§2 群的概念

代数最初主要研究的是数, 以及由数所衍生出来的对象, 例如: 代数方程的求根. 初等代数主要研究的就是数以及数的运算. 中学数学虽然有所谓代数式的概念, 但这些概念本质上代表的仍然是数. 高等代数虽引入了行列式、矩阵等概念, 但还是离不开数. 数的一个基本特征是可以进行加法、乘法等运算. 这些运算的共同特点是: 对任意两个数, 通过某个法则 (如加法法则或乘法法则等), 可惟一求得第三个数. 数学家们发现, 许多抽象的对象也都具有类似于数的这一特征, 于是对它们的结构和性质进行了研究, 并且应用它们解决了许多重大的数学问题和实际问题. 这就导致了近世代数的产生和发展. 近世代数拓展了代数的研究领域. 它所研究的已不再仅仅是数, 而是具有某种运算的代数系统, 这其中最基本的就是群、环和域.

这一节的主要目的就是介绍群的基本概念和简单性质. 为此, 我们首先要对运算这一概念给出明确的定义.

定义 2.1 设 A 是一个非空集合, 若对 A 中任意两个元素 a, b, 通过某个法则 "$\cdot$", 有 A 中惟一确定的元素 c 与之对应, 则称法则 "$\cdot$" 为集合 A 上的一个**代数运算** (*algebraic operation*). 元素 c 是 a, b 通过运算 "$\cdot$" 作用的结果, 我们将此结果记为 $a \cdot b = c$.

例 1 有理数的加法、减法和乘法都是有理数集 $\mathbf{Q}$ 上的代数运算, 但除法不是 $\mathbf{Q}$ 上的代数运算. 如果只考虑所有非零有理数的集合 $\mathbf{Q}^*$, 则除法是 $\mathbf{Q}^*$ 上的代数运算. □

例 2 设 m 为大于 1 的正整数, $\mathbf{Z}_m$ 为 $\mathbf{Z}$ 的模 m 剩余类集. 对 $\overline{a}, \overline{b} \in \mathbf{Z}_m$, 规定:

$$\overline{a} + \overline{b} = \overline{a+b},$$
$$\overline{a} \cdot \overline{b} = \overline{ab}.$$

则 $+$ 与 $\cdot$ 都是 $\mathbf{Z}_m$ 上的代数运算.

证明: 我们只要证明, 上面规定的运算与剩余类的代表元的选取无关即可. 设

$$\overline{a} = \overline{a'}, \quad \overline{b} = \overline{b'},$$

则

$$m \mid a - a', \quad m \mid b - b'.$$

于是

$$m \mid (a-a') + (b-b') = (a+b) - (a'+b'),$$
$$m \mid (a-a')b + (b-b')a' = (ab) - (a'b').$$

从而

$$\overline{a+b} = \overline{a'+b'}, \quad \overline{ab} = \overline{a'b'},$$

所以 $+$ 与 $\cdot$ 都是 $\mathbf{Z}_m$ 上的代数运算. □

分析上面几个例子中的代数运算, 我们发现, 这些代数运算不仅仅给出运算的结果, 而且它们还具有一些类似的运算性质. 比如说, 结合律、交换律等等. 在比较理想的情况下 (就象在 $\mathbf{Q}^*$ 中), 还有单位元、可逆元和逆元. 将这些加以综合与推广, 就得到群的概念.

定义 2.2 设 G 是一个非空集合, "$\cdot$" 是 G 上的一个代数运算, 即对所有的 $a, b \in G$, 有 $a \cdot b \in G$. 如果 G 的运算还满足:

(G1) 结合律, 即对所有的 $a, b, c \in G$, 有 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;

(G2) G 中有元素 e, 使对每个 $a \in G$, 有 $e \cdot a = a \cdot e = a$;

(G3) 对 G 中每个元素 a, 存在元素 $b \in G$, 使 $a \cdot b = b \cdot a = e$.

则称 G 关于运算 "$\cdot$" 构成一个**群** (*group*), 记作 $(G, \cdot)$. 在不致引起混淆的情况下, 也称 G 为群.

