

定义 1.1 若代数系统 $\{G; \bullet\}$ 满足以下条件

(1)运算“ $\bullet$ ”满足结合律，即对于 G 中的任意元素 a, b, c , 有 $a \bullet (b \bullet c) = (a \bullet b) \bullet c$

(2)在 G 中存在左单位元 e , 即对属于集合 G 的任意 a , 有 $e \bullet a = a$

(3) G 中的任意元素有左逆元，

即对属于集合 G 的任意 a , 存在属于集合 G 的 b , 使得 $b \bullet a = e$,

则称 $\{G; \bullet\}$ 是群或称 G (关于运算“ $\bullet$ ”)是群，

一般地，如果没有特别说明，那么我们就认为群 G 是乘法群，

并简记 $a \bullet b$ 为 ab ,

但是，若群 G 的运算满足交换律($ab=ba$, 任意 a, b 属于群 G),

则称 G 是交换群或加法群，并用 $a+b$ 表示 $a \bullet b$,

定义 1.2 若群 G 是有限集合，则称 G 所含元素的个数为群 G 的阶，并记为 $|G|$

若 $|G|=n$, 则称 G 是 n 阶有限群，若群 G 是无限集合，则称 G 是无限群，

例 1.1 有理数集合 Q 关于数的加法运算是群，

整数集合 Z 关于数的加法运算是群

Z_n 关于加法运算是群， Z_n 中的左单位元为 $\overline{0}$ ，任意元素 $\overline{a}$ 的左逆元为 $\overline{n-a}$ ，

$M_n(R)$ 关于矩阵的加法运算是群， $M_n(R)$ 中的左单位元为零矩阵 O_n ，

任意元素 A 的左逆元为 $-A$ ，

$\{Q; +\}$, $\{Z; +\}$ 和 $\{M_n(R); +\}$ 都是无限交换群， $\{Z_n; +\}$ 是有限交换群，其阶为 n ，

常称 $\{Z; +\}$ 为整数加法群， $\{Q; +\}$ 为有理数加法群，

$\{Z_n; +\}$ 为(模 n 的)剩余类加法群，

例 1.2 试证明: 如果规定整数集合 Z 上的运算“ $\circ$ ”为 $a \circ b = a + b - 2$, 其中 a, b 属于 Z 则 Z 关于运算“ $\circ$ ”是群,

证: 首先, 因为 $a \circ b = a + b - 2$ 属于 Z , 所以“ $\circ$ ”是 Z 上的运算,

其次, 对属于 Z 的任意 a, b, c , 有

$$(a \circ b) \circ c = (a + b - 2) \circ c = a + b - 2 + c - 2 = a + (b + c - 2) - 2 = a + (b \circ c) - 2 = a \circ (b \circ c),$$

