意思就是 $\alpha(1)=3$，$\alpha(2)=1$，$\alpha(3)=2$，$\alpha(4)=4$，$\alpha(5)=5$.

例 6.4.3 有如下的置换之间的等式

$$\begin{pmatrix}1&2&3&4&5\\5&1&4&2&3\end{pmatrix}=\begin{pmatrix}1&5&3&4&2\end{pmatrix}$$

$$\begin{pmatrix}1&2&3&4&5\\2&3&1&4&5\end{pmatrix}=\begin{pmatrix}1&2&3\end{pmatrix}$$

我们能够将任意置换分解为多个轮换的乘积（从现在开始，我们用“乘积”来称呼置换之间的复合，且在用符号表示两个置换复合的时候，省略“。”），我们将此称为置换的轮换分解.

例 6.4.4 如下的置换 $\alpha\in S_5$ 可以用两种不同的轮换的乘积进行表示

$$\alpha=(1\quad 2)\,(1\quad 3\quad 4\quad 2\quad 5)\,(2\quad 5\quad 1\quad 3)=(1\quad 4)\,(3\quad 5)\,(2).$$

观察例 6.4.4，我们看到尽管该置换可以用两种不同的轮换的乘积进行表示，但是显然第二种方式更简洁明了，因此，引入如下的概念.

定义 6.4.4 设 $\alpha, \beta\in S_n$ 是两个轮换，且这两个轮换的记号中没有共同的数字，则我们称 α 和 β **不相交**. 如果一组轮换中任意两个轮换都不相交，则我们称该组轮换**不相交**.

例 6.4.5 如下的置换 $\alpha\in S_5$ 是 3 个不相交的轮换的乘积

$$\alpha=(1\quad 4)\,(3\quad 5)\,(2).$$

由于 1−轮换都等于恒等置换，所以下面的讨论中一律不再写出 1−轮换，对于恒等置换，写作 1_n. 例如：上例中的置换写作如下的轮换分解

$$\alpha=(1\quad 4)\,(3\quad 5).$$

对于任意 $\alpha\in S_n$，如果已知它的轮换分解，那么求出它的逆置换的方法为：将它的轮换分解中的每一个轮换中的数字倒排即可.

另外，由于 S_2 只有两个元素，明显是一个交换群. 我们注意对于 $n\geq 3$，S_n 是非交换群.

例 6.4.6 对于任意 $S_n(n\geq 3)$都有

$$(1\quad 2)\,(1\quad 3)=(1\quad 3\quad 2)$$

和

$$(1\quad 3)\,(1\quad 2)=(1\quad 2\quad 3),$$

所以

$$(1\quad 2)\,(1\quad 3)\neq(1\quad 3)\,(1\quad 2).$$

尽管，对于 $n\geq 3$，S_n 是非交换群，然而，其中的很多元素是可交换的，特别是，不相交的轮换是可交换的.

定理 6.4.1 不相交的轮换是可交换的.

证明 因为轮换只针对自身记号内的数字进行换位，而对自身记号外的数字的作用只是固定该值，所以两个不相交的轮换在执行上不论谁先谁后，总体效果是一样的，即不相交的轮换是可交换的.

因此对一个置换的不相交轮换分解来说，随意调整其中各轮换的次序不会改变该置换.

例 6.4.7 (1 4)、(3 5)和(2 6)是 3 个不相交的 2−轮换，因此有

$$(1\ \ 4)\,(3\ \ 5)\,(2\ \ 6)=(3\ \ 5)\,(1\ \ 4)\,(2\ \ 6)=(2\ \ 6)\,(3\ \ 5)\,(1\ \ 4).$$

注意，实际上，一个轮换有不同的记号方式，即：将表示该轮换的记号中的数字进行循环换位，则不会改变该轮换(但是，习惯上我们一般将轮换中最小的数写在第一个位置).

例 6.4.8 $(1\ \ 2\ \ 3)=(2\ \ 3\ \ 1)=(3\ \ 1\ \ 2)$. 其中，我们一般采用(1 2 3)这个记号.

如果我们遵守以下的规定，我们将不加证明地给出重要的定理 6.4.2：

(1) 对一个置换的不相交轮换分解，随意调整其中各轮换的次序，我们把这些不同的记法看作同一个轮换分解；

(2) 我们把一个轮换的不同的记号方式看作同一个轮换.

(3) 对一个置换的不相交轮换分解，一定去掉任何 1−轮换.

定理 6.4.2 S_n 中的任意置换一定能够分解为不相交轮换的乘积，且这种分解是唯一的.

下面讨论置换的阶.

一个 r−轮换 $\alpha=(i_1,\ i_2,\cdots,\ i_r)$的 k 次幂 α^k 就是连续施行 k 次该 r−轮换 α，当 $k\leq r-1$ 时，$\alpha^k(i_1)=i_{1+k}\neq i_1$，所以 $\alpha^k\neq 1_n$；当 $k=r$ 时，对任意 m 有，$\alpha^k(i_m)=i_m$，所以 $\alpha^k=1_n$. 综上所述可知，$\mathrm{ord}(\alpha)=r$. 对任意置换来说，为了求得它的阶，则我们首先将该置换进行不相交的轮换分解，那么该置换的阶就等于所有轮换因子的长度的最小公倍数.