注: 1. (G2) 中的元素 e 称为群 G 的**单位元** (*unit element*) 或 **恒等元** (*identity*); (G3) 中的元素 b 称为 a 的**逆元** (*inverse*). 我们将证明: 群 G 的单位元 e 和每个元素的逆元都是惟一的. G 中元素 a 的惟一的逆元通常记作 a^{-1}.

2. 如果群 G 的运算还满足交换律, 即对任意的 $a, b \in G$, 有 $a \cdot b = b \cdot a$, 则称 G 是一个**交换群** (*commutative group*) 或**阿贝尔群** (*abelian group*).

3. 群 G 中元素的个数称为群 G 的**阶** (*order*), 记为 $|G|$. 如果 $|G|$ 是有限数, 则称 G 为**有限群** (*finite group*), 否则称 G 为**无限群** (*infinite group*).

例 3 整数集 $\mathbf{Z}$ 关于数的加法构成群. 这个群称为整数加群.

证明: 对任意的 $a, b \in \mathbf{Z}$, 有 $a + b \in \mathbf{Z}$, 所以 "+" 是 $\mathbf{Z}$ 上的一个代数运算. 同时, 对任意的 $a, b, c \in \mathbf{Z}$, 有

$$(a + b) + c = a + (b + c),$$

所以结合律成立. 另一方面, $0 \in \mathbf{Z}$, 且对每个 $a \in \mathbf{Z}$, 有

$$a + 0 = 0 + a = a,$$

所以 0 为 $\mathbf{Z}$ 的单位元. 又对每个 $a \in \mathbf{Z}$, 有

$$a + (-a) = (-a) + a = 0,$$

所以 $-a$ 是 a 的逆元, 从而 $\mathbf{Z}$ 关于 "+" 构成群, 显然这是一个交换群. □

当群 G 的运算用加号 "+" 表示时, 通常将 G 的单位元记作 0, 并称 0 为 G 的零元; 将 $a \in G$ 的逆元记作 $-a$, 并称 $-a$ 为 a 的负元. 习惯上, 只有当群为交换群时, 才用 "+" 来表示群的运算, 并称这个运算为**加法**, 把运算的结果叫做**和**, 同时称这样的群为**加群**. 相应地, 将不是加群的群称为**乘群**, 并把乘群的运算叫做**乘法**, 运算的结果叫做**积**. 在运算过程中, 乘群的运算符号通常省略不写. 今后, 如不作特别声明, 我们总假定群的运算是乘法. 当然, 所有关于乘群的结论对加群也成立 (必要时, 作一些相关的记号和术语上改变).

例 4 全体非零有理数的集合 $\mathbf{Q}^*$, 关于数的乘法构成交换群, 这个群的单位元是数 1, 非零有理数 $\frac{a}{b}$ 的逆元是 $\frac{a}{b}$ 的倒数 $\frac{b}{a}$. 同理, 全体非零实数的集合 $\mathbf{R}^*$、全体非零复数的集合 $\mathbf{C}^*$ 关于数的乘法也构成交换群. □

例 5 实数域 $\mathbf{R}$ 上全体 n 阶方阵的集合 $M_n(\mathbf{R})$, 关于矩阵的加法构成一个交换群. 全体 n 阶可逆方阵的集合 $GL_n(\mathbf{R})$ 关于矩阵的乘法构成群, 群 $GL_n(\mathbf{R})$ 中的单位元是单位矩阵 E_n, 可逆方阵 $A \in GL_n(\mathbf{R})$ 的逆元是 A 的逆矩阵 A^{-1}. 当 $n > 1$ 时, $GL_n(\mathbf{R})$ 是一个非交换群. □

例 6 集合 $\{1, -1, \mathbf{i}, -\mathbf{i}\}$ 关于数的乘法构成交换群. □

例 7 全体 n 次单位根组成的集合

$$\begin{aligned} U_n &= \{x \in \mathbf{C} \mid x^n = 1\} \\ &= \left\{ \cos\frac{2k\pi}{n} + \mathbf{i}\sin\frac{2k\pi}{n} \;\middle|\; k = 0, 1, 2, \cdots, n-1 \right\} \end{aligned}$$

关于数的乘法构成一个 n 阶交换群.

