信息安全的数学基础 (1)

唐　灯

上海交通大学网络空间安全学院

第二章 群

§2.1 群的定义和性质

- 群的定义
- 群的例子
- 群的性质
- 群的判定

定义 1

设 S 为集合. 我们称映射 $f: S\times S\to S,\ (a,b)\mapsto c$ 为集合 S 上的**一个代数运算或二元运算** (binary operation).

定义 1

设 S 为集合. 我们称映射 $f : S \times S \to S$, $(a, b) \mapsto c$ 为集合 S 上的一个**代数运算**或**二元运算** (binary operation).

注 1.1

集合 S 上的任意一个代数运算均具有唯一性和封闭性.

定义 1

设 S 为集合. 我们称映射 $f: S \times S \to S,\ (a,b) \mapsto c$ 为集合 S 上的**一个代数运算或二元运算** (binary operation).

注 1.1

集合 S 上的任意一个代数运算均具有唯一性和封闭性.

注 1.2

在数学应用中, 记号 $c = f(a,b)$ 并不是一个很适宜的记号. 实际上, 我们经常使用 "$\cdot$" 和 "$*$" 等符号来表示代数运算, 即

$$c = a \cdot b, a \times b, a * b, a + b, a \circ b \text{ 等}.$$

定义 2

集合 S 上的代数运算 “$\cdot$” 如果满足对任意 $a, b, c \in S$ 都有

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

则称该代数运算满足**结合律** (associative law). 如果对任意 $a, b \in S$ 都有

$$a \cdot b = b \cdot a,$$

则称其满足**交换律** (commutative law).

例

例 3

有理数的加法、减法和乘法都是有理数集 $\mathbb{Q}$ 上的代数运算, 但除法不是 $\mathbb{Q}$ 上的代数运算. 如果只考虑所有非零有理数的集合 $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, 则除法是 $\mathbb{Q}^*$ 上的代数运算.

例

例 3

有理数的加法、减法和乘法都是有理数集 $\mathbb{Q}$ 上的代数运算, 但除法不是 $\mathbb{Q}$ 上的代数运算. 如果只考虑所有非零有理数的集合 $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, 则除法是 $\mathbb{Q}^*$ 上的代数运算.

例 4

设 m 为大于 1 的正整数, $\mathbb{Z}_m$ 为 $\mathbb{Z}$ 的模 m 剩余类集. 对 $\bar{a}, \bar{b} \in \mathbb{Z}_m$, 规定

$$\bar{a} + \bar{b} = \overline{a+b}$$

$$\bar{a} \cdot \bar{b} = \overline{ab}$$

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

证明

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

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

则

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

证明

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

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

则

$$m\,\big|a-a',\quad m\big|\,b-b'.$$

于是

$$m\mid\left(a-a'\right)+\left(b-b'\right)=(a+b)-\left(a'+b'\right),$$

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

证明

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

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

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 “·” 都是 $\mathbb{Z}_m$ 上的代数运算.

群的定义

定义 5

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 $a \cdot b \in G$. 如果运算 “ $\cdot$ ” 满足下述三个条件:

群的定义

定义 5

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 $a \cdot b \in G$. 如果运算 “$\cdot$” 满足下述三个条件:

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

群的定义

定义 5

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 $a \cdot b \in G$. 如果运算 “ $\cdot$” 满足下述三个条件:

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

(2) G 中有单位元 (identity element) e，即对每个 $a \in G$，有 $e \cdot a = a \cdot e = a$;

群的定义

定义 5

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 $a \cdot b \in G$. 如果运算 “$\cdot$” 满足下述三个条件:

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

(2) G 中有单位元 (identity element) e, 即对每个 $a \in G$, 有 $e \cdot a = a \cdot e = a$;

(3) G 中每个元素 a 均有逆元 (inverse), 即存在元素 $b \in G$ 使得 $a \cdot b = b \cdot a = e$,

定义 5

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 $a \cdot b \in G$. 如果运算 “$\cdot$” 满足下述三个条件:

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

(2) G 中有单位元 (identity element) e, 即对每个 $a \in G$, 有 $e \cdot a = a \cdot e = a$;

(3) G 中每个元素 a 均有逆元 (inverse), 即存在元素 $b \in G$ 使得 $a \cdot b = b \cdot a = e$,

则称 G 关于运算 “$\cdot$” 构成一个群 (group), 记作 $(G, \cdot)$.

群的定义

定义 5

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 $a \cdot b \in G$. 如果运算 “ $\cdot$ ” 满足下述三个条件:

(1) 结合律成立, 即对所有的 $a, b, c \in G$, 有 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;
(2) G 中有单位元 (identity element) e, 即对每个 $a \in G$, 有 $e \cdot a = a \cdot e = a$;
(3) G 中每个元素 a 均有逆元 (inverse), 即存在元素 $b \in G$ 使得 $a \cdot b = b \cdot a = e$,

则称 G 关于运算 “ $\cdot$ ” 构成一个群 (group), 记作 $(G, \cdot)$.

注 5.1

(1) 如果群 $(G, \cdot)$ 仅满足结合律, 我们称之为半群; 如果 $(G, \cdot)$ 满足结合律且存在单位元, 我们称之为含幺半群.

群的定义

定义 5

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 $a \cdot b \in G$. 如果运算 “$\cdot$” 满足下述三个条件:

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

(2) G 中有单位元 (identity element) e, 即对每个 $a \in G$, 有 $e \cdot a = a \cdot e = a$;

(3) G 中每个元素 a 均有逆元 (inverse), 即存在元素 $b \in G$ 使得 $a \cdot b = b \cdot a = e$,

则称 G 关于运算 “$\cdot$” 构成一个群 (group), 记作 $(G, \cdot)$.

注 5.1

(1) 如果群 $(G, \cdot)$ 仅满足结合律, 我们称之为半群; 如果 $(G, \cdot)$ 满足结合律且存在单位元, 我们称之为含幺半群.

(2) 我们将证明群 G 的单位元 e 和每个元素的逆元都是唯一的. G 中元素 a 的唯一的逆元通常记作 a^{-1}.

群的阶

定义 6

群 $(G, \cdot)$ 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). 无限群的阶记为 ∞.

群的阶

定义 6

群 $(G, \cdot)$ 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). 无限群的阶记为 ∞.

定义 7

如果群 G 上的代数运算 "$\cdot$" 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).

注 7.1

(1) 我们通常用“$+$”法来表示阿贝尔群 G 的代数运算, 记为 $(G,+)$. 习惯上, 只有当一个群为交换群时, 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**.

注

注 7.1

(1) 我们通常用 “$+$” 法来表示阿贝尔群 G 的代数运算, 记为 $(G,+)$. 习惯上, 只有当一个群为交换群时, 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**.

(2) 我们通常将 $(G,+)$ 上的单位元记为 0, 并称 0 为 $(G,+)$ 的**零元**; 记 $(G,+)$ 中 a 的逆元为 $-a$, 并称 $-a$ 为 a 的**负元**.

注

注 7.1

(1) 我们通常用 "$+$" 法来表示阿贝尔群 G 的代数运算, 记为 $(G,+)$. 习惯上, 只有当一个群为交换群时, 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**.

(2) 我们通常将 $(G,+)$ 上的单位元记为 0, 并称 0 为 $(G,+)$ 的**零元**; 记 $(G,+)$ 中 a 的逆元为 $-a$, 并称 $-a$ 为 a 的**负元**.

(3) 将不是加群的群称为**乘群**, 并把乘群的代数运算叫做**乘法**, 运算的结果叫做**积**, 乘群的运算符号通常省略不写.

注 (续)

(4) 在不致引起混淆的情况下, 常将加群和乘群简称为群. 今后, 如不作特别声明, 总假定群的运算是乘法.

注 (续)

(4) 在不致引起混淆的情况下，常将加群和乘群简称为群. 今后，如不作特别声明，总假定群的运算是乘法.

(5) 在群 $(G,\cdot)$ 中，对任意的正整数 n 以及 $a\in G$，定义 a^n 表示 n 个 a 相乘，再约定 $a^0=e$ 以及 $a^{-n}=\left(a^{-1}\right)^n$，则 a^n 对任意整数 n 都有意义，且对任意 $m,n\in\mathbb{Z}$ 有 $a^n\cdot a^m=a^{n+m}$ 和 $(a^n)^m=a^{nm}$.

注 (续)

(4) 在不致引起混淆的情况下, 常将加群和乘群简称为群. 今后, 如不作特别声明, 总假定群的运算是乘法.

(5) 在群 $(G,\cdot)$ 中, 对任意的正整数 n 以及 $a \in G$, 定义 a^n 表示 n 个 a 相乘, 再约定 $a^0 = e$ 以及 $a^{-n} = \left(a^{-1}\right)^n$, 则 a^n 对任意整数 n 都有意义, 且对任意 $m, n \in \mathbb{Z}$ 有 $a^n \cdot a^m = a^{n+m}$ 和 $(a^n)^m = a^{nm}$. 在群 $(G,+)$ 中, 相应地定义 na 表示 n 个 a 相加, 再约定 $0a = 0$ 以及 $(-n)a = n(-a)$, 则 na 对任意整数 n 都有意义, 且对任意 $m, n \in \mathbb{Z}$ 有
$na + ma = (n+m)a$, $m(na) = mna$, 以及
$n(a+b) = na + nb$.

例

例 8

$\mathbb{Z}$ 关于数的加法运算构成阿贝尔群. 这个群称为整数加群.

例 8

$\mathbb{Z}$ 关于数的加法运算构成阿贝尔群. 这个群称为整数加群.

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

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

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

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

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

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

所以 $-a$ 是 a 的逆元, 从而 $\mathbb{Z}$ 关于 "+" 构成群, 显然这是一个阿贝尔群.

例

例 9

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ 关于数的加法运算都构成阿贝尔群, 0 为加法单位元; $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, 以及 $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ 关于数的乘法运算都构成阿贝尔群, 1 为乘法单位元.

例

例 9

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ 关于数的加法运算都构成阿贝尔群, 0 为加法单位元; $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, 以及 $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ 关于数的乘法运算都构成阿贝尔群, 1 为乘法单位元.

注 9.1

在上述例子中, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ 关于数的加法运算构成阿贝尔群, 而$\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$ 关于数的乘法运算亦构成阿贝尔群, 而且加法和乘法运算满足分配律, 即对 $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ 中任意三个元素 a, b, c 都有 $(a+b)c = ac + bc$. 这样的集合称为**域**. 域的定义将在第三章详细阐述, 在此之前, 我们常将 $\mathbb{Q}$ 称为**有理数域**, $\mathbb{R}$ 称为**实数域**, $\mathbb{C}$ 称为**复数域**.

例 10

实数域 $\mathbb{R}$ 上全体 n 阶方阵的集合 $\mathrm{M}_n(\mathbb{R})$ 关于矩阵的加法运算构成一个交换群.

例 10

实数域 $\mathbb{R}$ 上全体 n 阶方阵的集合 $\mathrm{M}_n(\mathbb{R})$ 关于矩阵的加法运算构成一个交换群.

例 11

集合 $\{1, -1, \mathrm{i}, -\mathrm{i}\}$ 关于数的乘法运算构成一个交换群.

例 12

全体 n 次单位根组成的集合

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

关于数的乘法运算构成一个 n 阶交换群.

例 12

全体 n 次单位根组成的集合

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

关于数的乘法运算构成一个 n 阶交换群.

证明: 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 $x \in U_n, x^{n-1} \in U_n$ 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, U_n 是一个具有 n 个元素的交换群.

例 13

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

剩余类加法群

例 13

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

证明: 由例 4 知, 剩余类的加法运算 "$+$" 是 $\mathbb{Z}_m$ 的代数运算.

例 13

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

证明: 由例 4 知, 剩余类的加法运算 “$+$” 是 $\mathbb{Z}_m$ 的代数运算. (1) 对任意的 $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m$,

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

所以结合律成立.

剩余类加法群

例 13

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

证明: 由例 4 知, 剩余类的加法运算 "+" 是 $\mathbb{Z}_m$ 的代数运算. (1) 对任意的 $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m$,

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

所以结合律成立.

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

$$\bar{a}+\bar{b} = \overline{a+b} = \overline{b+a} = \bar{b}+\bar{a},$$

所以交换律成立.

证明 (续)

(3) 对任意的 $\bar{a} \in \mathbb{Z}_m$,

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

$$\bar{0} + \bar{a} = \overline{0 + a} = \bar{a}.$$

所以 $\bar{0}$ 为 $\mathbb{Z}_m$ 的零元.

证明 (续)

(3) 对任意的 $\bar{a} \in \mathbb{Z}_m$,

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

$$\bar{0} + \bar{a} = \overline{0 + a} = \bar{a}.$$

所以 $\bar{0}$ 为 $\mathbb{Z}_m$ 的零元.

(4) 对任意的 $\bar{a} \in \mathbb{Z}_m$,

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

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

所以 $\overline{-a}$ 为 $\bar{a}$ 的负元.

于是, $\mathbb{Z}_m$ 关于剩余类的加法构成加群.

例 14

设 m 是大于 1 的正整数, 记

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

则 $U(m)$ 关于剩余类的乘法运算构成群.

剩余类乘法群

例 14

设 m 是大于 1 的正整数, 记

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

则 $U(m)$ 关于剩余类的乘法运算构成群.

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

例 14

设 m 是大于 1 的正整数, 记
$$U(m) = \{\bar{a} \in \mathbb{Z}_m \mid (a, m) = 1\},$$
则 $U(m)$ 关于剩余类的乘法运算构成群.

证明: (1) 对任意的 $\bar{a}, \bar{b} \in U(m)$, 有 $(a, m) = 1, (b, m) = 1$, 于是可得 $(ab, m) = 1$, 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 $\bar{a}, \bar{b}, \bar{c} \in U(m)$,
$$(\bar{a} \cdot \bar{b}) \cdot \bar{c} = \overline{ab} \cdot \bar{c} = \overline{(ab)c} = \overline{a(bc)}$$
$$= \bar{a} \cdot \overline{bc} = \bar{a} \cdot (\bar{b} \cdot \bar{c})$$
所以结合律成立.

证明 (续)

(3) 因为 $(1, m) = 1$, 从而 $\bar{1} \in U_m$, 且对任意的 $\bar{a} \in U(m)$,

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

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

所以 $\bar{1}$ 为 $U(m)$ 的单位元.

证明 (续)

(3) 因为 $(1,m)=1$, 从而 $\bar{1}\in U_m$, 且对任意的 $\bar{a}\in U(m)$,

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

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

所以 $\bar{1}$ 为 $U(m)$ 的单位元. (4) 对任意的 $\bar{a}\in U(m)$, 有 $(a,m)=1$. 由整除的性质可知, 存在 $u,v\in\mathbb{Z}$, 使

$$au+mv=1.$$

显然 $(u,m)=1$, 因此对任意 $t\in\mathbb{Z}$ 有 $(u+tm,m)=1$, 于是 $\bar{u}\in U(m)$.