例 6.4.9 观察 3−轮换$(1\ \ 2\ \ 3)\in S_3$,

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

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

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

所以，(1 2 3)的阶是 3.

例 6.4.10 求 $\alpha=(1\ \ 2\ \ 3)\,(4\ \ 5)\in S_5$ 的阶.

解 $\mathrm{ord}(\alpha)=[3,2]=6$.

定义 6.4.5 我们将任意全变换群的任意子群称为一个**置换群**.

例 6.4.11 S_4 的子集 $V=\{(1),\ (1\ \ 2)\,(3\ \ 4),\ (1\ \ 3)\,(2\ \ 4),\ (1\ \ 4)\,(2\ \ 3)\}$是一个子群，即 V 是一个置换群.

证明　恒等置换(1)∈S_4；对任意 $\alpha\in V$ 有 $\alpha^2=(1)$，所以 $\alpha^{-1}=\alpha\in V$. 另外,

$$[(1\ \ 2)(3\ \ 4)][(1\ \ 3)(2\ \ 4)]=[(1\ \ 3)(2\ \ 4)][(1\ \ 2)(3\ \ 4)]=(1\ \ 4)(2\ \ 3),$$

$$[(1\ \ 2)(3\ \ 4)][(1\ \ 4)(2\ \ 3)]=[(1\ \ 4)(2\ \ 3)][(1\ \ 2)(3\ \ 4)]=(1\ \ 3)(2\ \ 4),$$

$$[(1\ \ 3)(2\ \ 4)][(1\ \ 4)(2\ \ 3)]=[(1\ \ 4)(2\ \ 3)][(1\ \ 3)(2\ \ 4)]=(1\ \ 2)(3\ \ 4),$$

即运算在 V 上封闭，所以 V 是一个 S_4 的子群，因此 V 是一个置换群. 注意到，在 6.6 节介绍了同构的概念后，我们将发现这里的 V 与例 6.1.7 中的群是同构的.

习题 6.4

A 组

1. 将置换 $\begin{pmatrix}1&2&3&4&5&6&7&8\\2&5&6&8&1&4&7&3\end{pmatrix}$ 分解成不相交的轮换.

2. 将置换之积 $\begin{pmatrix}1&2&3&4&5&6&7&8\\2&5&6&8&1&4&7&3\end{pmatrix}\circ\begin{pmatrix}1&2&3&4&5&6&7&8\\2&5&6&4&1&8&7&3\end{pmatrix}$ 分解成不相交的轮换.

3. 试确定 S_5 中的元素 $\sigma\tau,\sigma^{-1}\tau\sigma,\sigma^2,\sigma^3$ 其中 $\sigma=\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix},\tau=\begin{pmatrix}1&2&3&4&5\\3&4&1&5&2\end{pmatrix}$.

B 组

4. 证明n次交错群A_n是 S_n 的子群.

6.5 陪集与商群

群和它的子群之间有一定的紧密的关系，本节我们详细介绍这种重要的关系. 这就是本小节拉格朗日定理所揭示的内容.

定义 6.5.1　$(G,\cdot)$为群，$H\leqslant G$，$a\in G$，我们用符号 aH 表示如下的 G 的子集

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

并且称这样的子集为子群 H 的**左陪集**.

明显，$a=a\cdot 1\in aH$. 如果 $a\notin H$，那么 $1\notin aH$，否则存在 $h\in H$，使得 $1=ah$，即 $a=h^{-1}\in H$，导出矛盾，这说明当 $a\notin H$ 时，左陪集 aH 不是群.

注意，如果我们对群上的二元运算采用“+”记号，则左陪集应该如下表示：

$$a+H=\{a+h\mid h\in H\}.$$

例 6.5.1　令<3>=$\{n\times 3\mid n\in \mathbf{Z}\}$，我们知道(<3>, +)是($\mathbf{Z}$, +)的子群，求出<3>的所有左陪集.

解　令 $a=0$，则相应的左陪集为$A=\{0+n\times 3\mid n\in \mathbf{Z}\}=\{k\mid k\equiv 0\ (\mathrm{mod}\ 3)\}$；若令 $a=1$，则相应的左陪集为 $B=\{1+n\times 3\mid n\in \mathbf{Z}\}=\{k\mid k\equiv 1(\mathrm{mod}3)\}$；若令 $a=2$，则相应的左陪集为 $C=\{2+n\times 3\mid n\in \mathbf{Z}\}=\{k\mid k\equiv 2(\mathrm{mod}\ 3)\}$；当然，我们还可以令 a 取其他数值，然后求相应的左

陪集，经过计算不难发现，当$a \equiv 0 (\mathrm{mod}\ 3)$时，得到的左陪集就是$A$；当$a \equiv 1 (\mathrm{mod}\ 3)$时，得到的左陪集就是$B$；当$a \equiv 2 (\mathrm{mod}\ 3)$时，得到的左陪集就是$C$. 因此所有三个左陪集是仅有的解.