事实上, 对任意的 $x, y \in U_n$, 因为 $x^n = 1, y^n = 1$, 所以

$$(xy)^n = x^n y^n = 1 \cdot 1 = 1.$$

因此 $xy \in U_n$. 因为数的乘法满足交换律和结合律, 所以 U_n 的乘法也满足交换律和结合律.

由于 $1 \in U_n$, 且对任意的 $x \in U_n$, $1 \cdot x = x \cdot 1 = x$, 所以 1 为 U_n 的单位元. 又由于对任意的 $x \in U_n$, 有 $x^{n-1} \in U_n$, 且

$$x \cdot x^{n-1} = x^{n-1} \cdot x = x^n = 1,$$

所以 x 有逆元 x^{n-1}. 因此, U_n 关于数的乘法构成一个群. 通常称这个群为 n **次单位根群**, 显然 U_n 是一个具有 n 个元素的交换群. □

例 8 设 m 是大于 1 的正整数, 则 $\mathbf{Z}_m$ 关于剩余类的加法构成加群. 这个群称为 $\mathbf{Z}$ 的**模** m **剩余类加群**.

证明: 由例 2 知, 剩余类的加法 "+" 是 $\mathbf{Z}_m$ 的代数运算.

(1) 对任意的 $\overline{a}, \overline{b}, \overline{c} \in \mathbf{Z}_m$,

$$\begin{aligned} (\overline{a} + \overline{b}) + \overline{c} &= \overline{a+b} + \overline{c} \\ &= \overline{(a+b)+c} \\ &= \overline{a+(b+c)} \\ &= \overline{a} + \overline{b+c} \\ &= \overline{a} + (\overline{b} + \overline{c}), \end{aligned}$$

所以结合律成立.

(2) 对任意的 $\overline{a}, \overline{b} \in \mathbf{Z}_m$,

$$\begin{aligned} \overline{a} + \overline{b} &= \overline{a+b} \\ &= \overline{b+a} \\ &= \overline{b} + \overline{a}, \end{aligned}$$

所以交换律成立.

(3) 对任意的 $\overline{a} \in \mathbf{Z}_m$,

$$\overline{a} + \overline{0} = \overline{a+0} = \overline{a},$$

且

$$\overline{0}+\overline{a}=\overline{0+a}=\overline{a},$$

所以 $\overline{0}$ 为 $\mathbf{Z}_m$ 的零元.

(4) 对任意的 $\overline{a}\in\mathbf{Z}_m$,

$$\overline{a}+\overline{-a}=\overline{a+(-a)}=\overline{0},$$

且

$$\overline{-a}+\overline{a}=\overline{(-a)+a}=\overline{0},$$

所以 $\overline{-a}$ 为 $\overline{a}$ 的负元.

从而知, $\mathbf{Z}_m$ 关于剩余类的加法构成加群. □

当 $m>1$ 时, $\mathbf{Z}_m$ 关于剩余类的乘法不构成群. 下面的例子说明, $\mathbf{Z}_m$ 的部分元素关于剩余类的乘法是可以构成群的.

例 9 设 m 是大于 1 的正整数, 记

$$U(m)=\{\overline{a}\in\mathbf{Z}_m \mid (a,m)=1\},$$

则 $U(m)$ 关于剩余类的乘法构成群.

证明: (1) 对任意的 $\overline{a},\overline{b}\in U(m)$, 有 $(a,m)=1$, $(b,m)=1$, 于是 $(ab,m)=1$, 从而 $\overline{ab}\in U(m)$. 所以剩余类的乘法 "$\cdot$" 是 $U(m)$ 的代数运算.