证明 (续)

(3) 因为 $(1,m)=1$, 从而 $\bar{1}\in U_m$, 且对任意的 $\bar{a}\in U(m)$,

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

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

所以 $\bar{1}$ 为 $U(m)$ 的单位元. (4) 对任意的 $\bar{a}\in U(m)$, 有 $(a,m)=1$. 由整除的性质可知, 存在 $u,v\in\mathbb{Z}$, 使

$$au+mv=1.$$

显然 $(u,m)=1$, 因此对任意 $t\in\mathbb{Z}$ 有 $(u+tm,m)=1$, 于是 $\bar{u}\in U(m)$. 由于

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

证明 (续)

(3) 因为 $(1,m)=1$, 从而 $\bar{1}\in U_m$, 且对任意的 $\bar{a}\in U(m)$,

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

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

所以 $\bar{1}$ 为 $U(m)$ 的单位元. (4) 对任意的 $\bar{a}\in U(m)$, 有 $(a,m)=1$. 由整除的性质可知, 存在 $u,v\in\mathbb{Z}$, 使

$$au+mv=1.$$

显然 $(u,m)=1$, 因此对任意 $t\in\mathbb{Z}$ 有 $(u+tm,m)=1$, 于是 $\bar{u}\in U(m)$. 由于

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

类似可得 $\bar{u}\cdot\bar{a}=\overline{ua}=\overline{au}=\bar{1}$. 所以 $\bar{u}$ 为 $\bar{a}$ 的逆元. 从而知, $U(m)$ 的每个元素在 $U(m)$ 中都可逆.

注 14.1

群 $(U(m),\cdot)$ 也称为 $\mathbb{Z}$ 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 $\mathbb{Z}_p^*$. 易知 $\mathbb{Z}_p^*=\{\overline{1},\overline{2},\cdots,\overline{p-1}\}$.

注 14.1

群 $(U(m),\cdot)$ 也称为 $\mathbb{Z}$ 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 $\mathbb{Z}_p^*$. 易知 $\mathbb{Z}_p^* = \{\overline{1},\overline{2},\cdots,\overline{p-1}\}$.

例 15 (一般线性群)

全体 n 阶可逆方阵的集合 $\mathrm{GL}_n(\mathbb{R})$ 关于矩阵的乘法运算构成群, 群 $\mathrm{GL}_n(\mathbb{R})$ 中的单位元是单位矩阵 E_n, $A \in \mathrm{GL}_n(\mathbb{R})$ 的逆元是 A 的逆矩阵 A^{-1}. 当 $n > 1$ 时 $\mathrm{GL}_n(\mathbb{R})$ 不是一个阿贝尔群.

注 14.1

群 $(U(m),\cdot)$ 也称为 $\mathbb{Z}$ 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 $\mathbb{Z}_p^*$. 易知 $\mathbb{Z}_p^*=\{\overline{1},\overline{2},\cdots,\overline{p-1}\}$.

例 15 (一般线性群)

全体 n 阶可逆方阵的集合 $\mathrm{GL}_n(\mathbb{R})$ 关于矩阵的乘法运算构成群，群 $\mathrm{GL}_n(\mathbb{R})$ 中的单位元是单位矩阵 E_n，$A\in\mathrm{GL}_n(\mathbb{R})$ 的逆元是 A 的逆矩阵 A^{-1}. 当 $n>1$ 时 $\mathrm{GL}_n(\mathbb{R})$ 不是一个阿贝尔群.

例 16 (对称群)

设 A 为非空集合. A到自身的一个一一映射称为A 的一个置换 (permutation). 记 A 的所有置换构成的集合为 $S(A)$，则 $S(A)$ 在映射的复合作为乘法运算下是群，其单位元为恒等映射，我们称 $S(A)$ 为 A 的对称群 (symmetric group) 或置换群 (permutation group). 特别地，设 $A=\{1,2,\ldots,n\}$，记 $S_n=S(A)$，则 S_n 为 $\{1,\ldots,n\}$ 所有置换构成的集合. 容易验证 S_2 为阿贝尔群，S_n $(n\geqslant 3)$ 不是阿贝尔群.

定理 17

设 G 为群, 则有

(1) 群 G 的单位元是唯一的;

(2) 群 G 的每个元素的逆元是唯一的;

(3) 对任意的 $a \in G$, 有 $\left(a^{-1}\right)^{-1} = a$;

(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

$$\begin{aligned} e_1e_2 &= e_2, \quad &\text{(因为 } e_1 \text{ 是 } G \text{ 的单位元)} \\ e_1e_2 &= e_1, \quad &\text{(因为 } e_2 \text{ 是 } G \text{ 的单位元)} \end{aligned}$$

证明

(1) 如果 e_1, e_2 都是 G 的单位元, 则

$$\begin{aligned} e_1e_2 &= e_2, \quad (\text{因为 } e_1 \text{ 是 } G \text{ 的单位元}) \\ e_1e_2 &= e_1, \quad (\text{因为 } e_2 \text{ 是 } G \text{ 的单位元}) \end{aligned}$$

因此,

$$e_2 = e_1e_2 = e_1,$$

所以单位元是唯一的.

证明

(1) 如果 e_1, e_2 都是 G 的单位元, 则

$$\begin{aligned} e_1 e_2 &= e_2, \quad (\text{因为 } e_1 \text{ 是 } G \text{ 的单位元}) \\ e_1 e_2 &= e_1, \quad (\text{因为 } e_2 \text{ 是 } G \text{ 的单位元}) \end{aligned}$$

因此,

$$e_2 = e_1 e_2 = e_1,$$

所以单位元是唯一的. (2) 设 b, c 都是 $a \in G$ 的逆元, 则

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

证明

(1) 如果 e_1, e_2 都是 G 的单位元, 则

$$\begin{aligned} e_1e_2 &= e_2, \quad (\text{因为 } e_1 \text{ 是 } G \text{ 的单位元}) \\ e_1e_2 &= e_1, \quad (\text{因为 } e_2 \text{ 是 } G \text{ 的单位元}) \end{aligned}$$

因此,

$$e_2 = e_1e_2 = e_1,$$

所以单位元是唯一的. (2) 设 b, c 都是 $a \in G$ 的逆元, 则

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

于是

$$c = ce = c(ab) = (ca)b = eb = b,$$

所以 a 的逆元是唯一的.

证明

(1) 如果 e_1, e_2 都是 G 的单位元, 则

$$\begin{aligned} e_1e_2 &= e_2, \quad &(\text{因为 } e_1 \text{ 是 } G \text{ 的单位元}) \\ e_1e_2 &= e_1, \quad &(\text{因为 } e_2 \text{ 是 } G \text{ 的单位元}) \end{aligned}$$

因此,

$$e_2 = e_1e_2 = e_1,$$

所以单位元是唯一的. (2) 设 b, c 都是 $a \in G$ 的逆元, 则

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

于是

$$c = ce = c(ab) = (ca)b = eb = b,$$

所以 a 的逆元是唯一的. (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.

证明

(1) 如果 e_1, e_2 都是 G 的单位元, 则

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

因此,

$$e_2 = e_1 e_2 = e_1,$$

所以单位元是唯一的. (2) 设 b, c 都是 $a \in G$ 的逆元, 则

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

于是

$$c = ce = c(ab) = (ca)b = eb = b,$$

所以 a 的逆元是唯一的. (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. 又由逆元的唯一性得

$$\left(a^{-1}\right)^{-1} = a.$$

证明 (续)

(4) 直接计算可得

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

(4) 直接计算可得

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

及

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

(4) 直接计算可得

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

及

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

从而由逆元的唯一性得

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

证明 (续)

(4) 直接计算可得

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

及

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

从而由逆元的唯一性得

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

(5) 如果 $ab=ac$, 由于 a 的逆存在, 则两边同时乘以 a^{-1} 立即可得 $b=c$. 同理可证另一消去律.

定理 18

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), 使得对任意的 $a \in G$, 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) 使得 $a'a = e$. 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.

证明

必要性. 由群的定义, 这是显然的.

充分性.

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.

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. 对任意 $a \in G$, 由 (3) 知, 存在 $a' \in G$, 使得

$$a'a = e.$$

右边同乘 e 有

$$a'ae = ee = e = a'a.$$

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. 对任意 $a \in G$, 由 (3) 知, 存在 $a' \in G$, 使得

$$a'a = e.$$

右边同乘 e 有

$$a'ae = ee = e = a'a.$$

左边同乘 a' 的左逆 a'' 有

$$a''a'ae = a''a'a \Rightarrow eae = ea \Rightarrow ae = a,$$

即 e 也是右单位元.

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. 对任意 $a \in G$, 由 (3) 知, 存在 $a' \in G$, 使得

$$a'a = e.$$

右边同乘 e 有

$$a'ae = ee = e = a'a.$$

左边同乘 a' 的左逆 a'' 有

$$a''a'ae = a''a'a \Rightarrow eae = ea \Rightarrow ae = a,$$

即 e 也是右单位元.

现证明左逆也是右逆.

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. 对任意 $a \in G$, 由 (3) 知, 存在 $a' \in G$, 使得

$$a'a = e.$$

右边同乘 e 有

$$a'ae = ee = e = a'a.$$

左边同乘 a' 的左逆 a'' 有

$$a''a'ae = a''a'a \Rightarrow eae = ea \Rightarrow ae = a,$$

即 e 也是右单位元.

现证明左逆也是右逆. 注意到

$$a'\left(aa'\right) = \left(a'a\right)a' = ea' = a' = a'e,$$

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. 对任意 $a \in G$, 由 (3) 知, 存在 $a' \in G$, 使得

$$a'a = e.$$

右边同乘 e 有

$$a'ae = ee = e = a'a.$$

左边同乘 a' 的左逆 a'' 有

$$a''a'ae = a''a'a \Rightarrow eae = ea \Rightarrow ae = a,$$

即 e 也是右单位元.

现证明左逆也是右逆. 注意到

$$a'\left(aa'\right) = \left(a'a\right)a' = ea' = a' = a'e,$$

左边同乘 a' 的左逆 a'' 有

$$e\left(aa'\right) = ee \Rightarrow \left(aa'\right) = e.$$

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. 对任意 $a \in G$, 由 (3) 知, 存在 $a' \in G$, 使得

$$a'a = e.$$

右边同乘 e 有

$$a'ae = ee = e = a'a.$$

左边同乘 a' 的左逆 a'' 有

$$a''a'ae = a''a'a \Rightarrow eae = ea \Rightarrow ae = a,$$

即 e 也是右单位元.

现证明左逆也是右逆. 注意到

$$a'\left(aa'\right) = \left(a'a\right)a' = ea' = a' = a'e,$$

左边同乘 a' 的左逆 a'' 有

$$e\left(aa'\right) = ee \Rightarrow \left(aa'\right) = e.$$

进而再由条件 (1) 知 G 为群.

群的性质

定理 19

设 G 是一个具有乘法运算的非空有限集合, 如果 G 满足结合律且对两个消去律成立, 则 G 构成群.

定理 19

设 G 是一个具有乘法运算的非空有限集合, 如果 G 满足结合律且对两个消去律成立, 则 G 构成群.

证明: 不妨设集合 $G=\{a_1,a_2,\cdots,a_n\}$. 对任意 $b\in G$, 如果 $ba_i=ba_j$, 则由左消去律得 $a_i=a_j$, 于是 $i=j$.

定理 19

设 G 是一个具有乘法运算的非空有限集合，如果 G 满足结合律且对两个消去律成立，则 G 构成群.

证明: 不妨设集合 $G=\{a_1,a_2,\cdots,a_n\}$. 对任意 $b\in G$, 如果 $ba_i=ba_j$, 则由左消去律得 $a_i=a_j$, 于是 $i=j$. 这说明, $ba_1,ba_2,\cdots,ba_n$ 是 G 中 n 个互不相同的元素. 同理 $a_1b,a_2b,\cdots,a_nb$ 也是 G 中 n 个互不相同的元素.

定理 19

设 G 是一个具有乘法运算的非空有限集合, 如果 G 满足结合律且对两个消去律成立, 则 G 构成群.

证明: 不妨设集合 $G=\{a_1,a_2,\cdots,a_n\}$. 对任意 $b\in G$, 如果 $ba_i=ba_j$, 则由左消去律得 $a_i=a_j$, 于是 $i=j$. 这说明, $ba_1,ba_2,\cdots,ba_n$ 是 G 中 n 个互不相同的元素. 同理 $a_1b,a_2b,\cdots,a_nb$ 也是 G 中 n 个互不相同的元素. 因为 $|G|=n$, 所以

$$\{a_1b,a_2b,\cdots,a_nb\}=G=\{ba_1,ba_2,\cdots,ba_n\}.$$

定理 19

设 G 是一个具有乘法运算的非空有限集合, 如果 G 满足结合律且对两个消去律成立, 则 G 构成群.

证明: 不妨设集合 $G=\{a_1,a_2,\cdots,a_n\}$. 对任意 $b\in G$, 如果 $ba_i=ba_j$, 则由左消去律得 $a_i=a_j$, 于是 $i=j$. 这说明, $ba_1,ba_2,\cdots,ba_n$ 是 G 中 n 个互不相同的元素. 同理 $a_1b,a_2b,\cdots,a_nb$ 也是 G 中 n 个互不相同的元素. 因为 $|G|=n$, 所以

$$\{a_1b,a_2b,\cdots,a_nb\}=G=\{ba_1,ba_2,\cdots,ba_n\}.$$

由于 $b\in G$, 因此必存在 $a_i\in G$ 使得 $a_ib=b$. 对任意 $a\in G$, 则必存在 $a_j\in G$ 使得 $ba_j=a$.

定理 19

设 G 是一个具有乘法运算的非空有限集合，如果 G 满足结合律且对两个消去律成立，则 G 构成群.

证明: 不妨设集合 $G=\{a_1,a_2,\cdots,a_n\}$. 对任意 $b\in G$，如果 $ba_i=ba_j$，则由左消去律得 $a_i=a_j$，于是 $i=j$. 这说明，$ba_1,ba_2,\cdots,ba_n$ 是 G 中 n 个互不相同的元素. 同理 $a_1b,a_2b,\cdots,a_nb$ 也是 G 中 n 个互不相同的元素. 因为 $|G|=n$，所以

$$\{a_1b,a_2b,\cdots,a_nb\}=G=\{ba_1,ba_2,\cdots,ba_n\}.$$

由于 $b\in G$，因此必存在 $a_i\in G$ 使得 $a_ib=b$. 对任意 $a\in G$，则必存在 $a_j\in G$ 使得 $ba_j=a$. 于是 $a_ia=a_iba_j=(a_ib)a_j=ba_j=a$，因此 a_i 为 G 的左单位元.

定理 19

设 G 是一个具有乘法运算的非空有限集合, 如果 G 满足结合律且对两个消去律成立, 则 G 构成群.