例 6.5.2 考虑向量空间$\mathbf{R}^2$，若定义加法为$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$，则过原点的一条直线是它的子空间，因此必然是它的子群，那么任何一条与该直线平行的直线都是它的陪集.

另一方面，我们来研究利用群$(G, \bullet)$的一个子群$(H, \bullet)$来对G进行分类的问题，为了说明这一点，我们先看一个例子.

对于群$(\mathbf{Z}, +)$，可以利用模3同余关系（注意同余关系是等价关系）将$\mathbf{Z}$划分成三个剩余类C_0, C_1, C_2. 我们尝试用另一种方法来表达这种同余关系：令$\langle 3\rangle = \{n \times 3 | n \in \mathbf{Z}\}$，则$(\langle 3\rangle, +)$是$(\mathbf{Z}, +)$的子群. 再来看$\mathbf{Z}$上的模3同余关系，由同余的定义知，若$a \equiv b\ (\mathrm{mod}\ 3)$，则有$3 | (a - b)$，也有$3 | (b - a)$，也就是必存在某个整数$k$，使得$-a + b = 3 \times k$，而$3 \times k \in H$，故有$a \equiv b\ (\mathrm{mod}\ 3)$等价于$-a + b \in \langle 3\rangle$.

因此，$\mathbf{Z}$上的任两个元素a与b模3同余的充要条件是$-a + b \in \langle 3\rangle$. 而同余关系是等价关系，因此，此例中$a$与$b$等价相当于$-a + b \in \langle 3\rangle$. 故我们可以用$-a + b \in H$来确定等价关系，从而对$\mathbf{Z}$进行分类. 这样，也可以说$\mathbf{Z}$的剩余类是利用$\mathbf{Z}$的子群$\langle 3\rangle$来划分的.

我们将这种情况推广至一般的群.

定义 6.5.2 设群$(H, \bullet)$为群$(G, \bullet)$的子群，我们确定G上的一个关系≡（注意该符号与同余符号的区别），$a \equiv b$当且仅当$a^{-1} \bullet b \in H$. 这个关系叫G上关于H的**左陪集关系**.

定理 6.5.1 设群$(H, \bullet)$为群$(G, \bullet)$的子群，则G上关于H的左陪集关系≡是等价关系.

证明

(1) 自反性：因为$a^{-1} \bullet a = 1 \in H$，所以有$a \equiv a$.

(2) 传递性：设$a \equiv b, b \equiv c$，则有

$$a^{-1} \bullet b \in H, \quad b^{-1} \bullet c \in H,$$

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

故有$a \equiv c$.

(3) 对称性：若$a \equiv b$，则有$a^{-1} \bullet b \in H, (a^{-1} \bullet b)^{-1} = b^{-1} \bullet a \in H$，故有$b \equiv a$.

由于左陪集关系≡同时满足以上三个性质，所以它是等价关系.

因为左陪集关系是一个等价关系，我们可以利用左陪集关系对G进行分类.

定义 6.5.3 群$(G, \bullet)$的子群$(H, \bullet)$所确定的左陪集关系对G划分等价类，我们将下面的等价类叫作**以 a 为代表元的等价类**.

$$[a] = \{x | x \in G \text{ 且 } a \equiv x\}.$$

定理 6.5.2 设群$(H, \bullet)$为群$(G, \bullet)$的子群，则$[a] = aH$.

证明 对任意$x \in [a]$，因为$a \equiv x$，所以存在$h \in H$，使得$a^{-1} \bullet x = h$，因此$x = ah \in aH$，所以我们可以知道$[a] \subseteq aH$.

反过来，对任意$x \in aH$，存在$h \in H$，使得$x = ah$，所以$a^{-1} \bullet x = a^{-1} ah = h \in H$，即$a \equiv x$，所以$x \in [a]$，因此我们知道$aH \subseteq [a]$.

所以，$[a] = aH$. 证毕.

定理 6.5.3 设群$(H, \bullet)$为群$(G, \bullet)$的子群，$a, b \in G$，则

(1) $aH = bH$当且仅当$b^{-1} \bullet a \in H$. 特别地，$aH = H$当且仅当$a \in H$.

(2) 如果$aH \cap bH \neq \varnothing$，那么$aH = bH$.

(3) 对任意$a \in G$，$|aH| = |H|$.

证明 (1) 如果$aH = bH$，则对任意$x \in aH = bH$，存在$h, h' \in H$，使得$x = ah = bh'$，所

以 $b^{-1}\cdot a=h'\cdot h^{-1}$，因为 H 是子群，所以 $h'\cdot h^{-1}\in H$，即 $b^{-1}\cdot a\in H$.