(2) 对任意的 $\overline{a},\overline{b},\overline{c}\in U(m)$,

$$\begin{aligned}(\overline{a}\cdot\overline{b})\cdot\overline{c}&=\overline{ab}\cdot\overline{c}\\&=\overline{(ab)c}\\&=\overline{a(bc)}\\&=\overline{a}\cdot\overline{bc}\\&=\overline{a}\cdot(\overline{b}\cdot\overline{c}),\end{aligned}$$

所以结合律成立.

(3) 因为 $(1,m)=1$, 从而 $\overline{1}\in\mathbf{Z}_m$, 且对任意的 $\overline{a}\in U(m)$,

$$\overline{a}\cdot\overline{1}=\overline{a\cdot 1}=\overline{a},$$

且

$$\overline{1}\cdot\overline{a}=\overline{1\cdot a}=\overline{a},$$

所以 $\overline{1}$ 为 $U(m)$ 的单位元.

(4) 对任意的 $\overline{a}\in U(m)$, 有 $(a,m)=1$, 由整数的性质可知, 存在 $u,v\in\mathbf{Z}$, 使

$$au+mv=1.$$

显然 $(u,m)=1$, 所以 $\overline{u}\in U(m)$, 且

$$\begin{aligned}\overline{a}\cdot\overline{u}&=\overline{au}\\&=\overline{au+mv}\qquad(\text{因为 } m\,|\,mv=(au+mv)-au)\\&=\overline{1},\\\overline{u}\cdot\overline{a}&=\overline{ua}=\overline{au}\\&=\overline{1},\end{aligned}$$

所以 $\overline{u}$ 为 $\overline{a}$ 的逆元. 从而知, $U(m)$ 的每个元素在 $U(m)$ 中都可逆.

这就证明了, $U(m)$ 关于剩余类的乘法构成群. $\square$

群 $(U(m),\cdot)$ 称为 $\mathbf{Z}$ 的**模** m **单位群**, 显然这是一个交换群. 当 p 为素数时, $U(p)$ 常记作 $\mathbf{Z}_p^*$. 易知,

$$\mathbf{Z}_p^*=\left\{\overline{1},\overline{2},\cdots,\overline{p-1}\right\}.$$

注: 由初等数论可知(参见[1]), $U(m)$ 的阶等于 $\phi(m)$, 这里 $\phi(m)$ 是欧拉函数. 如果

$$m=p_1^{r_1}p_2^{r_2}\cdots p_s^{r_s},$$

其中 $p_1,p_2,\cdots,p_s$ 为 m 的不同素因子, 那么

$$\begin{aligned}\phi(m)&=(p_1^{r_1}-p_1^{r_1-1})(p_2^{r_2}-p_2^{r_2-1})\cdots(p_s^{r_s}-p_s^{r_s-1})\\&=m\prod_{i=1}^{s}\left(1-\frac{1}{p_i}\right).\end{aligned}$$

例 10 具体写出 $\mathbf{Z}_5^*$ 中任意两个元素的乘积以及每一个元素的逆元素. 易知:

$$\mathbf{Z}_5^*=\left\{\overline{1},\overline{2},\overline{3},\overline{4}\right\}.$$

直接计算, 可得:

$$\begin{array}{cccc}1\cdot1=1 & 1\cdot2=2 & 1\cdot3=3 & 1\cdot4=4\\ 2\cdot1=2 & 2\cdot2=4 & 2\cdot3=1 & 2\cdot4=3\\ 3\cdot1=3 & 3\cdot2=1 & 3\cdot3=4 & 3\cdot4=2\\ 4\cdot1=4 & 4\cdot2=3 & 4\cdot3=2 & 4\cdot4=1\end{array}$$

表 2.1

在表 2.1 中, 我们把 $\overline{1},\overline{2},\overline{3},\overline{4}$ 简记为 $1,2,3,4$. 这在进行 $\mathbf{Z}_m$ 中的运算时是经常这样做的. 由表中很容易看出:

$$\overline{1}^{-1}=\overline{1},\quad \overline{2}^{-1}=\overline{3},\quad \overline{3}^{-1}=\overline{2},\quad \overline{4}^{-1}=\overline{4}.\quad\square$$