证明: 不妨设集合 $G=\{a_1,a_2,\cdots,a_n\}$. 对任意 $b\in G$, 如果 $ba_i=ba_j$, 则由左消去律得 $a_i=a_j$, 于是 $i=j$. 这说明, $ba_1,ba_2,\cdots,ba_n$ 是 G 中 n 个互不相同的元素. 同理 $a_1b,a_2b,\cdots,a_nb$ 也是 G 中 n 个互不相同的元素. 因为 $|G|=n$, 所以

$$\{a_1b,a_2b,\cdots,a_nb\}=G=\{ba_1,ba_2,\cdots,ba_n\}.$$

由于 $b\in G$, 因此必存在 $a_i\in G$ 使得 $a_ib=b$. 对任意 $a\in G$, 则必存在 $a_j\in G$ 使得 $ba_j=a$. 于是 $a_ia=a_iba_j=(a_ib)a_j=ba_j=a$, 因此 a_i 为 G 的左单位元. 进一步, 对任意 $a\in G$, 注意到 $\{a_1a,a_2a,\cdots,a_na\}=G$, 从而存在 $a_l\in G$ 使得 $a_la=a_i$, 即 a 有左逆元.

定理 19

设 G 是一个具有乘法运算的非空有限集合, 如果 G 满足结合律且对两个消去律成立, 则 G 构成群.

证明: 不妨设集合 $G=\{a_1,a_2,\cdots,a_n\}$. 对任意 $b\in G$, 如果 $ba_i=ba_j$, 则由左消去律得 $a_i=a_j$, 于是 $i=j$. 这说明, $ba_1,ba_2,\cdots,ba_n$ 是 G 中 n 个互不相同的元素. 同理 $a_1b,a_2b,\cdots,a_nb$ 也是 G 中 n 个互不相同的元素. 因为 $|G|=n$, 所以

$$\{a_1b,a_2b,\cdots,a_nb\}=G=\{ba_1,ba_2,\cdots,ba_n\}.$$

由于 $b\in G$, 因此必存在 $a_i\in G$ 使得 $a_ib=b$. 对任意 $a\in G$, 则必存在 $a_j\in G$ 使得 $ba_j=a$. 于是 $a_ia=a_iba_j=(a_ib)a_j=ba_j=a$, 因此 a_i 为 G 的左单位元. 进一步, 对任意 $a\in G$, 注意到 $\{a_1a,a_2a,\cdots,a_na\}=G$, 从而存在 $a_l\in G$ 使得 $a_la=a_i$, 即 a 有左逆元. 于是由定理 18 知 G 为群.

§2.2 子群和生成元集

- 子群的定义
- 子群的性质
- 子群的条件
- 子群的判定
- 子群的交
- 生成元集
- 生成子群的特征

§2.1 群的定义和性质

- 群的定义
- 群的例子
- 群的性质
- 群的判定

子群的定义

定义 20 (子群的定义)

设 G 是一个群, H 是 G 的一个非空子集. 如果 H 关于 G 的运算也构成群, 则称 H 为 G 的一个**子群**, 记作 $H < G$.

子群的定义

定义 20 (子群的定义)

设 G 是一个群, H 是 G 的一个非空子集. 如果 H 关于 G 的运算也构成群, 则称 H 为 G 的一个**子群**, 记作 $H < G$.

注 20.1

(1) 对任意群 G, G 本身以及只含单位元 e 的子集 $H = \{e\}$ 是 G 的子群;

(2) $H = \{e\}$ 和 G 称为 G 的**平凡子群** *(trivial subgroup)*, 群 G 的其它子群称为 G 的**非平凡子群** *(nontrivial subgroup)*;

(2) 群 G 的不等于它自身的子群称为 G 的**真子群** *(proper subgroup)*.

例 21

设 m 是一个整数, 令

$$H = \{mz \mid z \in \mathbb{Z}\},$$

则 H 为整数加群 $\mathbb{Z}$ 的子群. 这个群称为由 m 所生成的子群, 常记作 $m\mathbb{Z}$ 或 $\langle m \rangle$.

例 21

设 m 是一个整数, 令

$$H=\{mz \mid z\in\mathbb{Z}\},$$

则 H 为整数加群 $\mathbb{Z}$ 的子群. 这个群称为由 m 所生成的子群, 常记作 $m\mathbb{Z}$ 或 $\langle m\rangle$.

证明: (1) 因为 $0=m\times 0\in H$, 所以 H 非空.

(2) 对任意的 $mx, my\in H$, 有 $mx+my=m(x+y)\in H$, 所以 H 关于 $\mathbb{Z}$ 的运算封闭.

(3) 因为结合律对 $\mathbb{Z}$ 成立, 所以对 H 也成立.

(4) 因为 $0\in H$ 且对任意的 $mx\in H$, $0+mx=mx+0=mx$, 所以 0 为 H 的零元.

(5) 对 $mx\in H$, 有 $-mx=m(-x)\in H$, 且 $(-mx)+mx=mx+(-mx)=0$, 所以 $-mx$ 为 mx 的负元.

从而由子群的定义知, $H<G$.

例 22

在 $\mathbb{Z}$ 关于模 m 的剩余类加群 $\mathbb{Z}_m$ 中, 令 $H = \{mz \mid z \in \mathbb{Z}\}$, 则 H 是 $\mathbb{Z}_m$ 的平凡子群.

例

例 22

在 $\mathbb{Z}$ 关于模 m 的剩余类加群 $\mathbb{Z}_m$ 中，令 $H = \{mz \mid z \in \mathbb{Z}\}$，则 H 是 $\mathbb{Z}_m$ 的平凡子群.

例 23

令 $\mathbb{R}^n$ 为实数域 $\mathbb{R}$ 上全体 n 维向量的集合关于向量的加法运算构成的群. 设 $A \in \mathrm{M}_n(\mathbb{R})$ ，令

$$H = \{X \in \mathbb{R}^n \mid AX = 0\},$$

则 H 为 $\mathbb{R}^n$ 的子群.

问题

(1) 在上面两个例中, 注意到 H 作为子群有单位元, 而 $\mathbb{Z}_m$ 和 $\mathbb{R}^n$ 也有单位元.

(2) H 中的元素 a 在 H 中有逆元, 而 a 又是 $\mathbb{Z}_m$ 和 $\mathbb{R}^n$ 的元素, 它在 $\mathbb{Z}_m$ 和 $\mathbb{R}^n$ 中也有逆元.

问题

(1) 在上面两个例中，注意到 H 作为子群有单位元，而 $\mathbb{Z}_m$ 和 $\mathbb{R}^n$ 也有单位元.
(2) H 中的元素 a 在 H 中有逆元，而 a 又是 $\mathbb{Z}_m$ 和 $\mathbb{R}^n$ 的元素，它在 $\mathbb{Z}_m$ 和 $\mathbb{R}^n$ 中也有逆元.

问: 子群的单位元以及逆元与 $\mathbb{Z}_m$ 和 $\mathbb{R}^n$ 的单位元以及逆元之间有何关系?

定理 24

设 G 为群, H 是 G 的子群, 则

(1) 群 G 的单位元 e 是 H 的单位元;

(2) 对任意的 $a \in H$, a 在 G 中的逆元 a^{-1} 就是 a 在 H 中的逆元.

定理 24

设 G 为群, H 是 G 的子群, 则

(1) 群 G 的单位元 e 是 H 的单位元;

(2) 对任意的 $a \in H$, a 在 G 中的逆元 a^{-1} 就是 a 在 H 中的逆元.

证明: (1) 以 e' 表示 H 的单位元, e' 当然也是 G 的元素, 则

$$e'e' = e' = e'e,$$

由定理 17 知群 G 有消去律, 于是 $e' = e$.

(2) 以 a' 表示 a 在 H 中的逆元, 则

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

同样由 G 的消去律得 $a' = a^{-1}$.

子群的判定

注 24.1 (子群判定条件)

由于群 G 的运算满足结合律, 所以结合律在 G 的任何关于 G 的运算封闭的非空子集 H 上都成立. 于是, 由群的定义知, 如果群 G 的非空子集 H 满足下列三个条件:

子群的判定

注 24.1 (子群判定条件)

由于群 G 的运算满足结合律, 所以结合律在 G 的任何关于 G 的运算封闭的非空子集 H 上都成立. 于是, 由群的定义知, 如果群 G 的非空子集 H 满足下列三个条件:

(1) H 在群 G 的运算下封闭;

注 24.1 (子群判定条件)

由于群 G 的运算满足结合律, 所以结合律在 G 的任何关于 G 的运算封闭的非空子集 H 上都成立. 于是, 由群的定义知, 如果群 G 的非空子集 H 满足下列三个条件:

(1) H 在群 G 的运算下封闭;

(2) H 包含 G 的单位元;

注 24.1 (子群判定条件)

由于群 G 的运算满足结合律, 所以结合律在 G 的任何关于 G 的运算封闭的非空子集 H 上都成立. 于是, 由群的定义知, 如果群 G 的非空子集 H 满足下列三个条件:

(1) H 在群 G 的运算下封闭;

(2) H 包含 G 的单位元;

(3) H 包含它的每个元素的逆元,

注 24.1 (子群判定条件)

由于群 G 的运算满足结合律, 所以结合律在 G 的任何关于 G 的运算封闭的非空子集 H 上都成立. 于是, 由群的定义知, 如果群 G 的非空子集 H 满足下列三个条件:

(1) H 在群 G 的运算下封闭;
(2) H 包含 G 的单位元;
(3) H 包含它的每个元素的逆元,

则 $H < G$.

子群的判定

定理 25

设 G 为群, H 是群 G 的非空子集, 则 H 成为群 G 的子群的充分必要条件是:

(1) 对任意 $a, b \in H$, 有 $ab \in H$;
(2) 对任意 $a \in H$, 有 $a^{-1} \in H$.

定理 25

设 G 为群, H 是群 G 的非空子集, 则 H 成为群 G 的子群的充分必要条件是:

(1) 对任意 $a, b \in H$, 有 $ab \in H$;
(2) 对任意 $a \in H$, 有 $a^{-1} \in H$.

证明: 必要性. 如果 $H < G$, 则条件 (1) 自然成立. 又由定理 24 知, 条件 (2) 也成立.

充分性. 由条件 (1) 知, G 的乘法是 H 的代数运算. 乘法结合律对 G 的所有元素都成立, 自然对 H 的元素也成立. 由条件 (1) 知 H 关于 G 的运算封闭. 对任意的 $a \in H$, 由条件 (2) 知 $a^{-1} \in H$, 再由条件 (1) 得 $e = a^{-1}a \in H$. 由条件 (2) 知对任意 $a \in H$ 有 $a^{-1} \in H$. 则由注 24.1 立即可得 $H < G$.

子群的判定

定理 26 (子群判定定理)

设 G 为群, H 是群 G 的非空子集, 则 H 成为 G 的子群的充分必要条件是对任意的 $a, b \in H$, 有 $ab^{-1} \in H$.

子群的判定

定理 26 (子群判定定理)

设 G 为群, H 是群 G 的非空子集, 则 H 成为 G 的子群的充分必要条件是对任意的 $a, b \in H$, 有 $ab^{-1} \in H$.

证明: 必要性. 设 H 是 G 的子群, 则对任意的 $b \in H$, 有 $b^{-1} \in H$. 又对任意的 $a \in H$, 因 H 关于 G 的运算封闭, 所以 $ab^{-1} \in H$.

充分性. 由于 H 非空, 任取 $a \in H$. 则可得 $aa^{-1} = e \in H$. 注意到 H 包含 e, a, 则有 $ea^{-1} = a^{-1} \in H$. 最后, 对任意 $a, b \in H$, 已证 $a^{-1}, b^{-1} \in H$, 于是可得 $ab = a(b^{-1})^{-1} \in H$. 由定理 25 可得 H 是 G 的子群.

有限群的子群判定

定理 27

设 G 为一有限群, H 是群 G 的非空子集, 则 H 成为 G 的子群的充分必要条件是对任意的 $a, b \in H$, 有 $ab \in H$.

定理 27

设 G 为一有限群, H 是群 G 的非空子集, 则 H 成为 G 的子群的充分必要条件是对任意的 $a, b \in H$, 有 $ab \in H$.

证明: 必要性显然.

充分性. 根据定理 25, 只需证明对任意 $a \in H$ 有 $a^{-1} \in H$ 即可. 如果 $a = e \in H$, 则显然 $a^{-1} = e \in H$. 如果 $e \neq a \in H$, 则元素 $a, a^2, a^3, \cdots$ 都应在 H 中. 由于 G 有限, 故 H 有限, 因此必存在 $1 \leq i < j$ 使得 $a^i = a^j$, 从而 $e = a^{j-i} = a \cdot a^{j-i-1}$ (其中 $j - i > 1$, 否则 $a = e$), 于是 $a^{j-i-1} = a^{-1} \in H$.

例

例 28

$\mathrm{GL}_n(\mathbb{R})$ 表示所有 n 阶可逆实矩阵关于矩阵的乘法构成的群. 记

$$\mathrm{SL}_n(\mathbb{R}) = \{A \in \mathrm{M}_n(\mathbb{R}) \mid \det(A) = 1\},$$

则 $\mathrm{SL}_n(\mathbb{R})$ 是 $\mathrm{GL}_n(\mathbb{R})$ 的子群. $\mathrm{SL}_n(\mathbb{R})$ 称为**特殊线性群** (special linear group).

例 28

$GL_n(\mathbb{R})$ 表示所有 n 阶可逆实矩阵关于矩阵的乘法构成的群. 记

$$\mathrm{SL}_n(\mathbb{R})=\{A\in \mathrm{M}_n(\mathbb{R})\mid \det(A)=1\},$$

则 $\mathrm{SL}_n(\mathbb{R})$ 是 $\mathrm{GL}_n(\mathbb{R})$ 的子群. $\mathrm{SL}_n(\mathbb{R})$ 称为**特殊线性群** (special linear group).

证明: (1) 显然, 对单位方阵 $E_n\in \mathrm{M}_n(\mathbb{R})$, 有 $\det(E_n)=1$, 故 $E_n\in \mathrm{SL}_n(\mathbb{R})$. 且对每个 $A\in \mathrm{SL}_n(\mathbb{R})$, 由于 $\det(A)=1$, 故 A 可逆, 从而 $A\in \mathrm{GL}_n(\mathbb{R})$, 所以 $\mathrm{SL}_n(\mathbb{R})$ 是 $\mathrm{GL}_n(\mathbb{R})$ 的非空子集.

(2) 对任意的 $A,B\in \mathrm{SL}_n(\mathbb{R}),\det(A)=\det(B)=1$, 于是 B 可逆, $AB^{-1}\in M_n(\mathbb{R})$. 且

$$\det\left(AB^{-1}\right)=\det(A)\cdot\det(B)^{-1}=1\cdot 1^{-1}=1,$$

所以 $AB^{-1}\in \mathrm{SL}_n(\mathbb{R})$.