反过来，如果 $b^{-1}\cdot a\in H$，即 $b\equiv a$，则对任意 $x\in[b]$ 有 $b\equiv x$，由≡的对称性和传递性可知，$a\equiv x$，所以 $x\in[a]$，即 $[b]\subseteq[a]$；又由≡的对称性可知，$a\equiv b$，则同理可得 $[a]\subseteq[b]$．所以 $[a]=[b]$．由定理 6.5.2 立即可知 $aH=bH$.

因为 $eH=H$，所以 $aH=H=eH$ 当且仅当 $e^{-1}\cdot a\in H$，即 $a\in H$.

(2) 如果 $aH\cap bH\neq\varnothing$，则存在 $x\in aH, bH$，那么必然存在 $h, h'\in H$，使得 $x=ah=bh'$，所以 $b^{-1}\cdot a=h'\cdot h^{-1}$，因为 H 是子群，所以 $h'\cdot h^{-1}\in H$，即 $b^{-1}\cdot a\in H$．由(1)立即可知，$aH=bH$.

(3) 令函数 $f:H\to aH$ 为 $f(h)=ah$，则很明显这是一个双射，所以 aH 和 H 等势，即 $|aH|=|H|$.

证毕.

定理 6.5.4 （**拉格朗日定理**）设群$(H,\cdot)$为有限群$(G,\cdot)$的子群，则$|H|$是$|G|$的因子.

证明 设 $a_iH(1\le i\le n)$为 H 的所有共 n 个不同的左陪集，则

$$G=a_1H\cup a_2H\cup\cdots\cup a_nH,$$

由定理 6.5.3 我们知道 $a_iH(1\le i\le n)$两两不相交，所以

$$|G|=|a_1H|+|a_2H|+\cdots+|a_nH|,$$

由定理 6.5.3 我们知道$|a_iH|=|H|(1\le i\le n)$，所以$|G|=n|H|$，即$|H|$是$|G|$的因子．证毕.

定义 6.5.4 设群$(G,\cdot)$有一个子群$(H,\cdot)$，则 H 在 G 中的两两不相交左陪集组成的集合$\{aH\mid a\in G\}$叫作 H 在 G 中的**商集**，记为 G/H；G/H 中两两不相交的左陪集的个数叫作 H 在 G 中的**指标**，记为$[G:H]$.

如果$(G,\cdot)$为有限群，其阶为$|G|$，此时$[G:H]$就是定理 6.5.4 证明中的变量 n，所以

$$|G|=[G:H]\,|H|,$$

很明显，指标$[G:H]$也是$|G|$的因子.

例 6.5.3 $(n\mathbf{Z},+)(n\in\mathbf{Z})$在整数加法群$(\mathbf{Z},+)$的中的商集为

$\mathbf{Z}/n\mathbf{Z}=\{\{a+(n\mathbf{Z})\}\mid a\in\mathbf{Z}\}=\{\{a+nh\mid h\in\mathbf{Z}\}\mid a\in\mathbf{Z}\}=\{[0],[1],\cdots,[n-1]\}$.

定理 6.5.5 设$(G,\cdot)$是有限群，且 $a\in G$，则 ord(a)是$|G|$的因子.

证明 由定理 6.3.4 可知，ord$(a)=|\langle a\rangle|$．而$\langle a\rangle$是 G 的子群，则由拉格朗日定理可知，$|\langle a\rangle|$是$|G|$的因子，即 ord(a)是$|G|$的因子.

定理 6.5.6 设$(G,\cdot)$是有限群，则对任意 $a\in G$ 有，$a^{|G|}=1$.

证明 由循环群的性质可知，ord(a)是$|G|$的因子，即存在整数 k，使得$|G|=k$ ord(a)．所以，$a^{|G|}=a^{k\,\mathrm{ord}(a)}=(a^{\mathrm{ord}(a)})^k=(1)^k=1$.

定理 6.5.7 设 p 是一个素数，群$(G,\cdot)$的阶为 p，则 G 必为循环群.

证明 选择一个元素 $a\in G$，且 $a\neq1$，则由拉格朗日定理可知$|\langle a\rangle|$是 p 的因子，由于$|\langle a\rangle|>1$，且 p 是一个素数，所以$|\langle a\rangle|=p=|G|$，所以$\langle a\rangle=G$.

有了子群、陪集和商集的定义，我们可以介绍一个重要的概念：商群.

定理 6.5.8 群$(G,\cdot)$的子群$(N,\cdot)$是正规子群的充要条件是：对任意 $a\in G$ 有，

$$aN=Na.$$

证明 我们在定理 6.2.4 中已经证明了上述结论，这里仅给出更直接的证明.

充分性．对任意 $a\in G$，因为 $aN=Na$，所以对任意 $n\in N$ 必存在一个 $s\in N$，使得

$$a\cdot n=s\cdot a,$$

故有

$$a\cdot n\cdot a^{-1}=s\cdot a\cdot a^{-1}=s\in N,$$

即$(N,\cdot)$是正规子群.

