第二章　群

与熟悉的数、多项式、矩阵、函数等相比较, 群是我们遇到的第一个与它们“本质上”不同的数学概念. 理解和掌握群的概念能提高我们接受任何新的数学概念的修养.

我们将从群本身, 一个群和其他群的关系, 以及群对外部世界的作用三个方面对群进行研究. 这也是对任何事物都该采用的三个研究角度.

§1　群的定义

1.1　定义的引入

先看一个具体的群. 设 M 是一个集合, $T(M)$ 是 M 的所有变换 (即 M 到 M 的映射) 组成的集合. $T(M)$ 有一个自然的运算: 变换的乘法. 今考察 $T(M)$ 的一个特殊子集

$$S(M)=\{\text{集 } M \text{ 的所有一一变换}\},$$

这里“M 的一一变换”是指: 集 M 到 M 上的一一映射. 容易看到 $S(M)$ 中的两个一一变换的乘积仍然是 M 的一个一一变换, 即仍然在 $S(M)$ 中, 这样变换的乘法是集 $S(M)$ 的一个二元运算. M 的恒等变换 E 在 $S(M)$ 的运算中占据一个特殊地位: 对 $S(M)$ 中的任意元素 S 都有 $ES=SE=S$, 并且有 S 的逆变换 $S^{-1}\in S(M)$ 使得 $SS^{-1}=S^{-1}S=E$. 这样得到 $(S(M),\cdot)$ 具有下面三条好性质:

G1. $(X\cdot Y)\cdot Z=X\cdot(Y\cdot Z)$,　$X,Y,Z\in S(M)$ (结合律);

G2. 对任意 $X\in S(M)$, $E\cdot X=X\cdot E=X$;

G3. 对任意 $X\in S(M)$, 存在 $X^{-1}\in S(M)$, $X\cdot X^{-1}=X^{-1}\cdot X=E$.

称 $(S(M),\cdot)$ 为集 M 上的变换群. 当 $|M|=n<\infty$ 时, 特称 $(S(M),\cdot)$ 为 n 次对称群, 并记作 S_n.

再看一个具体群. 设

$$GL_n(\mathbb{R})=\{\text{实数域 } \mathbb{R} \text{上的所有 } n \text{ 阶非退化矩阵}\}.$$

由于非退化矩阵的乘积仍是非退化矩阵, 故知矩阵的乘法是集 $GL_n(\mathbb{R})$ 的一个二元运算. 单位矩阵 $\boldsymbol{I}_n$ 在 $GL_n(\mathbb{R})$ 的运算中占有一个特殊地位: 对 $GL_n(\mathbb{R})$ 中任意元素 $\boldsymbol{A}$, 都有 $\boldsymbol{I}_n\cdot\boldsymbol{A}=\boldsymbol{A}\cdot\boldsymbol{I}_n=\boldsymbol{A}$, 并且有 $\boldsymbol{A}$ 的逆矩阵 $\boldsymbol{A}^{-1}\in GL_n(\mathbb{R})$ 使得 $\boldsymbol{A}\cdot\boldsymbol{A}^{-1}=\boldsymbol{A}^{-1}\cdot\boldsymbol{A}=\boldsymbol{I}_n$, 即 $(GL_n(\mathbb{R}),\cdot)$ 满足上面的三条性质 G1, G2, G3. 我们称 $(GL_n(\mathbb{R}),\cdot)$ 为实数域 $\mathbb{R}$ 上的 n 阶一般线性群.

抽象、概括这些具体群, 我们有下面的定义.

定义 1.1　设 G 是一个非空集合, $\cdot$ 是 G 的一个二元运算. 如果 $(G,\cdot)$ 满足下列三个条件:

G1. $(a\cdot b)\cdot c=a\cdot(b\cdot c)$, $\forall\ a,\ b,\ c\in G$ (结合律);

G2. $\exists\ e\in G$, 使得 $e\cdot a=a\cdot e=a$, $\forall a\in G$ (称元素 e 为 G 的单位元);

G3. 对任意 $a\in G$, $\exists\ a'\in G$, 使得 $a\cdot a'=a'\cdot a=e$ (称 a' 为 a 的逆元).

则称 $(G,\cdot)$ 为群 (group) (简称 G 是群).

如果 $(G,\cdot)$ 满足 G1, 则称 G 是半群 (semigroup). 如果 $(G,\cdot)$ 满足 G1 和 G2, 则称 G 是有单位元的半群. 例如, $(T(M),\cdot)$ 是有单位元的半群.

在不引起混淆的情况下, 今后我们常将运算符号“$\cdot$”省略不写. 例如我们常将 $a\cdot b$ 简写成 ab.