从而由定理 26 可知 $\mathrm{SL}_n(\mathbb{R})$ 是 $\mathrm{GL}_n(\mathbb{R})$ 的子群.

练习

例 29

设乘群 $G = \mathbb{Z}_7^*$, 令 $H = \{1, 2, 4\} \subseteq G$, 则 H 是 $\mathbb{Z}_7^*$ 的子群.

子群的交

定理 30

群 G 的任意两个子群的交集还是 G 的子群.

定理 30

群 G 的任意两个子群的交集还是 G 的子群.

证明: 设 H_1, H_2 是群 G 的两个子群.

子群的交

定理 30

群 G 的任意两个子群的交集还是 G 的子群.

证明: 设 H_1, H_2 是群 G 的两个子群.

(1) 因 G 的单位元 $e \in H_1 \cap H_2$, 所以 $H_1 \cap H_2$ 是 G 的非空子集.

定理 30

群 G 的任意两个子群的交集还是 G 的子群.

证明: 设 H_1, H_2 是群 G 的两个子群.

(1) 因 G 的单位元 $e \in H_1 \cap H_2$, 所以 $H_1 \cap H_2$ 是 G 的非空子集.

(2) 对任意 $a, b \in H_1 \cap H_2$, 有 $a, b \in H_1, a, b \in H_2$, 而 H_1, H_2 都是 G 的子群, 所以 $ab^{-1} \in H_1, ab^{-1} \in H_2$.

子群的交

定理 30

群 G 的任意两个子群的交集还是 G 的子群.

证明: 设 H_1, H_2 是群 G 的两个子群.

(1) 因 G 的单位元 $e \in H_1 \cap H_2$, 所以 $H_1 \cap H_2$ 是 G 的非空子集.

(2) 对任意 $a, b \in H_1 \cap H_2$, 有 $a, b \in H_1, a, b \in H_2$, 而 H_1, H_2 都是 G 的子群, 所以 $ab^{-1} \in H_1, ab^{-1} \in H_2$. 于是 $ab^{-1} \in H_1 \cap H_2$, 从而由定理 26 知 $H_1 \cap H_2$ 是 G 的子群.

定理 30

群 G 的任意两个子群的交集还是 G 的子群.

证明: 设 H_1, H_2 是群 G 的两个子群.

(1) 因 G 的单位元 $e \in H_1 \cap H_2$, 所以 $H_1 \cap H_2$ 是 G 的非空子集.

(2) 对任意 $a, b \in H_1 \cap H_2$, 有 $a, b \in H_1, a, b \in H_2$, 而 H_1, H_2 都是 G 的子群, 所以 $ab^{-1} \in H_1, ab^{-1} \in H_2$. 于是 $ab^{-1} \in H_1 \cap H_2$, 从而由定理 26 知 $H_1 \cap H_2$ 是 G 的子群.

注 30.1

群 G 的两个子群的并集不一定是 G 的子群. 例如在整数加群 $\mathbb{Z}$ 中, 令 $H_1 = \{2z \mid z \in \mathbb{Z}\}$, $H_2 = \{3z \mid z \in \mathbb{Z}\}$, 则易验证 $H_1, H_2 < \mathbb{Z}$, 但是 $2 + 3 \notin H_1 \cup H_2$.

子群的交

定理 31

设 S 是群 G 的一个非空子集, 令 M 表示 G 中所有包含 S 的子群所组成的集合, 即

$$M = \{H < G \mid S \subseteq H\},$$

令

$$K = \bigcap_{H \in M} H,$$

则 K 是 G 的子群.

生成元集

定义 32

设 S 是群 G 的一个非空子集, $M=\{H<G\mid S\subseteq H\}$, $K=\bigcap_{H\in M}H$, 称 K 为群 G 的由子集 S 所生成的子群, 简称**生成子群**, 记作 $\langle S\rangle$, 即

$$\langle S\rangle=\bigcap_{S\subseteq H<G}H.$$

子集 S 称为 $\langle S\rangle$ 的**生成元集**或**生成元组**. 如果 $S=\{a_1,a_2,\cdots,a_r\}$ 为有限集, 则记

$$\langle S\rangle=\langle a_1,a_2,\cdots,a_r\rangle.$$

生成子群的特征

定理 33

设 S 是群 G 的一个非空子集, 则

(1) $\langle S\rangle$ 是 G 的包含 S 的最小子群;

(2) $\langle S\rangle = \left\{a_1^{l_1}a_2^{l_2}\cdots a_k^{l_k} \mid a_i \in S, l_i = \pm 1, k \in \mathbb{N}\right\}$.

生成子群的特征

定理 33

设 S 是群 G 的一个非空子集, 则

(1) $\langle S\rangle$ 是 G 的包含 S 的最小子群;

(2) $\langle S\rangle = \left\{a_1^{l_1}a_2^{l_2}\cdots a_k^{l_k} \mid a_i \in S, l_i = \pm 1, k \in \mathbb{N}\right\}$.

证明: (1) 设 H 是 G 的任一子群. 如果 $S \subseteq H$, 由于 $\langle S\rangle$ 是 G 的所有包含 S 的子群的交, 所以 $\langle S\rangle \subseteq H$, 且 $S \subseteq \langle S\rangle$. 这就证明了 (1).

生成子群的特征

定理 33

设 S 是群 G 的一个非空子集, 则

(1) $\langle S\rangle$ 是 G 的包含 S 的最小子群;

(2) $\langle S\rangle = \left\{a_1^{l_1}a_2^{l_2}\cdots a_k^{l_k} \mid a_i \in S, l_i = \pm 1, k \in \mathbb{N}\right\}$.

证明: (1) 设 H 是 G 的任一子群. 如果 $S \subseteq H$, 由于 $\langle S\rangle$ 是 G 的所有包含 S 的子群的交, 所以 $\langle S\rangle \subseteq H$, 且 $S \subseteq \langle S\rangle$. 这就证明了 (1).

(2) $\langle S\rangle$ 是包含 S 的子群, 所以对任意的 $a \in S, a^{-1} \in \langle S\rangle$. 从而对任意的 $a_i \in S$ 及任意的 $l_i = \pm 1$ $(i = 1, 2, \cdots, k)$,

$$a_1^{l_1}a_2^{l_2}\cdots a_k^{l_k} \in \langle S\rangle.$$

令

$$T = \left\{ a_1^{l_1} a_2^{l_2} \cdots a_k^{l_k} \mid a_i \in S, l_i = \pm 1, k \in \mathbb{N} \right\},$$

则 $T \subseteq \langle S \rangle$.

证明 (续)

令

$$T = \left\{ a_1^{l_1} a_2^{l_2} \cdots a_k^{l_k} \mid a_i \in S, l_i = \pm 1, k \in \mathbb{N} \right\},$$

则 $T \subseteq \langle S \rangle$. 现证, $T = \langle S \rangle$.

证明 (续)

令

$$T=\left\{a_1^{l_1}a_2^{l_2}\cdots a_k^{l_k}\mid a_i\in S, l_i=\pm 1, k\in\mathbb{N}\right\},$$

则 $T\subseteq\langle S\rangle$. 现证, $T=\langle S\rangle$. 因为形式为

$$a_1^{l_1}a_2^{l_2}\cdots a_k^{l_k}$$

的元素的乘积仍为这一形式, 所以 T 对乘法封闭. 又每个这种形式的元素的逆也是这种形式的元素, 所以 T 中每个元素的逆元仍在 T 中, 从而 T 是 G 的子群.

令

$$T=\left\{a_1^{l_1}a_2^{l_2}\cdots a_k^{l_k} \mid a_i\in S, l_i=\pm 1, k\in\mathbb{N}\right\},$$

则 $T\subseteq\langle S\rangle$. 现证, $T=\langle S\rangle$. 因为形式为

$$a_1^{l_1}a_2^{l_2}\cdots a_k^{l_k}$$

的元素的乘积仍为这一形式, 所以 T 对乘法封闭. 又每个这种形式的元素的逆也是这种形式的元素, 所以 T 中每个元素的逆元仍在 T 中, 从而 T 是 G 的子群. 又因为显然有 $S\subseteq T$, 所以又得 $\langle S\rangle\subseteq T$. 于是 $\langle S\rangle=T$. 从而 (2) 得证.

例 34

当 S 只包含群 G 的一个元素 a 时, 由于

$$a^{l_1}a^{l_2}\cdots a^{l_k}=a^{\sum_{i=1}^{k} l_i},$$

所以

$$\langle a\rangle=\{a^r \mid r\in\mathbb{Z}\}.$$

这种由一个元素 a 生成的子群称为由 a 生成的**循环群** (cyclic group).

例 34

当 S 只包含群 G 的一个元素 a 时, 由于

$$a^{l_1}a^{l_2}\cdots a^{l_k}=a^{\sum_{i=1}^{k}l_i},$$

所以

$$\langle a\rangle=\{a^r \mid r\in\mathbb{Z}\}.$$

这种由一个元素 a 生成的子群称为由 a 生成的**循环群** (cyclic group).

注 34.1

若 G 为有限群, 则对任意 $e\neq a\in G$ 集合 $S=\{a,a^2,a^3,\cdots\}$ 是 G 的一个循环子群. 事实上, 由于 G 有限, 故该集合有限, 因此必存在 $1\leq i<j$ 使得 $a^i=a^j$, 从而 $e=a^{j-i}=a\cdot a^{j-i-1}\in S$ $(j-i>1)$, $a^{-1}=a^{j-i-1}\in S$, 从而 $(a^t)^{-1}=(a^{j-i-1})^t\in S$, 由定理 *25* 可知 S 为 G 的一个子群. 循环群是公钥密码协议和对称密码理论的基础, 其具体性质和结构将在本章第 *6* 节详细叙述.

例 35

若 $S=\{a,b\}$ 是群 G 的一个子集且 $ab=ba$, 则

$$\langle a,b\rangle=\{a^m b^n \mid m,n\in\mathbb{Z}\}.$$

例 35

若 $S=\{a,b\}$ 是群 G 的一个子集且 $ab=ba$, 则

$$\langle a,b\rangle=\{a^m b^n \mid m,n\in\mathbb{Z}\}.$$

例 36

若 $S=\{a,b\}$ 是群 G 的一个子集且 a,b 满足关系 $a^2=b^3=e$ 和 $ba=ab^2$. 试列出群 $\langle a,b\rangle$ 的所有元素.

解

由 $a^2=b^3=e$ 得

$$a^{-1}=a,\quad b^{-1}=b^2.$$

从而由定理 33 知, $\langle a,b\rangle$ 中的每个元素都是一些形如

$$a^k,\ b^l\ (k=0,1;l=0,1,2)$$

的元素的乘积. 由 $ba=ab^2$ 可得

$$b^k a=ab^{2k},$$

所以对每一个由 a^{k_i} 与 b^{l_j} 所组成的乘式, 总可以连续地应用 $ba=ab^2$, 最终将所有的因子 a^{k_i} 移至乘式的左端, 而把因子 b^{l_j} 置于乘式的右端. 所以

$$\langle a,b\rangle=\left\{a^k b^l \mid k,l\in\mathbb{N}\cup\{0\}\right\}.$$

再应用关系 $a^2=b^3=e$ 得

$$\langle a,b\rangle=\left\{e,a,b,b^2,ab,ab^2\right\}.$$

作业

- Page 25: 3-9; 17; 22 (乘法表定义见 Page 11).

§2.3 陪集和陪集分解

- 群中集合的乘积
- 子群的乘积
- 子群的陪集
- 陪集的指数
- 元素的阶

§2.2 子群和生成元集

- 子群的定义
- 子群的性质
- 子群的条件
- 子群的判定
- 子群的交
- 生成元集
- 生成子群的特征

群中集合的乘积

定义 37

设 A 与 B 是乘群 G 的两个非空子集, 称集合
$$AB = \{ab \mid a \in A, b \in B\}$$
为群的子集 A 与 B 的**乘积** (product). 对任意 $g \in G$, 如果 $A = \{g\}$, 则 AB 与 BA 分别简记为 gB 和 Bg.

群中集合的乘积

定义 37

设 A 与 B 是乘群 G 的两个非空子集，称集合
$$AB = \{ab \mid a \in A, b \in B\}$$
为群的子集 A 与 B 的**乘积** (product). 对任意 $g \in G$, 如果 $A = \{g\}$, 则 AB 与 BA 分别简记为 gB 和 Bg.

注 37.1

(1) 当 G 为加群时，上述记号应相应地改为
$$A + B = \{a + b \mid a \in A, b \in B\},$$
$$g + A = \{g + a \mid a \in A\},$$
$$A + g = \{a + g \mid a \in A\},$$
并称 $A + B$ 为 A 与 B 的**和** (*sum*). 显然有
$$A + B = B + A, \quad g + A = A + g.$$

(2) 设 A, B, C 是群 G 的非空子集. 若 G 不是阿贝尔群时，通常不能推出 $AB = BA$; 若有 $AB = AC$, 通常不能推出 $B = C$.

定理 38

设 A, B, C 是群 G 的任意三个非空子集, g 是群 G 的任一元素. 则有

(1) $A(BC) = (AB)C$;

(2) $eA = A$, 其中 e 是 G 的单位元;

(3) 如果 $gA = gB$ 或 $Ag = Bg$, 则 $A = B$.

证明

(1) 对任意的 $x \in A(BC)$, 存在 $a \in A, b \in B, c \in C$, 使 $x = a(bc)$. 而 $x = a(bc) = abc = (ab)c \in (AB)C$, 于是 $A(BC) \subseteq (AB)C$. 同理可证, $(AB)C \subseteq A(BC)$. 所以 $A(BC) = (AB)C$.

(2) 对任意 $a \in eA$, 存在 $a' \in A$ 使得 $ea' = a$. 由于 $a = ea' = a' \in A$, 因此 $eA \subseteq A$. 另一方面, 对任意 $a' \in A$ 有 $a' = ea' \in eA$, 因此 $A \subseteq eA$. 由此可得 $eA = A$.

(3) 如果 $gA = gB$, 由 (2) 有 $A = eA = g^{-1}gA = g^{-1}gB = B$. 同理可证另一等式.

子群的乘积

定理 39

设 G 是群, H, K 是 G 的任意两个子群. 则

(1) $HH = H$;

(2) $HK < G \Longleftrightarrow HK = KH$.

子群的乘积

定理 39

设 G 是群, H, K 是 G 的任意两个子群. 则

(1) $HH = H$;

(2) $HK < G \Longleftrightarrow HK = KH$.

证明: (1) 如果 H 是群 G 的子群, 则对任意的 $g, h \in H$, $gh \in H$, 从而 $HH \subseteq H$. 另一方面, 由定理 38 第 (2) 条可得 $H = eH \subseteq HH$. 所以 $HH = H$.

定理 39

设 G 是群, H, K 是 G 的任意两个子群. 则

(1) $HH = H$;

(2) $HK < G \Longleftrightarrow HK = KH$.