所以, “ $\circ$ ”满足结合律,

再次, Z 中有左单位元 e , 若 $a = e \circ a = e + a - 2$, 则 $e = 2$,

最后, 对属于 Z 的任意 a , 有左逆元 b , 若 $2 = e = b \circ a = b + a - 2$, 则 $b = 4 - a$,

至此, 根据群的定义可知, Z 关于运算“ $\circ$ ”是群,

根据群的定义，我们容易验证群 G 具有如下的一些简单性质：

(1)对属于群 G 的任意 a ，有 $ea=ae=a$ ，

证：根据群定义的条件(3)可知，

对属于群 G 的 a ，存在属于群 G 的 b ，使得 $ba=e$ ，

当然，也存在属于群 G 的 c ，使得 $cb=e$ ，

所以 $ae=e(ae)=(cb)(ae)=c(ba)e=c(ee)=c(ba)=ea=a$ ，

这就是说，群的左单位元也是右单位元，

(2)对属于群 G 的任意 a ，存在属于群 G 的 b ，使得 $ba=ab=e$ ，

证：根据群定义的条件(3)可知，

对属于群 G 的 a ，存在属于群 G 的 b ，使得 $ba=e$ ，

对于属于群 G 的 b ，存在属于群 G 的 c ，使得 $cb=e$ ，

所以 $ab=e(ab)=(cb)(ab)=c(ba)b=c(eb)=cb=e$ ，

这就是说，群的左逆元也是右逆元，

(3)群 G 中有唯一元素 e 满足：对属于群 G 的任意 a ，有 $ea=ae=a$

(称这样的元素 e 为 G 的单位元)，

证：设存在属于群 G 的 e' ，满足对属于群 G 的任意 a ，有 $e'a=ae'=a$ ，则 $e=ee'=e'$ ，

(4)对属于群 G 的任意 a ，群 G 中满足 $ab=ba=e$ 的元素 b 是唯一的，

证：设存在属于群 G 的 c ，也满足 $ac=ca=e$ ，则 $b=eb=(ca)b=c(ab)=ce=c$ ，

以后，我们称 a 是可逆元， b 是 a 的逆元，并记为 $b=a^{-1}$ ，

(5)对属于群 G 的任意 a, b ，有 $(a^{-1})^{-1}=a$ ， $(ab)^{-1}=b^{-1}a^{-1}$ ，

(6)群 G 满足消去律，即对任意 G 中元素 a, b, c ，如果 $ab=ac$ ，则 $b=c$ ；

如果 $ba=ca$ ，则 $b=c$ ，

至此，根据群的性质，我们易知群有如下等价定义，

定义 1.1' 若代数系统 $\{G; \bullet\}$ 满足以下条件：

(1)运算“ $\bullet$ ”满足结合律，即对属于群 G 的任意 a, b, c ，有 $a \bullet (b \bullet c) = (a \bullet b) \bullet c$ ；

(2) G 中有单位元素 e ，即对属于群 G 的任意 a ，有 $e \bullet a = a \bullet e = a$ ；

(3) G 中任意元素都有逆元，即对属于群 G 的任意 a ，存在属于群 G 的 b ，使得 $b \bullet a = a \bullet b = e$ ，

则称 G 关于运算“ $\bullet$ ”是群，

简单来说，所谓群就是满足运算封闭，结合律成立，存在单位元，

而且每个元素都有逆元等条件的集合，

但是，若代数系统 $\{G; \bullet\}$ 满足条件(1)，则称 G 是半群，

若代数系统 $\{G; \bullet\}$ 满足条件(1)和(2)，则称 G 是有单位元的半群，

例如，代数系统 $\{Q; \bullet\}, \{Z; \bullet\}, \{Z_n; \bullet\}$ 和 $\{M_n(R); \bullet\}$ 都是有单位元的半群，

定理 1.1 有限半群 G 为群的充分必要条件是在 G 中消去律成立，

证：必要性是已知的，下面来证充分性，

设 $G = \{a_1, a_2, \dots, a_n\}$ ，

因为在 G 中消去律成立，所以 $a_1a_1, a_2a_1, \dots, a_na_1$ 是 G 中 n 个不同元素，

进而， $\{a_1a_1, a_2a_1, \dots, a_na_1\} = G$ ，因此，存在属于群 G 的 a ，使得 $aa_1 = a_1$ ，

接下来我们说明 a 就是 G 的单位元，

同样地，根据 G 中消去律成立，我们有 $\{a_1a_1, a_1a_2, \dots, a_1a_n\} = G$

那么，对属于群 G 的任意 a_j ，存在属于群 G 的 b ，使得 $a_1b = a_j$

从而， $aa_j = a(a_1b) = (aa_1)b = a_1b = a_j$ ，即 a 是 G 的左单位元，

对属于群 G 的任意 a_j

因为 $\{a_1a_j, a_2a_j, \dots, a_na_j\} = G$ ，所以存在属于群 G 的 c ，使得 $ca_j = a$ ，

即 a_j 有左逆元 c

从而，由群的定义可知， G 是群，

以后我们将群 G 中元素 a 的幂定义为

$$a^n = \underbrace{aa \cdots a}_{n \text{ 个 } a}, (a^{-1})^n = a^{-n} = \underbrace{(a^{-1})(a^{-1}) \cdots (a^{-1})}_{n \text{ 个 } a^{-1}}$$

其中 n 是正整数，并规定 $a^0 = e$ ，

若 G 是交换群，则 G 的单位元又叫零元，逆元又叫负元，

在不引起混淆的情况下，将零元记作 0 ，而将元素 a 的负元记作 $-a$ ，

$$\text{并且记 } na = \underbrace{a+a+\cdots+a}_{n \text{ 个 } a}, -na = \underbrace{(-a)+(-a)+\cdots+(-a)}_{n \text{ 个 } a^{-1}}$$