定义 1.2　设 $(G,\cdot)$ 是群, 若有 $ab=ba$, $\forall\ a,\ b\in G$ (交换律), 则称 $(G,\cdot)$ 为交换群.

交换群通常又称为 Abel 群, 以纪念挪威数学家 N. H. Abel (1802— 1829).

定义 1.3 若群 G 作为集合是有限集, 则称 G 为有限群 (finite group), 而称 $|G|$ 为群 G 的阶 (order). 若 G 是无限集, 则称群 $(G,\cdot)$ 为无限群.

类似地, 我们有有限半群的概念.

易见 $S(M)$, $GL_n(\mathbb{R})$, S_n 都是群. $GL_n(\mathbb{R})$ 是无限群, 而 S_n 是有限群.

1.2 简单的性质

有了用公理刻画的抽象群的定义之后, 很自然地把抽象群和一些具体群作一比较. 在群的定义中我们只要求存在一个单位元 e, 而在具体群 $S(M)$, $GL_n(\mathbb{R})$ 中单位元以及每个元的逆元还是唯一的. 自然要问: 在抽象群 G 中单位元以及元 a 的逆元是唯一的吗?

命题 1.4 (i) 群 G 的单位元是唯一的 (今后在群 G 中常用 e 表示这唯一的单位元).

(ii) 在群 G 中任意元 a 的逆元是唯一的 (今后用 a^{-1} 表示元素 a 的唯一逆元).

(iii) 在群 G 中有 $(ab)^{-1}=b^{-1}a^{-1}$, $\forall\, a,b\in G$ (穿脱原理).

证 (i) 证明唯一性的常用方法是假定有两个同时满足条件的元素而去证明它们彼此相等. 设 e,e' 都是群 G 的单位元, 即都满足 G2, 则由

$$e=ee'=e'$$

知两者相等. 这就证得单位元的唯一性.

(ii) 在群 G 中, 设 a_1,a_2 都是 a 的逆元, 即都满足 G3, 则由

$$a_1=a_1e=a_1(aa_2)=(a_1a)a_2=ea_2=a_2$$

即知 a 的逆元是唯一的.

(iii) 我们有

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

以及

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

由逆元的定义知 $(ab)^{-1}=b^{-1}a^{-1}$. ■

在数的乘法运算中, 我们有消去律, 它使用起来很方便, 在群的运算中也有如下消去律.

命题 1.5 (i) 在群 G 中若 $ab=ac$, 则有 $b=c$.(左消去律)

(ii) 在群 G 中若 $ba=ca$, 则有 $b=c$. (右消去律)

证 只证 (i). 由 $ab=ac$, 得 $a^{-1}(ab)=a^{-1}(ac)$. 利用结合律, 得 $(a^{-1}a)b=(a^{-1}a)c$, 即 $eb=ec$, 故得 $b=c$. ■

1.3 群的单边定义 *

在一个半群 G 中, 一个元 $e_l\in G$ 称为左单位元, 如果 $e_lg=g$, $\forall\, g\in G$.

设 G 是有左单位元 e_l 的半群. 称元 $a\in G$ (相对于 e_l) 有左逆元, 如果存在 $b\in G$ 使得 $ba=e_l$. 将 b 称为 a 的左逆元.

下面的定理表明群恰是有左单位元的半群, 并且其中任一元均有左逆元. 这比定义 1.1 使用起来要方便得多.

定理 1.6 *设 G 是半群, 则 G 是群当且仅当 G 有左单位元, 且任一元均有 (相对于这个左单位元的) 左逆元.*

证 *必要性是已知的. 下证充分性.*

设 e_l 是 G 的左单位元. 对 G 的任一元 g, 用 g_l 表示 g 的左逆元. 特别地, g_l 的左逆元记为 $(g_l)_l$. 于是 $(g_l)_lg_l=e_l=g_lg$. 从而

$$gg_l=(e_lg)g_l=((g_l)_lg_l)gg_l=(g_l)_l(g_lg)g_l=(g_l)_le_lg_l=(g_l)_lg_l=e_l.$$

于是

$$ge_l=g(g_lg)=(gg_l)g=e_lg=g,\ \forall\, g\in G.$$

这表明 e_l 是 G 的单位元; 从而 g_l 也是 g 的逆元, 即 G 是群. ■

将定理 1.6 中的“左”改为“右”, 结论仍然成立 (留作习题).

作为上述定理的一个应用, 我们得到有限半群是群的充要条件.

命题 1.7 设 G 是有限半群. 则 G 是群当且仅当 G 满足左消去律和右消去律.