证明: (1) 如果 H 是群 G 的子群, 则对任意的 $g, h \in H$, $gh \in H$, 从而 $HH \subseteq H$. 另一方面, 由定理 38 第 (2) 条可得 $H = eH \subseteq HH$. 所以 $HH = H$. (2) **必要性** 设 HK 为 G 的子群. 对任意的 $hk \in HK$, 其中 $h \in H, k \in K$, 则有 $(hk)^{-1} \in HK$. 因而存在 $h_1 \in H$, $k_1 \in K$, 使 $h_1k_1 = (hk)^{-1}$. 从而

$$hk = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH,$$

所以

$$HK \subseteq KH.$$

反之, 对任意的 $kh \in KH$, 其中 $k \in K, h \in H$, 有 $(kh)^{-1} = h^{-1}k^{-1} \in HK$, 因此 $(h^{-1}k^{-1})^{-1} \in HK$. 于是

$$kh = \left(h^{-1}k^{-1}\right)^{-1} \in HK,$$

所以

$$KH \subseteq HK.$$

这就证明了 $HK = KH$.

证明 (续)

反之, 对任意的 $kh \in KH$, 其中 $k \in K, h \in H$, 有 $(kh)^{-1} = h^{-1}k^{-1} \in HK$, 因此 $(h^{-1}k^{-1})^{-1} \in HK$. 于是

$$kh = \left(h^{-1}k^{-1}\right)^{-1} \in HK,$$

所以

$$KH \subseteq HK.$$

这就证明了 $HK = KH$. **充分性** 对任意的 $h_1k_1, h_2k_2 \in HK$, 其中 $h_i \in H, k_i \in K$ $(i = 1, 2)$. 由于 $HK = KH$, 因此有

$$\begin{aligned} h_1k_1(h_2k_2)^{-1} &= h_1k_1k_2^{-1}h_2^{-1} = h_1\left(k_1k_2^{-1}\right)h_2^{-1} \\ &\in HKH = H(KH) = H(HK) = (HH)K = HK. \end{aligned}$$

由此知, HK 是 G 的子群.

定义 40

设 G 是群, H 是 G 的子群. 对任意的 $a \in G$, 群 G 的子集

$$aH = \{ah \mid h \in H\} \quad \text{与} \quad Ha = \{ha \mid h \in H\}$$

分别称为 H 在 G 中的**左陪集** (left coset) 和**右陪集** (right coset).

观察例 21, 例 22, 例 23 则易得下述性质:

- H 的一个陪集一般不是 G 的子群;
- G 的两个不同的元素可能生成 H 的同一个左陪集.

定理 41

设 H 是群 G 的子群, $a, b \in G$, 则

(1) $aH = H \Longleftrightarrow a \in H$;

(2) $aH < G \Longleftrightarrow a \in H$;

(3) $aH = bH \Longleftrightarrow a^{-1}b \in H$.

定理 41

设 H 是群 G 的子群, $a, b \in G$, 则

(1) $aH = H \iff a \in H$;

(2) $aH < G \iff a \in H$;

(3) $aH = bH \iff a^{-1}b \in H$.

证明: (1) 如果 $aH = H$, 则因 $a = ae \in aH$, 所以 $a \in H$.

反之, 如果 $a \in H$, 则 $aH \subseteq HH = H$. 由于 $a \in H$, 则 $a^{-1} \in H$, 类似有 $a^{-1}H \subseteq HH \subseteq H$. 于是
$H = eH = \left(aa^{-1}\right) H = a\left(a^{-1}H\right) \subseteq aH$. 所以 $aH = H$.

(2) 因为 $a \in aH$ 且 $aH < G$, 所以 $a^2 \in aH$, 即存在 $h \in H$ 使得 $a^2 = ah$. 由消去律得 $a = h \in H$.

另一方面, 如果 $a \in H$, 则由 (1) 得 $aH = H$ 为子群.

(3) 如果 $aH = bH$, 则

$$a^{-1}bH = a^{-1}aH = eH = H,$$

从而由 (1) 知, $a^{-1}b \in H$.

反之, 如果 $a^{-1}b \in H$, 则又由 (1) 得 $a^{-1}bH = H$, 于是

$$aH = a\left(a^{-1}bH\right) = \left(aa^{-1}\right)bH = ebH = bH.$$

注 41.1

定理 *41* 的结论对右陪集也成立，结论为 $Ha = Hb \Leftrightarrow ba^{-1} \in H$.

陪集与等价

注 41.1

定理 *41* 的结论对右陪集也成立, 结论为 $Ha = Hb \Leftrightarrow ba^{-1} \in H$.

引理 42

设 G 是群, $H < G$. 定义 G 上的关系为: 对于 $a, b \in G$, $a \sim b \Leftrightarrow a^{-1}b \in H$. 则 $\sim$ 是 G 上的等价关系, 并且元素 a 对此等价关系的等价类是 aH.

陪集与等价

注 41.1

定理 *41* 的结论对右陪集也成立, 结论为 $Ha = Hb \Leftrightarrow ba^{-1} \in H$.

引理 42

设 G 是群, $H < G$. 定义 G 上的关系为: 对于 $a, b \in G, a \sim b \Leftrightarrow a^{-1}b \in H$. 则 $\sim$ 是 G 上的等价关系, 并且元素 a 对此等价关系的等价类是 aH.

证明: 对每个 $a \in G$, 由于 $a^{-1}a = e \in H$, 从而 $a \sim a$, 因此该关系具有反身性;

注 41.1

定理 *41* 的结论对右陪集也成立，结论为 $Ha = Hb \Leftrightarrow ba^{-1} \in H$.

引理 42

设 G 是群, $H < G$. 定义 G 上的关系为: 对于 $a, b \in G, a \sim b \Leftrightarrow a^{-1}b \in H$. 则 $\sim$ 是 G 上的等价关系, 并且元素 a 对此等价关系的等价类是 aH.

证明: 对每个 $a \in G$, 由于 $a^{-1}a = e \in H$, 从而 $a \sim a$, 因此该关系具有反身性;若 $a \sim b$, 则 $a^{-1}b \in H$, 由于 H 是子群, 从而 $b^{-1}a = \left(a^{-1}b\right)^{-1} \in H$, 于是 $b \sim a$, 因此该关系满足对称性;

注 41.1

定理 *41* 的结论对右陪集也成立，结论为 $Ha = Hb \Leftrightarrow ba^{-1} \in H$.

引理 42

设 G 是群，$H < G$. 定义 G 上的关系为：对于 $a, b \in G, a \sim b \Leftrightarrow a^{-1}b \in H$. 则 $\sim$ 是 G 上的等价关系，并且元素 a 对此等价关系的等价类是 aH.

证明：对每个 $a \in G$，由于 $a^{-1}a = e \in H$，从而 $a \sim a$，因此该关系具有反身性;若 $a \sim b$，则 $a^{-1}b \in H$，由于 H 是子群，从而 $b^{-1}a = \left(a^{-1}b\right)^{-1} \in H$，于是 $b \sim a$，因此该关系满足对称性；若 $a \sim b, b \sim c$，则 $a^{-1}b, b^{-1}c \in H$. 因此 $a^{-1}c = \left(a^{-1}b\right)\left(b^{-1}c\right) \in H$. 于是 $a \sim c$.

注 41.1

定理 *41* 的结论对右陪集也成立，结论为 $Ha = Hb \Leftrightarrow ba^{-1} \in H$.

引理 42

设 G 是群，$H < G$. 定义 G 上的关系为：对于 $a, b \in G, a \sim b \Leftrightarrow a^{-1}b \in H$. 则 $\sim$ 是 G 上的等价关系，并且元素 a 对此等价关系的等价类是 aH.

证明：对每个 $a \in G$，由于 $a^{-1}a = e \in H$，从而 $a \sim a$，因此该关系具有反身性；若 $a \sim b$，则 $a^{-1}b \in H$，由于 H 是子群，从而 $b^{-1}a = \left(a^{-1}b\right)^{-1} \in H$，于是 $b \sim a$，因此该关系满足对称性；若 $a \sim b, b \sim c$，则 $a^{-1}b, b^{-1}c \in H$. 因此 $a^{-1}c = \left(a^{-1}b\right)\left(b^{-1}c\right) \in H$. 于是 $a \sim c$.综上即得 $\sim$ 为 G 上的等价关系.

注 41.1

定理 *41* 的结论对右陪集也成立，结论为 $Ha = Hb \Leftrightarrow ba^{-1} \in H$.

引理 42

设 G 是群，$H < G$. 定义 G 上的关系为：对于 $a, b \in G, a \sim b \Leftrightarrow a^{-1}b \in H$. 则 $\sim$ 是 G 上的等价关系，并且元素 a 对此等价关系的等价类是 aH.

证明：对每个 $a \in G$，由于 $a^{-1}a = e \in H$，从而 $a \sim a$，因此该关系具有反身性;若 $a \sim b$，则 $a^{-1}b \in H$，由于 H 是子群，从而 $b^{-1}a = \left(a^{-1}b\right)^{-1} \in H$，于是 $b \sim a$，因此该关系满足对称性；若 $a \sim b, b \sim c$，则 $a^{-1}b, b^{-1}c \in H$. 因此 $a^{-1}c = \left(a^{-1}b\right)\left(b^{-1}c\right) \in H$. 于是 $a \sim c$.综上即得 $\sim$ 为 G 上的等价关系.进一步，由 $a \sim b \Leftrightarrow a^{-1}b = h \in H \Leftrightarrow b = ah \in aH$. 从而与 a 等价的元素全体为集合 aH.

注 42.1

由引理 *42* 和定理 *41* 第 *(3)* 条可知若有 $H < G$, 则对任意 $a, b \in G$ 有 aH 与 bH 或者完全相同或者无公共元素. 因此群 G 可表示成子群 H 的一些互不相交的左陪集之并. 从而群 G 的子群 H 的全体左陪集的集合组成群 G 的一种分类, 即

$$G = \bigcup_{g_i \in \mathcal{R}} g_i H,$$

其中 g_i 取遍 H 的不同陪集的代表元的集合 $\mathcal{R}$. 特别地, 如果 G 为有限群, 则

$$|G| = \sum_{i=1}^{t} |g_i H| = \sum_{i=1}^{t} |H| = t|H|,$$

其中 t 为 H 的不同左陪集的个数.

定理 43

设 H 为 G 的子群, 则

$$\begin{aligned}\phi : G/H &\longrightarrow H\backslash G,\\ aH &\longmapsto Ha^{-1},\end{aligned}$$

是 G/H 到 $H\backslash G$ 的一一映射, 其中

$$G/H = \{gH \mid g \in G\},$$

$$H\backslash G = \{Hg \mid g \in G\}.$$

证明

(1) 如果 $aH = bH$, 则由定理 41 的第 (3) 条知 $a^{-1}b \in H$, 则

$$Ha^{-1} = Ha^{-1}\left(bb^{-1}\right) = H\left(a^{-1}b\right)b^{-1} = Hb^{-1}.$$

这说明, ϕ 是 G/H 到 $H\backslash G$ 的映射.

(2) 设 $aH, bH \in G/H$, 如果 $\phi(aH) = \phi(bH)$, 即 $Ha^{-1} = Hb^{-1}$, 则由注 41.1 得 $b^{-1}a \in H$, 于是
$aH = (bb^{-1})aH = b(b^{-1}aH) = bH$, 所以 ϕ 是 G/H 到 $H\backslash G$ 的单映射.

(3) 对任意的 $Ha \in H\backslash G$, 有 $\phi\left(a^{-1}H\right) = Ha$, 所以 ϕ 是 G/H 到 $H\backslash G$ 的满映射.

陪集的指数

定义 44

设 G 是群, H 是 G 的子群. 称子群 H 在群 G 中的左陪集或右陪集的个数 (有限或无限) 为 H 在 G 中的**指数** (index), 记作 $[G:H]$.

陪集的指数

定义 44

设 G 是群, H 是 G 的子群. 称子群 H 在群 G 中的左陪集或右陪集的个数 (有限或无限) 为 H 在 G 中的**指数** (index), 记作 $[G:H]$.

定理 45 (Lagrange 定理)

设 G 是一个有限群, H 是 G 的子群, 则
$$|G| = |H|[G:H].$$

元素的阶

定义 46

设 G 是一个群, e 是 G 的单位元, $a \in G$. 如果存在正整数 r, 使 $a^r = e$, 则称 a **是有限阶元素**, 否则称 a **是无限阶元素**. 使 $a^r = e$ 的最小正整数 r 称为元素 a **的阶** (order), 记作 $\operatorname{ord} a = r$. 如果 a 是无限阶元素, 则记作 $\operatorname{ord} a = \infty$.

例 47

在 $\mathbb{Z}_6$ 中, 计算每个元素的阶.

例 47

在 $\mathbb{Z}_6$ 中, 计算每个元素的阶.

解: $\mathbb{Z}_6=\{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4},\overline{5}\}$. 因为

$$1\cdot\overline{2}=\overline{2},\quad 2\cdot\overline{2}=\overline{4},\quad 3\cdot\overline{2}=\overline{6}=\overline{0},$$

所以 $\operatorname{ord}\overline{2}=3$. 类似可得

$$\operatorname{ord}\overline{0}=1,\quad \operatorname{ord}\overline{1}=6,\quad \operatorname{ord}\overline{3}=2,\quad \operatorname{ord}\overline{4}=3,\quad \operatorname{ord}\overline{5}=6.$$

例 47

在 $\mathbb{Z}_6$ 中, 计算每个元素的阶.

解: $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$. 因为

$$1 \cdot \overline{2} = \overline{2}, \quad 2 \cdot \overline{2} = \overline{4}, \quad 3 \cdot \overline{2} = \overline{6} = \overline{0},$$

所以 $\operatorname{ord} \overline{2} = 3$. 类似可得

$$\operatorname{ord} \overline{0} = 1, \quad \operatorname{ord} \overline{1} = 6, \quad \operatorname{ord} \overline{3} = 2, \quad \operatorname{ord} \overline{4} = 3, \quad \operatorname{ord} \overline{5} = 6.$$

例 48

在整数加群 $\mathbb{Z}$ 中, 除零元外每个元素都是无限阶的.

元素的阶

定理 49

设 G 为群, e 为 G 的单位元.

(1) 对任意的 $a \in G$, 有 $\operatorname{ord} a = \operatorname{ord} a^{-1}$;
(2) 设 $\operatorname{ord} a = n$, 如果有 $m \in \mathbb{Z}$, 使 $a^m = e$, 则 $n \mid m$;
(3) 设 $\operatorname{ord} a = n$, 则对任意的 $m \in \mathbb{Z}$, $\operatorname{ord} a^m = \frac{n}{(n,m)}$;
(4) 设 $\operatorname{ord} a = n, \operatorname{ord} b = m$, 如果 $ab = ba$ 且 $\gcd(n, m) = 1$, 则 $\operatorname{ord} ab = mn$.