必要性. 因为$(N, \cdot)$是正规子群, 所以对任意 $a\in G$ 和任意 $n\in N$ 都有, $a\cdot n\cdot a^{-1}\in N$, 故存在一个 $s\in N$ 使得

$$a\cdot n\cdot a^{-1}=s,$$

于是

$$a\cdot n=s\cdot a,$$

因此对任意 $a\cdot n\in aN$ 必存在 $s\in N$, 使得 $a\cdot n=s\cdot a\in Na$, 即 $a\cdot n\in Na$, 所以 $aN\subseteq Na$.

反过来对任意 $a\in G$ 和任意 $n\in N$ 都有, $a^{-1}\cdot n\cdot (a^{-1})^{-1}\in N$, 故存在一个 $s\in N$ 使得

$$a^{-1}\cdot n\cdot (a^{-1})^{-1}=s,$$

于是

$$n\cdot a=a\cdot s,$$

因此对任意 $n\cdot a\in Na$ 必存在 $s\in N$, 使得 $n\cdot a=a\cdot s\in aN$, 即 $n\cdot a\in aN$, 所以 $Na\subseteq aN$.

综上得 $aN=Na$. 证毕.

从这个定理可知, 由正规子群形成的陪集没有左右之分, 此时我们就能够使用陪集这个术语, 相应地, 由正规子群形成的商集 G/N 是由没有左右之分的陪集组成的.

定理 6.5.9 设群$(G, \cdot)$有一个正规子群$(N, \cdot)$, $T=G/N$ 是 N 在 G 中的商集, 在商集 T 上定义二元运算“$\odot$”为: 对任意 $aN, bN\in T(a, b\in G)$,

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

则$(T, \odot)$构成群.

证明 首先我们证明运算“$\odot$”的定义中两个任意元素(陪集)的计算结果不依赖于陪集代表元的选择. 即要证明对任意 $aN=a'N$, $bN=b'N$, 都有$(ab)N=(a'b')N$ 成立. 事实上, 由 G 中的结合律和正规子群的性质, 我们有

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

首先, “$\odot$”满足结合律, 因为

$$(aN\odot bN)\odot cN=(a\cdot b)N\odot cN=((a\cdot b)\cdot c)N=(a\cdot (b\cdot c))N=aN\odot (b\cdot c)N=aN\odot (bN\odot cN).$$

设 e 是$(G, \cdot)$的单位元, 则 $eN=N$ 是$(T, \odot)$的单位元. 这是因为对任意 $a\in G$,

$$aN\odot N=aN\odot eN=(a\cdot e)N=aN,$$

$$N\odot aN=eN\odot aN=(e\cdot a)N=aN.$$

对任意 $a\in G$, aN 存在逆元 $a^{-1}N$. 事实上,

$$aN\odot a^{-1}N=(a\cdot a^{-1})N=eN=N,$$

$$a^{-1}N\odot aN=(a^{-1}\cdot a)N=eN=N.$$

综上所述可知, $(T, \odot)$构成群. 证毕.

为了方便表示, 在不致混淆的情况下, 我们将群$(G, \cdot)$的子群与商群中的运算都记做 $\cdot$.

定义 6.5.5 定理 6.5.9 中的群$(T, \cdot)$叫作群$(G, \cdot)$对正规子群$(N, \cdot)$的**商群**. 记为

$$(T, \cdot)=(G, \cdot)/(N, \cdot)=(G/N, \cdot).$$

习题 6.5

A 组

1. 质数阶的群没有非平凡子群, 且一定是循环群.
2. 已知群G_1, G_2是 G 的有限子群,证明:

$$|G_1G_2|=[G_1:1]\,[G_2:1]\,/\,[G_1\cap G_2:1]$$

3. 已知群G_1, G_2是 G 的有限子群且$G_1\subseteq G_2$,证明:

$$[G:G_1]=[G:G_2]\,[G_2:G_1].$$

B 组

4. 设 H 是群 G 的正规子群,证明商群 G/H 是 Abel 群的充要条件是:

$$gkg^{-1}h^{-1}\in H,\quad \forall g,k\in G.$$

6.6 同态、同构

同态和同构是代数学中至关重要的内容, 同态基本定理作为本章的核心内容, 在代数学中有广泛的应用, 而且也将贯穿之后的环与域的内容. 我们这里讨论群同态与同构的基本概念, 而后直接介绍群的同态基本定理.

定义 6.6.1 $(X,\cdot)$与$(Y,*)$是两个群, 如果存在一个映射 $f:X\to Y$, 使得对任意 $x_1,x_2\in X$, 都有

$$f(x_1\cdot x_2)=f(x_1)*f(x_2),$$

则称 f 是一个从$(X,\cdot)$到$(Y,*)$的**同态映射**或称群$(X,\cdot)$与$(Y,*)$**同态**, 记作$(X,\cdot)\sqcup(Y,*)$或 $X\sqcup Y$.