其中 n 是正整数，规定 $0a = 0$ ，

下面我们来看几个常用群的例子，

例 1.3 非零有理数集合 Q^* 关于数的乘法运算是群，

$\{Q^*; \cdot\}$ 的单位元是数 1 ， $\{Q^*; \cdot\}$ 的每个元素 a 的逆元是数 a^{-1} ，

例 1.4 证明代数系统 $\{Z_p^*; \cdot\}$ 是交换群，这里 p 是素数， $Z_p^* = Z_p - \{\bar{0}\}$ ，

证：对属于 Z_p^* 的任意 $\bar{a}$ ，有 $\bar{1}\bar{a} = \bar{a}$ ，即 $\bar{1}$ 是 Z_p^* 的左单位元，

因为 $\bar{a}$ 属于 Z_p^* ，所以 a 与 p 互素，进而存在整数 s, t ，使得 $sa + tp = 1$ ，

因此 $\overline{sa} = \overline{sa} + \overline{tp} = \overline{sa + tp} = \bar{1}$ ，即 $\bar{a}$ 有左逆元，

另外，代数系统 Z_p^* 上的乘法运算满足结合律和交换律，因而 $\{Z_p^*; \cdot\}$ 是交换群

例 1.5 易知， $M_n(R)$ 的子集合 $CL_n(R) = \{A \in M_n(R) | \det(A) \neq 0\}$

关于矩阵的乘法运算是群，

一般地，我们称 $GL_n(R)$ 为实数域 R 上的 n 阶一般线性群，

另外，当 $n > 1$ 时， $GL_n(R)$ 不是交换群，

例如， $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ 与 $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ 不相等，

例 1.6 非空集合 A 上所有双变换构成的集合 S_A 关于变换的乘法运算构成群
称为集合 A 上的全变换群，

这个群的单位元是 A 上的恒等变换，每个变换的逆元是其逆变换，

特别地，当 A 是含 n 个元素的有限集合时，

A 上所有双变换构成的集合 S_n 关于变换的乘法运算构成的群称为 n 次对称群

当 $n \geq 3$ 时， S_n 不是交换群，

例 1.7 试求 $S_n(n \geq 3)$ 中的乘积 $(123)(12)$ 和 $(12)(123)$ ，

解：如下式

$$(123)(12) = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \downarrow & \downarrow & \downarrow & \cdots & \downarrow (12) \\ 2 & 1 & 3 & \cdots & n \\ \downarrow & \downarrow & \downarrow & \cdots & \downarrow (123) \\ 3 & 2 & 1 & \cdots & n \end{pmatrix}$$

知 $(123)(21)=(13)$ ，而 $(12)(123)=(12)(12)(23)=(23)$ ，

此例表明， $S_n(n \geq 3)$ 的乘法运算不满足交换律，即 $n \geq 3$ 时， S_n 不是交换群，

但是，当 $n \leq 2$ 时， S_n 是交换群，

例 1.8 证明 2, 3, 4 阶群一定是交换群，

证：

记 2 阶群为 $G=\{e, a\}$ ，则 G 显然是交换群，且 $a^2=e, a^{-1}=a$ ，

记 3 阶群为 $G=\{e, a, b\}$ ，则 ab 属于 G ，但是 $ab \neq a$ (否则 $b=e$)， $ab \neq b$ (否则 $a=e$)，

因此， $ab=e, b=a^{-1}$ ，即 3 阶群 $G=\{e, a, a^{-1}\}$ 是交换群，且 $a^2=a^{-1}, a^3=e$ ，

记 4 阶群为 $\{e, a, b, c\}$ ，则根据逆元的唯一性知，

表达式 $ab=e$ 和 $ac=e$ 至少有一个不成立，不妨设 $ab \neq e$ ，

事实上， ab 也不等于 a 或 b (否则，若 $ab=a$ 或 $ab=b$ ，则 $b=e$ 或 $a=e$ ，矛盾)，

因此， $ab=c$ ，同理可证 $ba=c$ ，所以 $G=\{e, a, b, ab=ba\}$ 是交换群，