定理 49

设 G 为群, e 为 G 的单位元.

(1) 对任意的 $a \in G$, 有 $\operatorname{ord} a = \operatorname{ord} a^{-1}$;
(2) 设 $\operatorname{ord} a = n$, 如果有 $m \in \mathbb{Z}$, 使 $a^m = e$, 则 $n \mid m$;
(3) 设 $\operatorname{ord} a = n$, 则对任意的 $m \in \mathbb{Z}$, $\operatorname{ord} a^m = \frac{n}{(n,m)}$;
(4) 设 $\operatorname{ord} a = n, \operatorname{ord} b = m$, 如果 $ab = ba$ 且 $\gcd(n, m) = 1$, 则 $\operatorname{ord} ab = mn$.

证明: (1) 当 $\operatorname{ord} a = \infty$ 时, 显然有 $\operatorname{ord} a^{-1} = \infty$. 设 $\operatorname{ord} a = r$, 易得 $e = (aa^{-1})^r = a^r(a^{-1})^r = e(a^{-1})^r = (a^{-1})^r$. 从而 $\operatorname{ord} a^{-1} \leq r$. 设 $\operatorname{ord} a^{-1} = t$, 则显然 $t \leq r$. 由 $e = (aa^{-1})^t = a^t(a^{-1})^t = a^t$ 可得 $r \leq t$. 从而 $r = t$.

(2) 根据元素阶的定义显然有 $m \geq n$. 因为 $n \neq 0$, 所以存在 $q, r \in \mathbb{Z}$, 使 $m = qn + r$, 其中 $0 \leq r < n$. 则有 $a^m = a^{nq+r} \Rightarrow e = (a^n)^q a^r = ea^r \Rightarrow e = a^r$, 则 $r = 0$, 否则与 a 的阶为 n 定义矛盾.

证明 (续)

(3) 设 $\operatorname{ord} a^m = r$, 则 $a^{rm} = (a^m)^r = e$, 于是, $n \mid rm$. 从而 $\frac{n}{(n,m)} \mid \frac{m}{(n,m)} \cdot r$. 因为 $\left(\frac{n}{(n,m)}, \frac{m}{(n,m)}\right) = 1$ (否则若 $\left(\frac{n}{(n,m)}, \frac{m}{(n,m)}\right) = s > 1$ 则 $s(m,n)$ 是 m,n 的公因子, 与 (m,n) 是最大公因子矛盾), 则有 $\frac{n}{(n,m)} \mid r$. 另一方面, 注意到

$$(a^m)^{\frac{n}{(n,m)}} = a^{\frac{mn}{(n,m)}} = (a^n)^{\frac{m}{(n,m)}} = e,$$

于是由 (2) 可得 $r \mid \frac{n}{(n,m)}$. 综上可知 $r = \frac{n}{(n,m)}$.

(4) 设 $\operatorname{ord} ab = r$, 则

$$a^{rm} = a^{rm} \cdot b^{rm} \qquad (\text{因为} \quad \operatorname{ord} b = m\ )$$
$$= (ab)^{rm} = e,$$

所以 $n \mid rm$. 又因为 $\gcd(n, m) = 1$, 所以 $n \mid r$. 同理可证 $b^{rn} = b^{rn} \cdot a^{rn} = e$, 从而 $m \mid r$. 由 $\gcd(n, m) = 1$, 可得存在整数 s, t 使得 $sn + tm = 1 \Rightarrow snr + tmr = r \Rightarrow mn \mid r$. 另一方面,

$$(ab)^{mn} = a^{mn} \cdot b^{mn} = e \cdot e = e.$$

所以又有 $r \mid mn$. 综上可得 $r = mn$.

元素的阶

定理 50

设 G 是一个有限群, $|G| = n$, 则对任意的 $a \in G$, a 是有限阶的, 且 $\operatorname{ord} a \mid |G|$, 即有限群的任何一个元素的阶都是群阶数的因子.

定理 50

设 G 是一个有限群, $|G| = n$, 则对任意的 $a \in G$, a 是有限阶的, 且 $\operatorname{ord} a \mid |G|$, 即有限群的任何一个元素的阶都是群阶数的因子.

证明: 由注 34.1 知集合 $\{a, a^2, a^3, \cdots\}$ 是 G 的一个循环子群, 可记为 $\langle a \rangle$. 显然 a 的阶就是子群 $\langle a \rangle$ 的阶, 从而由拉格朗日定理知 $\langle a \rangle$ 的阶是 $|G|$ 的因子, 所以 a 的阶是 $|G|$ 的因子.

推论 51

设 G 为有限群, $|G| = n$, 则对任意的 $a \in G$, 有 $a^n = e$.

推论 51

设 G 为有限群, $|G| = n$, 则对任意的 $a \in G$, 有 $a^n = e$.

证明: 设 a 的阶为 d, 则有正整数 n_1, 使 $n = dn_1$. 于是

$$a^n = a^{dn_1} = \left(a^d\right)^{n_1} = e^{n_1} = e.$$

推论 51

设 G 为有限群, $|G|=n$, 则对任意的 $a\in G$, 有 $a^n=e$.

证明: 设 a 的阶为 d, 则有正整数 n_1, 使 $n=dn_1$. 于是

$$a^n=a^{dn_1}=\left(a^d\right)^{n_1}=e^{n_1}=e.$$

注 51.1

将推论 *51* 应用到例 *14* 中, 可以从群的角度再次证明 *Euler* 定理和 *Fermat* 小定理.

作业

- Page 71: 2, 6, 8, 12, 13, 21.

§2.4 正规子群和商群

- 正规子群
- 正规子群的判定
- 正规子群的性质
- 陪集的运算
- 商群
- 商群的应用

§2.3 陪集和陪集分解

- 群中集合的乘积
- 子群的乘积
- 子群的陪集
- 陪集的指数
- 元素的阶

正规子群

定义 52

设 H 是群 G 的子群, 如果对每个 $a \in G$, 都有 $aH = Ha$, 则称 H 是群 G 的**一个正规子群** (normal subgroup) **或不变子群** (invariant subgroup), 记作 $H \lhd G$.

正规子群

定义 52

设 H 是群 G 的子群, 如果对每个 $a \in G$, 都有 $aH = Ha$, 则称 H 是群 G 的**一个正规子群** (normal subgroup) **或不变子群** (invariant subgroup), 记作 $H \triangleleft G$.

注 52.1

在上述定义中, 条件 $aH = Ha$ 仅仅表示两个集合 aH 与 Ha 相等, 通常无法由 $aH = Ha$ 推出 $ah = ha$ 对 H 中所有的元素 h 都成立. $aH = Ha$ 意味着对任意的 $h_1 \in H$, 存在 $h_2 \in H$, 使得 $ah_1 = h_2a$.

正规子群

定义 52

设 H 是群 G 的子群, 如果对每个 $a \in G$, 都有 $aH = Ha$, 则称 H 是群 G 的**一个正规子群** (normal subgroup) **或不变子群** (invariant subgroup), 记作 $H \lhd G$.

注 52.1

在上述定义中, 条件 $aH = Ha$ 仅仅表示两个集合 aH 与 Ha 相等, 通常无法由 $aH = Ha$ 推出 $ah = ha$ 对 H 中所有的元素 h 都成立. $aH = Ha$ 意味着对任意的 $h_1 \in H$, 存在 $h_2 \in H$, 使得 $ah_1 = h_2 a$.

例 53

由正规子群的定义容易知道, 群 G 的单位元群 $\{e\}$ 和群 G 本身都是 G 的正规子群. 这两个正规子群称为 G 的**平凡正规子群**. 如果群 G 只有平凡的正规子群, 且 $G \neq \{e\}$, 则称 G 为**单群** (simple group).

例 54

如果 G 是交换群, 则 G 的一切子群都是 G 的正规子群.

例 54

如果 G 是交换群, 则 G 的一切子群都是 G 的正规子群.

证明: 因为

$$aH = \{ah \mid h \in H\} = \{ha \mid h \in H\} = Ha, \quad \forall a \in G,$$

所以 H 是 G 的正规子群.

例 54

如果 G 是交换群, 则 G 的一切子群都是 G 的正规子群.

证明: 因为

$$aH = \{ah \mid h \in H\} = \{ha \mid h \in H\} = Ha, \quad \forall a \in G,$$

所以 H 是 G 的正规子群.

例 55

设 H, K 都是 G 的子群. 如果 H 是 G 的正规子群且 $H \subseteq K$, 则 H 也是 K 的正规子群.

例 54

如果 G 是交换群, 则 G 的一切子群都是 G 的正规子群.

证明: 因为

$$aH = \{ah \mid h \in H\} = \{ha \mid h \in H\} = Ha, \quad \forall a \in G,$$

所以 H 是 G 的正规子群.

例 55

设 H, K 都是 G 的子群. 如果 H 是 G 的正规子群且 $H \subseteq K$, 则 H 也是 K 的正规子群.

证明: 显然 H 是 K 的子群. 因为 H 是 G 的正规子群, 所以对任意的 $a \in G$, 有 $aH = Ha$. 特别地, 对任意的 $a \in K$, 由于 $K < G$ 的子群, 所以也有 $aH = Ha$. 从而 H 为 K 的正规子群.

例 56

设 G 为群, H 是 G 的子群. 如果 H 在 G 中的指数 $[G:H]=2$, 则 H 是 G 的正规子群.

例 56

设 G 为群, H 是 G 的子群. 如果 H 在 G 中的指数 $[G:H]=2$, 则 H 是 G 的正规子群.

证明: 对任意 $a\in G$, 若 $a\in H$, 则 $aH=H=Ha$. 若 $a\notin H$, 则由定理 41 第 (1) 条知 aH 与 H 是 G 的两个不同的陪集. 由于 $[G:H]=2$, 由此 $G=H\cup aH$. 同理有 $G=H\cup Ha$.

因为 $aH\cap H=\emptyset$, 而 $aH\subseteq G=H\cup Ha$, 所以 $aH\subseteq Ha$. 同理有 $Ha\subseteq aH$, 所以 $aH=Ha$. 因此 H 是 G 正规子群.

正规子群的判定

定理 57

设 G 是群, H 是 G 的子群, 则下列三个条件等价:

(1) H 是 G 的正规子群;

(2) 对任意的 $a \in G$, 有 $aHa^{-1} \subseteq H$;

(3) 对任意的 $a \in G, h \in H$, 有 $aha^{-1} \in H$.

证明

$((1) \Rightarrow (2))$ 因为 $H \lhd G$, 所以对任意的 $a \in G$, 有 $aH = Ha$. 因而

$$aHa^{-1} = (Ha)a^{-1} = H\left(aa^{-1}\right) = He = H \subseteq H.$$

证明

((1) $\Rightarrow$ (2)) 因为 $H \lhd G$, 所以对任意的 $a \in G$, 有 $aH = Ha$. 因而

$$aHa^{-1} = (Ha)a^{-1} = H\left(aa^{-1}\right) = He = H \subseteq H.$$

((2) $\Rightarrow$ (3)) 因为 $aHa^{-1} = H$, 所以显然有 $aHa^{-1} \subseteq H$. 于是对任意 $h \in H$, 有 $aha^{-1} \in H$.

证明

$((1) \Rightarrow (2))$ 因为 $H \lhd G$, 所以对任意的 $a \in G$, 有 $aH = Ha$. 因而

$$aHa^{-1} = (Ha)a^{-1} = H\left(aa^{-1}\right) = He = H \subseteq H.$$

$((2) \Rightarrow (3))$ 因为 $aHa^{-1} = H$, 所以显然有 $aHa^{-1} \subseteq H$. 于是对任意 $h \in H$, 有 $aha^{-1} \in H$. $((3) \Rightarrow (1))$ 对任意的 $a \in G, h \in H$, 有 $aha^{-1} \in H$, 所以

$$ah = ahe = ah(a^{-1}a) = \left(aha^{-1}\right)a \in Ha,$$

从而 $aH \subseteq Ha$.

证明

$((1) \Rightarrow (2))$ 因为 $H \lhd G$, 所以对任意的 $a \in G$, 有 $aH = Ha$. 因而

$$aHa^{-1} = (Ha)a^{-1} = H\left(aa^{-1}\right) = He = H \subseteq H.$$

$((2) \Rightarrow (3))$ 因为 $aHa^{-1} = H$, 所以显然有 $aHa^{-1} \subseteq H$. 于是对任意 $h \in H$, 有 $aha^{-1} \in H$. $((3) \Rightarrow (1))$ 对任意的 $a \in G, h \in H$, 有 $aha^{-1} \in H$, 所以

$$ah = ahe = ah(a^{-1}a) = \left(aha^{-1}\right)a \in Ha,$$

从而 $aH \subseteq Ha$. 另一方面, 对任意的 $a \in G, h \in H$, 有

$$a^{-1}ha = a^{-1}h\left(a^{-1}\right)^{-1} \in H,$$

于是

$$ha = eha = (aa^{-1})ha = a(a^{-1}ha) \in aH,$$

从而 $Ha \subseteq aH$. 于是 $aH = Ha$. 由此得 $H \lhd G$.

正规子群的性质

定理 58

设 G 为群, H, K 是 G 的正规子群, 则
$$H \cap K \text{ 与 } HK$$
都是 G 的正规子群.

正规子群的性质

定理 58

设 G 为群, H, K 是 G 的正规子群, 则

$$H \cap K \text{ 与 } HK$$

都是 G 的正规子群.

证明: (1) 由定理 30 知 $H \cap K < G$. 对任意的 $x \in G$, 有

$$x(H \cap K)x^{-1} \subseteq xHx^{-1} = Hxx^{-1} \subseteq H,$$

$$x(H \cap K)x^{-1} \subseteq xKx^{-1} = Kxx^{-1} \subseteq K.$$

于是 $x(H \cap K)x^{-1} \subseteq H \cap K$. 由定理 57 第 (2) 条可得 $H \cap K$ 是 G 的正规子群.

正规子群的性质

定理 58

设 G 为群, H, K 是 G 的正规子群, 则
$$H \cap K \text{ 与 } HK$$
都是 G 的正规子群.

证明: (1) 由定理 30 知 $H \cap K < G$. 对任意的 $x \in G$, 有
$$x(H \cap K)x^{-1} \subseteq xHx^{-1} = Hxx^{-1} \subseteq H,$$
$$x(H \cap K)x^{-1} \subseteq xKx^{-1} = Kxx^{-1} \subseteq K.$$
于是 $x(H \cap K)x^{-1} \subseteq H \cap K$. 由定理 57 第 (2) 条可得 $H \cap K$ 是 G 的正规子群. (2) 由于 H 与 K 都是 G 的正规子群, 因此 $HK = KH$, 于是由定理 39 第 (2) 条可得 HK 是 G 的子群. 对任意的 $x \in G$, 由于 H, K 都是 G 的正规子群, 则
$$x(HK) = (xH)K = (Hx)K = H(xK) = H(Kx) = (HK)x,$$
所以 HK 是 G 的正规子群.