观察表 2.1, 我们发现可以把表 2.1 表示为更加简单的形式:

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

表 2.2

形如表 2.2 的表通常称为群的**乘法表** (*multiplication table*), 也称**群表** (*group table*) 或**凯莱表** (*Cayley table*). 人们常用群表来表述有限群的运算. 如下表所示:

$\circ$	e	$\cdots$	b	$\cdots$
e	e	$\cdots$	b	$\cdots$
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$
a	a	$\cdots$	$a\circ b$	$\cdots$
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$

在一个群表中, 表的左上角列出了群的运算符号 (有时省略), 表的最上面一行则依次列出群的所有元素 (通常单位元列在最前面), 表的最左列按同样的次序列出群的所有元素. 表中的其余部分则是最左列的元素和最上面一行的元素的乘积. 注意, 在乘积 $a \circ b$ 中, 左边的因子 a 总是左列上的元素, 右边的因子 b 总是最上面一行的元素. 由群表很容易确定一个元素的逆元素. 又如果一个群的群表是对称的, 则可以肯定, 这个群一定是交换群.

在对群有了初步的认识以后, 我们来讨论群的一些简单性质.

定理 2.1 *设 G 为群, 则有*

(1) *群 G 的单位元是惟一的;*

(2) *群 G 的每个元素的逆元是惟一的;*

(3) *对任意的 $a \in G$, 有 $(a^{-1})^{-1} = a$.*

(4) *对任意的 $a, b \in G$, 有 $(ab)^{-1} = b^{-1}a^{-1}$;*

(5) *在群中消去律成立. 即设 $a, b, c \in G$, 如果 $ab = ac$, 或 $ba = ca$, 则 $b = c$.*

证明: (1) 如果 e_1, e_2 都是 G 的单位元, 则

$$e_1 \cdot e_2 = e_2 \qquad (\text{因为 } e_1 \text{ 是 } G \text{ 的单位元})$$
$$e_1 \cdot e_2 = e_1 \qquad (\text{因为 } e_2 \text{ 是 } G \text{ 的单位元})$$

因此,

$$e_2 = e_1 \cdot e_2 = e_1,$$

所以单位元是惟一的.

(2) 设 b, c 都是 $a \in G$ 的逆元, 则

$$ab = ba = e, \quad ac = ca = e,$$

于是

$$\begin{aligned} c &= c \cdot e = c(ab) \\ &= (ca)b = e \cdot b \\ &= b. \end{aligned}$$

所以 a 的逆元是惟一的.

(3) 因为 a^{-1} 是 a 的逆元, 所以

$$a^{-1}a = aa^{-1} = e.$$

从而由逆元的定义知, a 是 a^{-1} 的逆元. 又由逆元的惟一性得

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

(4) 直接计算可得

$$(ab) \cdot (b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e,$$

及

$$(b^{-1}a^{-1}) \cdot (ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e,$$

从而由逆元的惟一性得

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

(5) 如果 $ab = ac$, 则

$$b = eb = (a^{-1}a)b = a^{-1}(ab) = a^{-1}(ac) = (a^{-1}a)c = ec = c.$$

同理可证另一消去律. □

定理 2.2 *设 G 是群, 那么对任意的 $a, b \in G$, 方程*

$$ax = b \quad 及 \quad ya = b$$

在 G 中都有惟一解.

证明: 取 $x = a^{-1}b$, 则

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

所以方程 $ax = b$ 有解 $x = a^{-1}b$.

又如 $x = c$ 为方程 $ax = b$ 的任一解, 即 $ac = b$, 则

$$c = ec = (a^{-1}a)c = a^{-1}(ac) = a^{-1}b.$$

这就证明了惟一性.

同理可证另一方程也有惟一解. □

群的定义中的结合律表明, 群中三个元素 a, b, c 的乘积与运算的顺序无关, 因此可以简单地写成: abc. 进一步可知, 在群 G 中, 任意 k 个元素 $a_1, a_2, \cdots, a_k$ 的乘积与运算的顺序无关, 因此可以写成 $a_1a_2\cdots a_k$.