如果 f 是单射, 则称此同态为**单同态**, 如果 f 是满射, 则称此同态为**满同态**, 如果 f 是双射, 则此同态为**同构**. 记作$(X,\cdot)\cong(Y,*)$或 $X\cong Y$.

一个群到自身的同态叫**自同态**, 自身的同构叫**自同构**, 并记作 Aut G.

例 6.6.1 群$(\mathbf{Z}_I,+)$到群$(\mathbf{Z}_n,+)$的映射 f: $\mathbf{Z}_I\to\mathbf{Z}_n$是

$$f(a)=a \bmod n$$

是一个同态映射.

证明 对任意 $a,b\in\mathbf{Z}_I$, 有

$$f(a+b)=(a+b) \bmod n,$$

$$f(a)\oplus f(b)=(a \bmod n)\oplus(b \bmod n)=((a \bmod n)+(b \bmod n)) \bmod n=(a+b) \bmod n,$$

所以 $f(a+b)=f(a)\oplus f(b)$. 而且这个同态明显是一个满同态.

例 6.6.2 群$(\mathbf{R},+)$和$(\mathbf{R}^+,\times)$同构

证明 对$(\mathbf{R},+)$与$(\mathbf{R}^+,\times)$有一个一一对应的映射 f: $\mathbf{R}\to\mathbf{R}^+$,

$$f(x)=e^x,$$

且对任意 $a,b\in\mathbf{R}$, 有

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

这个例子中的映射 f 的逆函数 g: $\mathbf{R}^+\to\mathbf{R}$ 为

$$g(x)=\ln(x),$$

它也是一个同构映射, 因为 $g(a\times b)=\ln(a\times b)=\ln a+\ln b=g(a)+g(b)$.

例 6.6.3 群$(\mathbf{C},+)$和$(\mathbf{R}^2,+)$同构

证明 对$(\mathbf{C},+)$与$(\mathbf{R}^2,+)$有一个一一对应的映射 f: $\mathbf{C}\to\mathbf{R}^2$,

$$f(a+ib)=(a,b),$$

且对任意 $a+ib$, $c+id\in\mathbf{C}$, 有

$$f([a+ib]+[c+id])=f([a+c]+i[b+d])=(a+c,\ b+d)=(a,b)+(c,d)=f(a+ib)+f(c+id).$$

定理 6.6.1 设两个群满足$(S,\cdot)\sqcup(G,\odot)$, e 和 e'分别为它们的单位元, 同态映射为 $f:S\to G$, 则有

(1) $f(e)=e'$;

(2) 对任意 $a\in S$, $f(a^{-1})=f(a)^{-1}$;

(3) 对任意 $n\in \mathbf{Z}_{\mathbf{I}}$和 $a\in S$，$f(a^n)=f(a)^n$.

证明 (1) 因为群$(S,\cdot)$和群$(G,\odot)$同态，所以

$$f(e)=f(e\cdot e)=f(e)\odot f(e),$$

所以

$$e'=f(e)\odot f(e)^{-1}=(f(e)\odot f(e))\odot f(e)^{-1}=f(e)\odot(f(e)\odot f(e)^{-1})=f(e)\odot e'=f(e).$$

(2) $e'=f(e)=f(a^{-1}\cdot a)=f(a^{-1})\odot f(a)$, 由逆元的定义有

$$f(a)^{-1}=f(a^{-1}).$$

(3) 对于 $n\geq 0$，我们能够利用数学归纳法很容易证明 $f(a^n)=f(a)^n$. 对于 $n<0$，有

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

定义 6.6.2 设两个群满足$(S,\cdot)\sqcup(G,\odot)$，e 和 e'分别为它们的单位元，同态映射为 $f:S\to G$，令集合

$$\ker f=\{a\mid a\in S \text{ 且 } f(a)=e'\},$$

我们称该集合为同态 f 的**核**，且令集合

$$\mathrm{im}f=f(S)=\{f(a)\mid a\in S\},$$

我们称该集合为同态 f 的**像**.

定理 6.6.2 设两个群满足$(S,\cdot)\sqcup(G,\odot)$，e 和 e'分别为它们的单位元，同态映射为 $f:S\to G$，则有

(1) $\ker f\leqslant S$(我们将 $\ker f$ 称为同态 f 的**核子群**)，且 f 是单同态的充要条件是 $\ker f=\{e\}$;

(2) $\mathrm{im}f\leqslant G$ (我们将 $\mathrm{im}f$ 称为同态 f 的**像子群**)，且 f 是满同态的充要条件是 $f(S)=G$;

(3) 如果 $G'\leqslant G$，$f^{-1}(G')=\{a\mid a\in S \text{ 且 } f(a)\in G'\}$，则 $f^{-1}(G')\leqslant S$.

证明 (1) 由定理 6.6.1 知 $f(e)=e'$，所以 $e\in\ker f$，即 $\ker f$ 不是空集.

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

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

因此有 $a\cdot b^{-1}\in\ker f$，由定理 6.2.1 的子群判别标准知 $\ker f\leqslant S$.