陪集的运算

- 若 H 是群 G 的正规子群, 则由正规子群的定义可知 H 的左陪集 aH 与右陪集 Ha 完全相同, 因而可直接称 aH 或 Ha 为它的一个陪集.

陪集的运算

- 若 H 是群 G 的正规子群, 则由正规子群的定义可知 H 的左陪集 aH 与右陪集 Ha 完全相同, 因而可直接称 aH 或 Ha 为它的一个陪集.

定义 59

设 $H \lhd G$, 令 $G/H = \{aH \mid a \in G\}$. 对任意的 $aH, bH \in G/H$, 规定 G/H 中关于陪集的运算 "$\cdot$" 为

$$(aH) \cdot (bH) = (ab)H. \tag{1}$$

引理 60

设 $H \lhd G$, 则 G/H 中关于陪集的运算 "$\cdot$" 是 G/H 的一个代数运算.

引理 60

设 $H \triangleleft G$, 则 G/H 中关于陪集的运算 "$\cdot$" 是 G/H 的一个代数运算.

证明: 只需证明 H 的任意两个陪集 aH, bH 的乘积是唯一确定的, 它与陪集的代表元 a, b 的选取无关. 设 $a'H = aH, b'H = bH$, 则

$$\begin{aligned} a'H \cdot b'H &= \left(a'b'\right) H = a' \left(b'H\right) = a'(bH) = a'(Hb) \\ &= \left(a'H\right) b = (aH)b = a(Hb) = (ab)H, \\ &= aH \cdot bH. \end{aligned}$$

所以上述运算是 G/H 的一个代数运算.

定理 61

设 $H \lhd G$, 则 G/H 关于定义 59 规定的运算 “$\cdot$” 构成群.

定理 61

设 $H \triangleleft G$, 则 G/H 关于定义 *59* 规定的运算 “$\cdot$” 构成群.

证明: (1) 引理 60 已证该运算为代数运算.

定理 61

设 $H \lhd G$, 则 G/H 关于定义 59 规定的运算 “$\cdot$” 构成群.

证明: (1) 引理 60 已证该运算为代数运算. (2) 对任意的 $a, b, c \in G$, 有

$$
\begin{aligned}
(aH \cdot bH) \cdot cH &= (ab)H \cdot cH = ((ab)c)H \\
&= (a(bc))H = aH \cdot (bc)H \\
&= aH \cdot (bH \cdot cH),
\end{aligned}
$$

所以结合律成立.

定理 61

设 $H \lhd G$, 则 G/H 关于定义 59 规定的运算 “$\cdot$” 构成群.

证明: (1) 引理 60 已证该运算为代数运算. (2) 对任意的 $a, b, c \in G$, 有

$$\begin{aligned}(aH \cdot bH) \cdot cH &= (ab)H \cdot cH = ((ab)c)H \\ &= (a(bc))H = aH \cdot (bc)H \\ &= aH \cdot (bH \cdot cH),\ \text{所以结合律成立.}\end{aligned}$$

(3) 任意 $a \in G$, 有 $eH \cdot aH = (ea)H = aH = (ae)H = aH \cdot eH$, 所以 $eH (= H)$ 为 G/H 的单位元.

定理 61

设 $H \lhd G$, 则 G/H 关于定义 *59* 规定的运算 “$\cdot$” 构成群.

证明: (1) 引理 60 已证该运算为代数运算. (2) 对任意的 $a, b, c \in G$, 有

$$\begin{aligned}(aH \cdot bH) \cdot cH &= (ab)H \cdot cH = ((ab)c)H \\ &= (a(bc))H = aH \cdot (bc)H \\ &= aH \cdot (bH \cdot cH), \text{ 所以结合律成立.}\end{aligned}$$

(3) 任意 $a \in G$, 有 $eH \cdot aH = (ea)H = aH = (ae)H = aH \cdot eH$, 所以 $eH (= H)$ 为 G/H 的单位元. (4) 对任意的 $aH \in G/H$, 有 $a^{-1}H \in G/H$, 且

$$a^{-1}H \cdot aH = \left(a^{-1}a\right) H = eH = \left(aa^{-1}\right) H = aH \cdot a^{-1}H,$$

所以 G/H 中每个元素 aH 都有逆元 $a^{-1}H$.

商群

定义 62

设 G 为群, H 是 G 的正规子群. H 的所有陪集 G/H 关于由式 (1) 所规定的运算构成的群称为群 G 关于子群 H 的**商群** (quotient group), 仍记作 G/H.

商群

定义 62

设 G 为群, H 是 G 的正规子群. H 的所有陪集 G/H 关于由式 (1) 所规定的运算构成的群称为群 G 关于子群 H 的**商群** (quotient group), 仍记作 G/H.

推论 63

设 $H \lhd G$, 则

(1) 商群 G/H 的单位元是 $eH(= H)$;
(2) aH 在 G/H 中的逆元是 $a^{-1}H$.

定义 62

设 G 为群, H 是 G 的正规子群. H 的所有陪集 G/H 关于由式 (1) 所规定的运算构成的群称为群 G 关于子群 H 的**商群** (quotient group), 仍记作 G/H.

推论 63

设 $H \lhd G$, 则

(1) 商群 G/H 的单位元是 $eH(=H)$;
(2) aH 在 G/H 中的逆元是 $a^{-1}H$.

推论 64

设 $H \lhd G$. 如果 G 是交换群, 则商群 G/H 也是交换群.

- 由于 H 在 G 中的指数 $[G:H]$ 就是 H 在 G 中的陪集的个数, 所以 $|G/H| = [G:H]$.
- 特别地, 当 G 是有限群时,

$$|G/H| = [G:H] = \frac{|G|}{|H|}.$$

商群

- 由于 H 在 G 中的指数 $[G:H]$ 就是 H 在 G 中的陪集的个数, 所以 $|G/H| = [G:H]$.
- 特别地, 当 G 是有限群时,

$$|G/H| = [G:H] = \frac{|G|}{|H|}.$$

推论 65

有限群 G 的商群的阶是群 G 的阶数的因子.

例 66

设 $\mathbb{Q}^*$ 是所有非零有理数构成的乘法群, $H = \{1, -1\}$, 则 $H \lhd \mathbb{Q}^*$. 对任意的 $a \in \mathbb{Q}^*$, 有 $aH = \{a, -a\}$, 所以

$$\mathbb{Q}^*/H = \{aH \mid a > 0, a \in \mathbb{Q}\}.$$

显然, $\mathbb{Q}^*/H$ 是无限群.

例 66

设 $\mathbb{Q}^*$ 是所有非零有理数构成的乘法群, $H = \{1, -1\}$, 则 $H \lhd \mathbb{Q}^*$. 对任意的 $a \in \mathbb{Q}^*$, 有 $aH = \{a, -a\}$, 所以

$$\mathbb{Q}^*/H = \{aH \mid a > 0, a \in \mathbb{Q}\}.$$

显然, $\mathbb{Q}^*/H$ 是无限群.

例 67

设 $G = \mathbb{Z}_{18}, H = \langle\overline{6}\rangle$, 则

$G/H = \{\overline{0} + H, \overline{1} + H, \overline{2} + H, \overline{3} + H, \overline{4} + H, \overline{5} + H\} = \langle\overline{1} + H\rangle$.

由于这是一个阶为 6 的循环群.

例 68

设 $G=\mathbb{Z}, m$ 为任一大于 1 的正整数. 令 $H=\langle m\rangle$, 则 $H \lhd \mathbb{Z}$. 易知,

$$a+H=b+H \Longleftrightarrow m \mid a-b.$$

由此推出, H 的全体陪集为

$$\begin{aligned}
&\overline{0}=0+H=\{zm \mid z\in\mathbb{Z}\},\\
&\overline{1}=1+H=\{1+zm \mid z\in\mathbb{Z}\},\\
&\cdots\cdots\\
&\overline{m-1}=(m-1)+H=\{(m-1)+zm \mid z\in\mathbb{Z}\}.
\end{aligned}$$

显然, $\mathbb{Z}$ 关于 $\langle m\rangle$ 的商群 $\mathbb{Z}/\langle m\rangle$ 就是 $\mathbb{Z}$ 关于模 m 的剩余类加群 $\mathbb{Z}_m$. 因此有

$$\mathbb{Z}/\langle m\rangle=\mathbb{Z}_m.$$

定理 69 (Cauchy Theorem)

设 G 为有限交换群, $|G| = n$. 证明: 对 n 的任一素因子 p, G 必有阶为 p 的元素.

定理 69 (Cauchy Theorem)

设 G 为有限交换群, $|G|=n$. 证明: 对 n 的任一素因子 p, G 必有阶为 p 的元素.

证明: 对 n 应用数学归纳法. 首先, 当 $n=2$ 时, 结论显然成立. 假设结论对所有阶小于 n 的交换群成立. 考察阶为 n 的交换群 G, 设 p 为 n 的任一素因子. 任取 $a \in G, a \neq e$, 设 $\operatorname{ord} a = r$.

(1) 如果 $r=pk$, 则由定理 49 第 (3) 条立即可得 $\operatorname{ord} a^k = p$, 结论成立.

证明 (续)

(2) 如果 $p \nmid r$, 令 $H = \langle a \rangle$, 则 H 为 G 的正规子群, 且商群 G/H 为交换群. 由于 $|G/H| = \frac{n}{r} < n$, 且有 $p \nmid r$ 以及 $p \mid n$, 所以 $p \mid \frac{n}{r}$. 从而由归纳假设知, 存在 $bH \in G/H$, 使得 $\operatorname{ord} bH = p$, $(bH)^p = e_{G/H} = eH = H$, 其中 $e_{G/H}$ 是 G/H 的单位元, e 是 G 的单位元. 由于 G/H 是交换群, 故 $(bH)^p = bH \cdot bH \cdot \cdots \cdot bH = b^p H$, 因此 $b^p H = H$, 于是由定理 41 第 (1) 条可知 $b^p \in H$. 从而 $b^{pr} = e$. 由于 $p \nmid r$, 由定理 49 第 (2) 条知 $(bH)^r \neq H$, 即 $b^r \notin H$, 于是 $b^r \neq e$. 而 $(b^r)^p = e$, 所以 $\operatorname{ord} b^r \mid p$, 从而 $\operatorname{ord} b^r = p$. 于是由归纳法原理知结论成立.

作业

- Page 79: 2, 4, 9, 11, 13, 23, 25 (选做).

§2.4 正规子群和商群

- 正规子群
- 正规子群的判定
- 正规子群的性质
- 陪集的运算
- 商群
- 商群的应用

§2.5 群的同态和同构

- 同态与同构
- 同态的性质
- 同构的性质
- 同态的核
- 同态基本定理
- 同构的证明步骤

定义 70

设 $(G,\cdot)$ 与 $(G',\circ)$ 是两个群, ϕ 是 G 到 G' 的一个映射. 如果对任意的 $a,b\in G$ 都有

$$\phi(a\cdot b)=\phi(a)\circ\phi(b),$$

则称 ϕ 是群 G 到群 G' 的**一个同态映射** (homomorphism), 简称**同态**. 当同态映射 ϕ 作为集合映射为满射时, 称 ϕ 为群 G 到 G' 的**满同态** (epimorphism); 当同态映射 ϕ 作为集合映射是单射时, 称 ϕ 为群 G 到 G' 的**单同态** (monomorphism); 当同态映射 ϕ 作为集合映射是一一映射时, 称 ϕ 为群 G 到 G' 的**同构** (isomorphism), 表示成 $G\cong G'$. 群 G 到它自身的同态 (同构) 映射称为群 G 的**自同态** (**自同构**).

定义 70

设 $(G,\cdot)$ 与 $(G',\circ)$ 是两个群, ϕ 是 G 到 G' 的一个映射. 如果对任意的 $a,b\in G$ 都有

$$\phi(a\cdot b)=\phi(a)\circ\phi(b),$$

则称 ϕ 是群 G 到群 G' 的一个**同态映射** (homomorphism), 简称**同态**. 当同态映射 ϕ 作为集合映射为满射时, 称 ϕ 为群 G 到 G' 的**满同态** (epimorphism); 当同态映射 ϕ 作为集合映射是单射时, 称 ϕ 为群 G 到 G' 的**单同态** (monomorphism); 当同态映射 ϕ 作为集合映射是一一映射时, 称 ϕ 为群 G 到 G' 的**同构** (isomorphism), 表示成 $G\cong G'$. 群 G 到它自身的同态 (同构) 映射称为群 G 的**自同态** (**自同构**).

注 70.1

在同态映射的定义中, 等式左边的 $a\cdot b$ 是在 G 中进行的运算, 而等式右边的 $\phi(a)\circ\phi(b)$ 却是在 G' 中进行运算. 当 G 和 G' 都是乘群时我们常将两边的代数运算符号省略.

例 71

设 $\mathbb{R}^n$ 为实数域 $\mathbb{R}$ 上全体 n 维向量的集合关于向量的加法运算构成的群, $H = \{AX \mid X \in \mathbb{R}^n\}$, 其中 $A \in \mathrm{M}_n(\mathbb{R})$. 令

$$\begin{aligned} \phi: \quad \mathbb{R}^n &\longrightarrow \quad H \\ X &\longmapsto AX, \end{aligned}$$

则 ϕ 是 $\mathbb{R}^n$ 到 H 的同态映射.

例 71

设 $\mathbb{R}^n$ 为实数域 $\mathbb{R}$ 上全体 n 维向量的集合关于向量的加法运算构成的群, $H = \{AX \mid X \in \mathbb{R}^n\}$, 其中 $A \in \mathrm{M}_n(\mathbb{R})$. 令

$$\begin{aligned} \phi: \quad \mathbb{R}^n &\longrightarrow \quad H \\ X &\longmapsto AX, \end{aligned}$$

则 ϕ 是 $\mathbb{R}^n$ 到 H 的同态映射.

例 72

设 G, G' 是两个群, e' 是 G' 的单位元. 对任意的 $a \in G$, 令

$$\begin{aligned} \phi: \quad G &\longrightarrow G', \\ a &\longmapsto e', \end{aligned}$$

则对任意的 $a, b \in G$,

$$\phi(ab) = e' = e'e' = \phi(a)\phi(b),$$

所以 ϕ 是 G 到 G' 的同态映射.

例

例 73

设 G 是整数加群 $\mathbb{Z}, G'$ 是全体非零实数 $\mathbb{R}^*$ 关于数的乘法所构成的乘法群. 令

$$\begin{aligned} \phi: \quad \mathbb{Z} &\longrightarrow \quad \mathbb{R}^* \\ n &\longmapsto (-1)^n. \end{aligned}$$

显然 ϕ 是 G 到 G' 的映射. 且对任意的 $m, n \in \mathbb{Z}$, 有

$$\phi(m+n) = (-1)^{m+n} = (-1)^m \cdot (-1)^n = \phi(m) \cdot \phi(n).$$

因此 ϕ 是 $(\mathbb{Z}, +)$ 到 $(\mathbb{R}^*, \cdot)$ 的同态映射.