据此, 我们可以定义群的元素的**方幂**:

对任意的正整数 n, 定义

$$a^n = \underbrace{a \cdot a \cdot \cdots \cdot a}_{n个\,a},$$

再约定

$$a^0 = e,$$

$$a^{-n} = (a^{-1})^n, \quad (n \text{ 为正整数})$$

则 a^n 对任意整数 n 都有意义, 并且不难证明: 对任意的 $a \in G$, $m, n \in \mathbf{Z}$, 有下列的**指数法则**:

(1) $a^n \cdot a^m = a^{n+m}$;

(2) $(a^n)^m = a^{nm}$;

(3) 如果 G 是交换群, 则 $(ab)^n = a^n b^n$.

如果群 G 不是交换群, 则

$$(ab)^n = a^n b^n$$

一般是不成立的.

当 G 是加群时, 元素的方幂则应改写为**倍数**:

$$na = \underbrace{a + a + \cdots + a}_{n个\,a},$$

$$0a = 0,$$

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

相应地, 指数法则变为**倍数法则**:

(1) $na+ma=(n+m)a$;

(2) $m(na)=(mn)a$;

(3) $n(a+b)=na+nb$.

因为加群是交换群, 所以 (3) 对加群总是成立的.

下面两个定理, 给出了判别一个非空集合关于所给的运算是否构成群的另一途径.

定理 2.3 *设 G 是一个具有代数运算的非空集合, 则 G 关于所给的运算构成群的充分必要条件是:*

(1) *G 的运算满足结合律;*

(2) *G 中有一个元素 e (称为 G 的左单位元), 使对任意的 $a\in G$, 有 $ea=a$.*

(3) *对 G 的每一个元素 a, 存在 $a'\in G$ (称为 a 的左逆元), 使 $a'a=e$. 这里 e 是 G 的左单位元.*

证明: (**必要性**) 由群的定义, 这是显然的.

(**充分性**) 只需证: e 是 G 的单位元, a' 是 a 的逆元即可.

设 $a\in G$, 由 (3) 知, 存在 $a'\in G$, 使

$$a'a=e.$$

又由 (3) 知, 存在 $a''\in G$, 使

$$a''a'=e.$$

于是

$$aa'=e(aa')=(a''a')(aa')=a''(a'a)a'=a''(ea')=a''a'=e,$$

且

$$ae=a(a'a)=(aa')a=e\cdot a=a.$$

又联系到条件 (2) 和 (3) 知, e 是 G 的单位元, a' 是 a 的逆元. 进而再由条件 (1) 知, G 为群. □

这个定理说明, 一个具有乘法运算的非空集合 G, 只要满足结合律, 有左单位元, 每个元素有左逆元, 就构成一个群.

同理可证, 一个具有乘法运算的非空集合 G, 如果满足结合律, 有右单位元, 且 G 中每个元素有右逆元, 则 G 构成群 (见习题 15).

定理 2.4 *设 G 是一个具有乘法运算且满足结合律的非空集合, 则 G 构成群的充分必要条件是: 对任意的 $a,b\in G$, 方程*

$$ax=b \quad 与 \quad ya=b$$

在 G 中有解.

证明: (**必要性**) 已证 (见定理 2.2).

(**充分性**) 任取 $b\in G$, 由条件知, $yb=b$ 有解, 设为 e, 则 $eb=b$. 又对任意的 $a\in G$, $bx=a$ 有解, 设为 c. 于是

$$ea=e(bc)=(eb)c=bc=a,$$

从而知 e 是 G 的左单位元.

其次, 对每个 $a \in G$, $ya = e$ 有解, 设为 a'. 于是

$$a'a = e.$$

从而知 a 有左逆元.

于是由定理 2.3 知, G 构成群. □

最后, 作为定理 2.4 的一个应用, 我们来证明:

例 11 设 G 是一个具有乘法运算的非空有限集合, 如果 G 满足结合律, 且两个消去律成立, 则 G 是一个群.