设 f 为单同态，则 S 中满足 $f(a)=e'=f(e)$的元素只有 $a=e$，因此 $\ker f=\{e\}$.

反过来，设 $\ker f=\{e\}$，对任意 $a,b\in S$，若 $f(a)=f(b)$，则必有

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

因此 $a\cdot b^{-1}\in\ker f$，$a\cdot b^{-1}=e$，所以 $a=b$. 因此，f 是单同态.

(2) 由定理 6.6.1 知 $f(e)=e'$，所以 $e'\in\mathrm{im}f$，即 $\mathrm{im}f$ 不是空集.

对任意 $x,y\in\mathrm{im}f$，必存在 $a,b\in S$，使得 $f(a)=x$，$f(b)=y$，显然 $a\cdot b^{-1}\in S$(S 是群),

$$x\odot y^{-1}=f(a)\odot f(b)^{-1}=f(a)\odot f(b^{-1})=f(a\cdot b^{-1}).$$

因为 $a\cdot b^{-1}\in S$，所以 $f(a\cdot b^{-1})\in\mathrm{im}f$，即 $x\odot y^{-1}\in\mathrm{im}f$，由定理 6.2.1 的子群判别标准知 $\mathrm{im}f\leqslant G$.

由满同态的定义知 f 为满同态的充要条件为 $f(S)=G$.

(3) 因为 $G'\leqslant G$，所以 $e'\in G'$，由定理 6.6.1 知 $f(e)=e'$，所以 $e\in f^{-1}(G')$，即 $f^{-1}(G')$ 不是空集. 对任意 $a,b\in f^{-1}(G')$，必存在 $x,y\in G'$，满足 $f(a)=x$，$f(b)=y$，因为 $G'\leqslant G$，所以有

$$x\odot y^{-1}\in G',$$

即

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

所以 $a\cdot b^{-1}\in f^{-1}(G')$，由定理 6.2.1 的子群判别标准知 $f^{-1}(G')\leqslant S$.

定理 6.6.3 设 f 是群$(S, \cdot)$到群$(G, \odot)$的同态映射，e 和 e'分别是$(S, \cdot)$和$(G, \odot)$的单位元，则 $\ker f \lhd S$;

证明 对任意 $a \in S$，$b \in \ker f$，我们有

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

所以 $a \cdot b \cdot a^{-1} \in \ker f$，由正规子群的定义知 $\ker f \lhd S$. 证毕.

定理 6.6.4 如果两个群满足$(N, \cdot) \lhd (S, \cdot)$，构造商群$(S/N, \odot)$，且定义如下映射 $f: S \to S/N$,

$$f(a) = aN,$$

则 f 是一个同态映射，且 $\ker f = N$.

证明 映射 f 满足

$$f(a \cdot b) = (a \cdot b)N = aN \odot bN = f(a) \odot f(b),$$

所以 f 是从群$(S, \cdot)$到群$(S/N, \odot)$的同态映射. 而群$(S/N, \odot)$的单位元为 N，设 $a \in S$，如果

$$f(a) = N,$$

则有

$$aN = f(a) = N = eN,$$

由定理 6.5.3，$aN = eN$ 的充要条件是 $e^{-1} \cdot a \in N$，即 $a \in N$，所以 $\ker f = N$.

定义 1.6.3 $(N, \cdot) \lhd (S, \cdot)$，定义映射 $f: S \to S/N$,

$$f(a) = aN,$$

则 f 是群$(S, \cdot)$到其商群$(S/N, \odot)$的一个同态映射，由 f 建立的从群$(S, \cdot)$到群$(S/N, \odot)$的同态叫**自然同态**.

定理 6.6.5 （同态基本定理）设 $f: S \to G$ 是群$(S, \cdot)$到群$(G, \times)$的同态映射，则存在 $S/\ker f$ 到 $\operatorname{im} f$ 的一一映射 $h: S/\ker f \to \operatorname{im} f$，使得

$$(S/\ker f, \odot) \cong (\operatorname{im} f, \times)$$

即 $S/\ker f \cong \operatorname{im} f$.

证明 设群$(S, \cdot)$的单位元为 e，群$(G, \times)$的单位元为 e'. 由定理 6.6.3 我们知道

$$(\ker f, \cdot) \lhd (S, \cdot),$$

所以商群$(S/\ker f, \odot)$一定存在，由定理 6.5.9 可知商群$(S/\ker f, \odot)$的单位元为 $\ker f$. 定义如下映射 $h: S/\ker f \to \operatorname{im} f$，对任意陪集 $x\ker f \in S/\ker f$，有

$$h(x\ker f) = f(x),$$

则对任意 $a\ker f, b\ker f \in S/\ker f$ 有

$$\begin{aligned} h(a\ker f \odot b\ker f) &= h((a \cdot b)\ker f) \\ &= f(a \cdot b) \\ &= f(a) \times f(b) \\ &= h(a\ker f) \times h(b\ker f) \end{aligned}$$

所以 h 是从群$(S/\ker f, \odot)$到群$(\operatorname{im} f, \times)$的同态映射.