证 必要性是已知的. 下证充分性.

设 $G=\{g_1,\cdots,g_n\}$. 取 $a\in G$. 令 $Ga=\{g_1a,\cdots,g_na\}$. 因为 G 满足右消去律, 故 Ga 也由 n 个不同元素组成, 随之, $Ga=G$. 又因为 $a\in G=Ga$, 故存在唯一的元 $e\in G$ 使得 $a=ea$.

又因为 G 满足左消去律, 故 $aG=G$. 因此对于任一 $g\in G$, 存在 $h\in G$ 使得 $ah=g$. 于是

$$eg=e(ah)=(ea)h=ah=g.$$

也就是说 e 是 G 的左单位元.

对于任一 $g\in G$ 有 $Gg=G$. 故存在唯一的元 $g_l\in G$ 使得 $g_lg=e$, 即任一元均有 (相对于左单位元 e_l 的) 左逆元. 从而由定理 1.6 知 G 是群. ■

1.4 例子

下面给出群的一些例子.

例 1.8 n 阶正交群 $\boldsymbol{O}(n,\mathbb{R})$. 设

$$\boldsymbol{O}(n,\mathbb{R})=\{\text{实数域 }\mathbb{R}\text{上的所有 }n\text{ 阶正交矩阵}\},$$

这里正交矩阵指满足条件 $\boldsymbol{A}\cdot\boldsymbol{A}^{\mathrm{T}}=\boldsymbol{I}$(单位矩阵) 的 n 阶实矩阵 $\boldsymbol{A}$, 其中 $\boldsymbol{A}^{\mathrm{T}}$ 是 $\boldsymbol{A}$ 的转置矩阵. 由于正交矩阵 $\boldsymbol{A},\boldsymbol{B}$ 之积 $\boldsymbol{AB}$ 仍有性质

$$\boldsymbol{AB}\cdot(\boldsymbol{AB})^{\mathrm{T}}=\boldsymbol{AB}\cdot\boldsymbol{B}^{\mathrm{T}}\boldsymbol{A}^{\mathrm{T}}=\boldsymbol{AIA}^{\mathrm{T}}=\boldsymbol{I},$$

故集 $\boldsymbol{O}(n,\mathbb{R})$ 有矩阵的乘法运算, $\boldsymbol{I}$ 是正交矩阵, 且有

$$\boldsymbol{IA}=\boldsymbol{AI}=\boldsymbol{A},\quad\forall\boldsymbol{A}\in\boldsymbol{O}(n,\mathbb{R}).$$

若 $\boldsymbol{A}$ 是正交矩阵, 则 $\boldsymbol{A}^{-1}$ 也是正交矩阵, 因而也在 $\boldsymbol{O}(n,\mathbb{R})$ 中. 矩阵的乘法是满足结合律的, 故根据群的定义, $(\boldsymbol{O}(n,\mathbb{R}),\cdot)$ 是一个群.

例 1.9 平面 P 的运动群 $M(P)$. 设 P 为一个平面上所有点的集合. 称集 P 的一个一一变换 ϕ 是保距变换, 如果任意两点 a,b 变换前的距离 $\overline{ab}$ 和变换后 (即 ϕa 和 ϕb) 的距离 $\overline{\phi a\phi b}$ 相等. 我们把 P 的保距变换简称为平面 P 的运动. 设 $M(P)$ 是平面 P 的所有运动的集合. 由于两个平面 P 的运动 (在变换乘法运算下) 的乘积仍是平面 P 的运动. 故 $M(P)$ 有乘法运算. 显然恒等变换 E 是平面 P 的运动, 故 $M(P)$ 有单位元. 若 ϕ 是运动, 得 $\overline{\phi^{-1}a\phi^{-1}b}=\overline{ab}$, 即 ϕ^{-1} 也是运动. 综合起来便知 $(M(P),\cdot)$ 是群, 称之为平面运动群.

例 1.10 有不动点 O 的平面运动群 $M(P,O)$. 如果 P 的一个变换 ϕ 保持点 O 不动, 即有 $\phi O=O$, 则称点 O 为变换 ϕ 的不动点. 今考察 $M(P)$ 的一个子集

$$M(P,O)=\{P\text{的以点 }O\text{ 为不动点的所有运动}\}.$$

读者不难验证 $M(P,O)$ 对变换的乘法作成一个群. 用一点平面几何的知识我们可以证明, P 的以点 O 为不动点的运动或是绕点 O 的旋转或是关于过点 O 的一条直线 l 的翻折 (或称反射). 称群 $M(P,O)$ 为有不动点 O 的平面运动群.