证明: 设

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

对任意的 $a, b \in G$, 考察 aa_i 与 aa_j. 如果 $aa_i = aa_j$, 则由左消去律得 $a_i = a_j$, 于是 $i = j$. 这说明, $aa_1, aa_2, \cdots, aa_n$ 是 G 中 n 个不同的元素. 因 $|G| = n$, 所以

$$\{aa_1, aa_2, \cdots, aa_n\} = G = \{a_1, a_2, \cdots, a_n\},$$

因 $b \in G$, 必存在 $a_i \in G$, 使 $aa_i = b$. 这说明, 方程 $ax = b$ 在 G 中有解. 同理可证, 方程 $ya = b$ 在 G 中也有解. 从而由定理 2.4 知, G 是群. □

要注意的是, 如果没有有限的条件, 一个具有代数运算的集合, 仅仅满足结合律和两个消去律, 并不一定构成群.

习题 1 − 2

1. 证明: 实数域 $\mathbf{R}$ 上全体 n 阶方阵的集合 $M_n(\mathbf{R})$, 关于矩阵的加法构成一个交换群.

2. 证明: 实数域 $\mathbf{R}$ 上全体 n 阶可逆方阵的集合 $GL_n(\mathbf{R})$ 关于矩阵的乘法构成群. 这个群称为 n 阶**一般线性群**.

3. 证明: 实数域 $\mathbf{R}$ 上全体 n 阶正交矩阵的集合 $O_n(\mathbf{R})$, 关于矩阵的乘法构成一个群. 这个群称为 n阶**正交群**.

4. 证明: 所有行列式等于 1 的 n 阶整数矩阵组成的集合 $SL_n(\mathbf{Z})$, 关于矩阵的乘法构成群.

5. 在整数集 $\mathbf{Z}$ 中, 规定运算"$\oplus$"如下:

$$a \oplus b = a + b - 2, \qquad \forall\, a, b \in \mathbf{Z}.$$

证明: $(\mathbf{Z}, \oplus)$ 构成群.

6. 分别写出下列各群的乘法表.

(1) 例 6 中的群;

(2) 群 U_7;

(3) 群 $\mathbf{Z}_7^*$;

(4) 群 $U(18)$.

7. 设 $G = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} \,\middle|\, a \in \mathbf{R}, a \neq 0 \right\}$. 证明 G 关于矩阵的乘法构成群.

8. 证明所有形如 2^m3^n 的有理数 $(m,n\in\mathbf{Z})$ 的集合关于数的乘法构成群.

9. 证明所有形如

$$\begin{pmatrix}1 & a & b\\ 0 & 1 & c\\ 0 & 0 & 1\end{pmatrix}$$

的 3×3 实矩阵关于矩阵的乘法构成一个群. 这个群以诺贝尔物理学奖获得者海森伯格 (Werner Heisenberg) 的名字命名, 称为**海森伯格群** (*Heisenberg group*).

10. 设 G 是群, $a_1,a_2,\cdots,a_r\in G$. 证明:

$$(a_1a_2\cdots a_r)^{-1}=a_r^{-1}a_{r-1}^{-1}\cdots a_1^{-1}.$$

11. 设 G 是群, $a,b\in G$. 证明: 如果 $ab=e$, 则 $ba=e$.

12. 设 G 是群. 证明: 如果对任意的 $x\in G$, 都有 $x^2=e$, 则 G 是一个交换群.

13. 设 G 是群. 证明: G 是交换群的充分必要条件是对任意的 $a,b\in G$, $(ab)^2=a^2b^2$.

14. 设 G 是一个具有乘法运算的非空有限集合. 证明, 如果 G 满足结合律, 有左单位元, 且右消去律成立, 则 G 是一个群.

15. 证明: 一个具有乘法运算的非空集合 G, 如果满足结合律, 有右单位元 (即有 $e\in G$, 使对任意的 $a\in G$, 有 $ae=a$). 且 G 中每个元素有右逆元 (即对每个 $a\in G$, 有 $a'\in G$, 使 $aa'=e$), 则 G 构成群.