其次，h 是单同态映射. 事实上，由定理 6.6.2 可知$(\operatorname{im} f, \times)$是$(G, \times)$的子群，故$(\operatorname{im} f, \times)$的单位元是 e'. 对任意 $a\ker f \in \ker h$，下面两式同时成立，

$$h(a\ker f) = f(a),$$

$$h(a\ker f) = e',$$

所以有

$$f(a) = e',$$

即 $a\in\ker f$，又知当 $a\in\ker f$ 时，$a\ker f=\ker f$，即 $\ker h$ 中只有一个元素 $\ker f$，所以有

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

而 $\ker f$ 是商群$(S/\ker f,\odot)$的单位元，由定理 6.6.2 知 h 为单同态映射.

最后，我们来证明 h 是满同态．事实上，对任意 $c\in\operatorname{im} f$，存在 $a\in S$，使得 $f(a)=c$，从而

$$h(a\ker f)=f(a)=c.$$

所以任意 $\operatorname{im} f$ 中的元素 c 在映射 h 下都有原像 $a\ker f$．至此我们证明了 h 是从群$(S/\ker f,\odot)$到群$(\operatorname{im} f,\times)$的单同态映射，又是满同态映射，所以 h 是从群$(S/\ker f,\odot)$到群$(\operatorname{im} f,\times)$的同构映射.

例 6.6.4 例 6.6.1 中群$(\mathbf{Z},+)$到群$(\mathbf{Z}_n,+)$的映射 f: $\mathbf{Z}\to\mathbf{Z}_n$，其中 $f(a)=a \bmod n$ 是一个同态映射．显然 $\ker f=\{a\mid a\in\mathbf{Z}\text{ 且 }f(a)=0 \bmod\}=n\mathbf{Z}$.

同时，容易证明 $n\mathbf{Z}$ 是 $\mathbf{Z}$ 的正规子群．如果考虑 $\mathbf{Z}$ 对 $n\mathbf{Z}$ 的商群，则有

$$\mathbf{Z}/n\mathbf{Z}=\{\{a+(n\mathbf{Z})\}\mid a\in\mathbf{Z}\}=\{\{a+nh\mid h\in\mathbf{Z}\}\mid a\in\mathbf{Z}\}=\{[0],[1],\cdots,[n-1]\}=\mathbf{Z}_n$$

进一步地，我们有 $\mathbf{Z}/n\mathbf{Z}\cong\mathbf{Z}_n$.

习题 6.6

A 组

1. 设 f 为群 G 群 H 的映射，分别判断如下的 f 是否为同态，是则给出 $\ker f$.
   (1) 加法群 $G=\mathbf{R}$，$H=\mathbf{Z}$，$f(x)=[x]$，其中$[x]$为 x 取整函数，即为不大于的最大整数;
   (2) 乘法群 $G=\mathbf{R}^*$，$H=\mathbf{R}^+$，$f(x)=|x|$;
   (3) $G=S_n$，$H=\{+1,-1\}$，$f(\alpha)=\operatorname{sgn}\alpha$; $\mathbf{R}^*$
   (4) $G=GL(n,R)$，$H=\mathbf{R}^*$，$f(A)=\det A$;
   (5) $G=\mathbf{Z}_5$，$H=\mathbf{Z}_2$，$f(x)=x \bmod 2$;
2. G 是一个群，证明其自同构集合 Aut G 是一个群.
3. 设 G 是一个群，证明:
   (1) $g\to g^{-1}$是 G 的自同构当且仅当 G 是 Abel 群.
   (2) 若 G 是 Abel 群，对任意整数 k，$g\to g^k$是 G 的自同态.
4. 证明例 1.17 中的 Klein 四元群 K 的自同构群 Aut K 与S_3同构.

B 组

5. 给定一组群$\{G_i\}_{i\in\mathbf{Z}}$，以及同态映射$\{f_i\}_{i\in\mathbf{Z}}$构成的序列：

   $$\cdots\to G_{i-1}\xrightarrow{f_{i-1}}G_i\xrightarrow{f_i}G_{i+1}\to\cdots,$$

   若对 $\forall i\in\mathbf{Z}$，$f_{i-1}(G_{i-1})=\ker f_i$，则称该序列是**正合**的．规定：$0\to G$ 为将零元映射为中零元的同态映射，$G\to 0$ 为将所有元素映射为零元的同态映射．试证明：
   (1) f 是单同态当且仅当序列$0\to H\xrightarrow{f}K$ 是正合的;
   (2) f 是满同态当且仅当序列$H\xrightarrow{f}K\to 0$ 是正合的;
   (3) f 是同构当且仅当序列$0\to H\xrightarrow{f}K\to 0$ 是正合的.
6. 已知群H_1,H_2分别是G_1,G_2的正规子群，f 是G_1到G_2的同态，证明：若 $f(H_1)\subseteq H_2$，则 f 可诱导出的G_1/H_1到G_2/H_2一个同态.