例 1.11 整数加法群 $\mathbb{Z}$. 容易验证 $(\mathbb{Z},+)$ 是一个群:$\mathbb{Z}$ 有加法运算且满足结合律. 数 0 是它的 (关于加法) 单位元:$0+n=n+0=n$, $\forall n\in\mathbb{Z}$. 在这里 $-a$ 扮演着逆元的角色:$(-a)+a=a+(-a)=0$. 它是一个 Abel 群.

例 1.12 模 n 的剩余类加群 $\mathbb{Z}_n$. 设 n 是正整数. 在第一章 §2 中我们定义了模 n 的剩余类的集合 $\mathbb{Z}_n$ 的加法运算 $+$:

$$\bar{a}+\bar{b}=\overline{a+b}, \quad \forall\ a,\ b\in\mathbb{Z}.$$

容易验证 $(\mathbb{Z}_n,\ +)$ 是 n 阶 Abel 群, 称之为模 n 的剩余类加群. 它的单位元是 $\bar{0}$, $\bar{a}$ 的逆元为 $\overline{-a}=\overline{n-a}$.

例 1.13 四元群. 取由四个元素 e,a,b,c 作成的集合 Q. 下表给出 Q 的一个二元运算:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

例如 $e\cdot a=a$, $a\cdot b=c$. 直接验证这是一个满足结合律的运算, 例如

$$(a\cdot a)\cdot b=e\cdot b=b;$$
$$a\cdot(a\cdot b)=a\cdot c=b,$$

故有 $(a\cdot a)\cdot b=a\cdot(a\cdot b)$. 类似地去验证所有共 4^3 种情形. e 具有单位元的性质, 而这四个元素中每一元素都是它自己的逆元. 这样 $(Q,\cdot)$ 作成一个 4 阶 Abel 群, 称之为四元群.

以上列举的群都是自然的. 应该说, 当我们把“群”作为对象去研究时, 一切具体群, 不管它是自然出现的或是人为的, 都是我们喜爱和需要的.

下面将首先对一个群进行研究, 然后研究两个群之间的关系, 研究一个抽象群和具体群之间的联系. 把具有某种特殊性质的群类中每一个群都列举出来, 这是研究群的重要问题之一. 最后还要从群作用到外部世界这一角度来研究群本身的结构.

习 题

1. 令 $\boldsymbol{N}$ 是所有 n 阶下三角非奇异复方阵的集合, $\boldsymbol{D}$ 是主对角线上的元都是非零复数的 n 阶对角矩阵的集合. 说明矩阵的乘法是 $\boldsymbol{N},\boldsymbol{D}$ 的运算, 并证明 $\boldsymbol{N}$ 和 $\boldsymbol{D}$ 对矩阵的乘法作成群.

2. 令 G 是实数对 (a,b), $a\neq 0$, 的集合. 在 G 上定义二元运算 $(a,b)\,(c,d)=(ac,\ ad+b)$. 试证 G 对此二元运算作成群.

3. 令 Ω 是任意一个非空集合, G 是一个群, G^Ω 是 Ω 到 G 的所有映射的集合. 对任意两个映射 $f,g\in G^\Omega$, 定义乘积 fg 是这样的映射: 对任意 $a\in\Omega$, $(fg)(a)=f(a)\,g(a)$. 试证 G^Ω 是群.

4. 设 G 是一个半群. 如果

(i) G 中含有右单位元 e_r, 即对任意 $a\in G$, $ae_r=a$,

(ii) G 的每个元 a 有右逆元 b, 即 $ab=e_r$,

试证 G 是群.

5. (这可作为群的另一定义: 即群的除法定义) 设 G 是半群. 若对任意 $a,\ b\in G$, 方程 $xa=b$ 和 $ay=b$ 在 G 内有解, 则 G 是群.

6. 证明有限群 G 中满足 $x^2\neq e$ 的元 x 有偶数个. (提示: 若 $a^2\neq e$, 则 $(a^{-1})^2\neq e$, 且 $a\neq a^{-1}$.)

7. 在偶数阶群 G 中, 方程 $x^2=e$ 总有偶数个解. (提示: 利用上题.)

8. 设 G 是群. 若 $a^2=e$, $\forall\ a\in G$, 则 G 是 Abel 群.

9. 举例说明命题 1.7 对于无限半群不成立. (提示: 例如考虑非负整数集 $\mathbb{N}_0$ 对于数的加法作成的半群.)

§2 子 群

我们总希望把所研究的新对象与熟悉的对象相对比, 以便容易接受和学习这个新对象——群. 数、多项式、矩阵似乎离群远