16. 设 G 是有限群. 证明 G 中使 $x^3=e$ 的元素 x 的个数是奇数.

17.* 设 p,q 是不同的素数. 假设 H 是整数集的真子集, 且 H 关于加法是群, H 恰好包含集合 $\{p,p+q,pq,p^q,q^p\}$ 中的三个元素. 试确定以下各组元中哪一组是 H 中的这三个元素?

(A) pq, p^q, q^p; (B) p, $p+q$, pq;

(C) p, pq, p^q; (D) $p+q$, pq, p^q;

(E) p, p^q, q^p.

18.* 假设下表是一个群的乘法表. 试填出未列出的元.

	e	a	b	c	d
e	e	—	—	—	—
a	—	b	—	—	e
b	—	c	d	e	—
c	—	d	—	a	b
d	—	—	—	—	—

参考文献及阅读材料

[1] 潘承洞, 潘承彪 著. 初等数论. 北京: 北京大学出版社, 1998

[2] 中国大百科全书 • 数学. 北京, 上海: 中国大百科全书出版社, 1988

[3] 数学百科全书 (第二卷). 北京: 科学出版社, 1995

文献 [2] 和 [3] 中有关于群, 特别是群的起源及其发展的较详细的介绍. 文献 [3] 是根据苏联大百科全书出版社出版的, 由著名数学家维诺格拉多夫主编、

几百位数学家共同撰写的同名大型数学工具书, 经由中国数学会组织编译而成的巨著, 全书共有五卷.

群论的起源

群的概念在数学史上出现是在19世纪的上半叶, 但是其思想的萌芽在古希腊欧几里德(Euclid, 约公元前330—公元前275)的《几何原本》中就已经出现了. 此后, 群的概念以运动和变换作为基础潜在地形成. 到了19世纪后期, 它才正式出现, 不久就在整个数学中占有重要的地位, 成为现代数学的基础之一.

有意识地开辟通向群的概念的道路始于18世纪末, 当时, 拉格朗日 (J. L. Lagrange, 1736—1813), 范德蒙 (A. T. Vandermonde, 1735—1796), 鲁菲尼 (P. Ruffini, 1765—1822) 等试图求出高次代数方程的代数解法, 由于研究方程诸根之间的置换而注意到了群的概念. 基于这种思考方式, 阿贝尔(N. H. Abel, 1802—1829)证明了5次以上的一般的代数方程没有根式解. 而置换群与代数方程之间的关系的完全描述是由伽罗瓦(E. Galois, 1811—1832)在1830年左右作出的(现称为伽罗瓦理论), 这一工作后来在若尔当(C. Jordan, 1838—1921)的名著《置换和代数方程专论》中得到了很好的介绍和发展. 置换群是最终形成抽象群的第一个主要来源.

群的思想也以独立的方式产生于几何学. 19世纪中叶, 几何学的研究重点逐渐转移到研究几何图形的变换以及它们的分类上. 这种研究被麦比乌斯(A. Möbius, 1790—1868)广泛地进行. 以凯莱(A. Cayley, 1821—1895)为首的不变量理论的英国学派给出了几何学的更为系统的分类: 凯莱明确地使用了“群”这个术语. 这个发展的最后阶段是克莱因(C. F. Klein, 1849—1925)在1872年提出了的著名的“埃尔兰根纲领”, 他指出: 几何的分类可以通过变换群来实现.

数论是群的概念的第三个来源. 早在1761年, 欧拉(L. Euler, 1707—1783)就使用了同余式和它们分成的同余类, 这在群论的语言中就意味着把一个群分解成子群的陪集. 高斯(C. F. Gauss, 1777—1855)则研究了分圆方程, 并且实际上确定了它们的伽罗瓦群的子群. 戴德金(J. W. R. Dedekind, 1831—1916)于1858年和克罗内克(L. Kronecker, 1823—1891)于1870年在其代数数论的研究中也引入了有限交换群以至有限群.

到了19世纪80年代, 综合上述三个主要来源, 数学家们终于成功地概括出了抽象群论的公理系统, 并大约在1890年得到公认.