例 74

设 $\mathbb{R}[x]$ 为全体实系数多项式关于多项式的加法所构成的群. 令

$$\begin{aligned} \phi: \quad \mathbb{R}[x] &\longrightarrow \mathbb{R}[x] \\ f(x) &\longmapsto f'(x) \qquad \text{(即 } f(x) \text{ 的导数)}, \end{aligned}$$

则 ϕ 是 $\mathbb{R}[x]$ 到它自身的映射. 且对任意的 $f(x), g(x) \in \mathbb{R}[x]$, 有

$$\begin{aligned} \phi(f(x)+g(x)) &= (f(x)+g(x))' \\ &= f'(x)+g'(x) \\ &= \phi(f(x))+\phi(g(x)) \end{aligned}$$

所以 ϕ 是 $\mathbb{R}[x]$ 到它自身的同态映射. 易知, 这是一个满同态.

例 75

设 G 为群, H 是 G 的正规子群. 对商群 G/H, 令

$$\eta : G \longrightarrow G/H,$$
$$a \longmapsto aH,$$

则 η 是满映射, 且对任意 $a, b \in G$, 有

$$\eta(ab) = (ab)H = aH \cdot bH = \eta(a)\eta(b),$$

所以 η 是 G 到它的商群 G/H 的同态映射. 通常称这样的同态映射为**自然同态** (natural homomorphism).

例 76

设 G 是群, ι 是 G 的恒等映射:

$$\begin{aligned} \iota: G &\longrightarrow G, \\ a &\longmapsto a, \quad \forall a \in G, \end{aligned}$$

显然 ι 是一一映射. 又对任意的 $a, b \in G$,

$$\iota(ab) = ab = \iota(a)\iota(b),$$

所以, ι 是 G 的一个自同构, 这个同构称为**恒等同构**.

例 77

设 $\mathbb{R}$ 是全体实数组成的加法群, $\mathbb{R}^+$ 表示全体正实数组成的乘法群, 则群 $\mathbb{R}$ 与 $\mathbb{R}^+$ 同构.

例 77

设 $\mathbb{R}$ 是全体实数组成的加法群, $\mathbb{R}^+$ 表示全体正实数组成的乘法群, 则群 $\mathbb{R}$ 与 $\mathbb{R}^+$ 同构.

证明: (1) 对任意的 $x \in \mathbb{R}$, 令

$$\phi(x) = 2^x,$$

则 ϕ 是 $\mathbb{R}$ 到 $\mathbb{R}^+$的映射.

例 77

设 $\mathbb{R}$ 是全体实数组成的加法群, $\mathbb{R}^+$ 表示全体正实数组成的乘法群, 则群 $\mathbb{R}$ 与 $\mathbb{R}^+$ 同构.

证明: (1) 对任意的 $x \in \mathbb{R}$, 令

$$\phi(x) = 2^x,$$

则 ϕ 是 $\mathbb{R}$ 到 $\mathbb{R}^+$的映射. (2) 设 $x, y \in \mathbb{R}$, 如果 $\phi(x) = \phi(y)$, 即 $2^x = 2^y$, 则 $x = y$. 所以 ϕ 是 $\mathbb{R}$ 到 $\mathbb{R}^+$ 的单映射.

例 77

设 $\mathbb{R}$ 是全体实数组成的加法群, $\mathbb{R}^+$ 表示全体正实数组成的乘法群, 则群 $\mathbb{R}$ 与 $\mathbb{R}^+$ 同构.

证明: (1) 对任意的 $x \in \mathbb{R}$, 令

$$\phi(x) = 2^x,$$

则 ϕ 是 $\mathbb{R}$ 到 $\mathbb{R}^+$的映射. (2) 设 $x, y \in \mathbb{R}$, 如果 $\phi(x) = \phi(y)$, 即 $2^x = 2^y$, 则 $x = y$. 所以 ϕ 是 $\mathbb{R}$ 到 $\mathbb{R}^+$ 的单映射. (3) 对任意的 $r \in \mathbb{R}^+$, 令 $x = \log_2 r$, 则 $x \in \mathbb{R}$, 且

$$\phi(x) = 2^x = 2^{\log_2 r} = r,$$

所以 ϕ 是 $\mathbb{R}$ 到 $\mathbb{R}^+$的满映射.

例 77

设 $\mathbb{R}$ 是全体实数组成的加法群, $\mathbb{R}^+$ 表示全体正实数组成的乘法群, 则群 $\mathbb{R}$ 与 $\mathbb{R}^+$ 同构.

证明: (1) 对任意的 $x \in \mathbb{R}$, 令

$$\phi(x) = 2^x,$$

则 ϕ 是 $\mathbb{R}$ 到 $\mathbb{R}^+$的映射. (2) 设 $x, y \in \mathbb{R}$, 如果 $\phi(x) = \phi(y)$, 即 $2^x = 2^y$, 则 $x = y$. 所以 ϕ 是 $\mathbb{R}$ 到 $\mathbb{R}^+$ 的单映射. (3) 对任意的 $r \in \mathbb{R}^+$, 令 $x = \log_2 r$, 则 $x \in \mathbb{R}$, 且

$$\phi(x) = 2^x = 2^{\log_2 r} = r,$$

所以 ϕ 是 $\mathbb{R}$ 到 $\mathbb{R}^+$的满映射. (4) 对任意的 $x, y \in \mathbb{R}$,

$$\phi(x + y) = 2^{x+y} = 2^x \cdot 2^y = \phi(x) \cdot \phi(y),$$

所以 ϕ 保持运算. 从而 ϕ 是 $\mathbb{R}$ 到 $\mathbb{R}^+$ 的同构映射.

例 78

由例 12 知全体 n 次单位根组成的集合 $U_n = \{\mathrm{e}^{\frac{2\pi ik}{n}} \mid 0 \leq k \leq n-1\}$ 关于数的乘法构成群. 由例 13 知 $\mathbb{Z}$ 的模 n 剩余类可构成加群 $(\mathbb{Z}_n, +)$.

例 78

由例 12 知全体 n 次单位根组成的集合 $U_n=\{\mathrm{e}^{\frac{2\pi ik}{n}}\mid 0\le k\le n-1\}$ 关于数的乘法构成群. 由例 13 知 $\mathbb{Z}$ 的模 n 剩余类可构成加群 $(\mathbb{Z}_n,+)$. 作映射

$$\begin{aligned}\phi:\quad U_n &\longrightarrow (\mathbb{Z}_n,+),\\ \mathrm{e}^{\frac{2\pi ik}{n}} &\longmapsto \bar{k}.\end{aligned}$$

例 78

由例 12 知全体 n 次单位根组成的集合 $U_n=\{\mathrm{e}^{\frac{2\pi ik}{n}} \mid 0\le k\le n-1\}$ 关于数的乘法构成群. 由例 13 知 $\mathbb{Z}$ 的模 n 剩余类可构成加群 $(\mathbb{Z}_n,+)$. 作映射

$$\begin{aligned}\phi:\quad U_n &\longrightarrow (\mathbb{Z}_n,+),\\ \mathrm{e}^{\frac{2\pi ik}{n}} &\longmapsto \bar{k}.\end{aligned}$$

则有

$$\begin{aligned}\phi\left(\mathrm{e}^{\frac{2\pi ik}{n}}\cdot\mathrm{e}^{\frac{2\pi ik'}{n}}\right) &= \phi\left(\mathrm{e}^{\frac{2\pi i(k+k')}{n}}\right)\\ &= \overline{k+k'}=\bar{k}+\bar{k'}\\ &= \phi\left(\mathrm{e}^{\frac{2\pi in}{n}}\right)+\phi\left(\mathrm{e}^{\frac{2\pi ib}{n}}\right),\end{aligned}$$

所以 ϕ 是群同态, 显然 ϕ 是一一映射, 从而 ϕ 为群同构.

定理 79

设 ϕ 是群 G 到群 G' 的同态映射, e 与 e' 分别是 G 与 G' 的单位元, $a \in G$, 则

(1) ϕ 将 G 的单位元映到 G' 的单位元, 即 $\phi(e) = e'$;
(2) ϕ 将 a 的逆元映到 $\phi(a)$ 的逆元, 即 $\phi\left(a^{-1}\right) = (\phi(a))^{-1}$;
(3) 设 n 是任一整数, 则 $\phi\left(a^{n}\right) = (\phi(a))^{n}$;
(4) 如果 $\operatorname{ord} a$ 有限, 则 $\operatorname{ord} \phi(a) \mid \operatorname{ord} a$.

证明

(1) 因 e 与 e' 分别是 G 与 G' 的单位元, 所以对 $\forall a \in G$ 有

$$\phi(a)e' = \phi(a) = \phi(ae) = \phi(a)\phi(e),$$

从而由消去律得

$$e' = \phi(e),$$

即 $\phi(e)$ 为 G' 的单位元.

(2) 直接计算可得

$$\phi(a)\phi\left(a^{-1}\right) = \phi\left(aa^{-1}\right) = \phi(e) = e' = \phi(a)(\phi(a))^{-1}.$$

由消去律得

$$\phi\left(a^{-1}\right) = (\phi(a))^{-1},$$

即 $\phi\left(a^{-1}\right)$ 为 $\phi(a)$ 的逆元.

证明 (续)

(3) 当 $n=0$ 时,

$$\phi\left(a^{0}\right)=\phi(e)=e'=(\phi(a))^{0}.$$

当 $n>0$ 时,

$$\begin{aligned}\phi\left(a^{n}\right)=\phi\left(a^{n-1}a\right)&=\phi\left(a^{n-1}\right)\phi(a)\\&=\cdots=(\phi(a))^{n-1}\phi(a)=(\phi(a))^{n}.\end{aligned}$$

当 $n<0$ 时,

$$\begin{aligned}\phi\left(a^{n}\right)=\phi\left(\left(a^{-1}\right)^{-n}\right)&=\left(\phi\left(a^{-1}\right)\right)^{-n}\\&=\left(\phi(a)^{-1}\right)^{-n}=(\phi(a))^{n}.\end{aligned}$$

(4) 设 ord $a=r$, 则

$$(\phi(a))^{r}=\phi\left(a^{r}\right)=\phi(e)=e',$$

所以 $\operatorname{ord}\phi(a)\mid\operatorname{ord}a$.

同构的性质

定理 80

设 ϕ 是群 G 到 G' 的同构映射, e 与 e' 分别是 G 与 G' 的单位元, 则 ϕ 是可逆映射, 且 ϕ 的逆映射 ϕ^{-1} 是群 G' 到群 G 的同构映射.

同构的性质

定理 80

设 ϕ 是群 G 到 G' 的同构映射, e 与 e' 分别是 G 与 G' 的单位元, 则 ϕ 是可逆映射, 且 ϕ 的逆映射 ϕ^{-1} 是群 G' 到群 G 的同构映射.

证明: ϕ 是群 G 到 G' 的一一映射, 所以 ϕ 是可逆的映射, 且其逆映射 ϕ^{-1} 是 G' 到 G 的一一映射. 下面证明 ϕ^{-1} 为同态映射.

证明 (续)

对任意的 $a', b' \in G'$, 由于可逆映射是满映射, 所以存在 $a, b \in G$, 使

$$\phi(a) = a', \quad \phi(b) = b'.$$

对任意的 $a', b' \in G'$, 由于可逆映射是满映射, 所以存在 $a, b \in G$, 使

$$\phi(a) = a', \quad \phi(b) = b'.$$

于是, $\phi^{-1}(a') = a$, $\phi^{-1}(b') = b$, 并且

$$\begin{aligned} \phi^{-1}\left(a'b'\right) &= \phi^{-1}(\phi(a)\phi(b)) \\ &= \phi^{-1}(\phi(ab)) \\ &= \left(\phi^{-1} \circ \phi\right)(ab) \\ &= ab \\ &= \phi^{-1}\left(a'\right)\phi^{-1}\left(b'\right), \end{aligned}$$

这就证明了 ϕ^{-1} 是 G' 到 G 的同构映射.

例 81

设 $\mathbb{R}_+^*$ 为所有正实数构成的乘法群, 则指数函数

$$\begin{aligned} \exp: \ \mathbb{R} &\longrightarrow \mathbb{R}_+^*, \\ x &\longmapsto 2^x, \end{aligned}$$

是群同构. 其逆为对数函数

$$\begin{aligned} \mathrm{lb}: \ \mathbb{R}_+^* &\longrightarrow \mathbb{R}, \\ y &\longmapsto \log_2 y. \end{aligned}$$

例 81

设 $\mathbb{R}_+^*$ 为所有正实数构成的乘法群, 则指数函数

$$\begin{aligned} \exp: \ \mathbb{R} &\longrightarrow \mathbb{R}_+^*, \\ x &\longmapsto 2^x, \end{aligned}$$

是群同构. 其逆为对数函数

$$\begin{aligned} \mathrm{lb}: \ \mathbb{R}_+^* &\longrightarrow \mathbb{R}, \\ y &\longmapsto \log_2 y. \end{aligned}$$

注 81.1

设群 G 与 G' 同构. 如果 G 是交换群, 则 G' 也是交换群; 如果 G 是有限群, 则 G' 也是有限群且 $|G| = |G'|$.

同构的性质

定理 82

群的同构是一个等价关系, 即

(1) $G \cong G$ (反身性);

(2) 若 $G \cong G'$, 则 $G' \cong G$ (对称性);

(3) 若 $G \cong G', G' \cong G''$, 则 $G \cong G''$ (传递性), 其中 G, G', G'' 都是群.

证明

(1) 见例 76.

(2) 由定理 80 立即可证.

证明

(1) 见例 76.

(2) 由定理 80 立即可证. (3) 设 ϕ 是 G 到 G' 的同构映射, ψ 是 G' 到 G'' 的同构映射. 由映射复合的性质知 $\psi \circ \phi$ 是 G 到 G'' 的一一映射.

证明

(1) 见例 76.

(2) 由定理 80 立即可证. (3) 设 ϕ 是 G 到 G' 的同构映射, ψ 是 G' 到 G'' 的同构映射. 由映射复合的性质知 $\psi \circ \phi$ 是 G 到 G'' 的一一映射. 又对任意的 $x, y \in G$ 有

$$\begin{aligned}(\psi \circ \phi)(xy) &= \psi(\phi(xy)) \\ &= \psi(\phi(x)\phi(y)) \\ &= \psi(\phi(x))\psi(\phi(y)) \\ &= (\psi \circ \phi)(x)(\psi \circ \phi)(y).\end{aligned}$$

所以 $\psi \circ \phi$ 是 G 到 G'' 的同构映射, 从而 $G \cong G''$.

(原) 象集

定义 83

设 ϕ 为群 G 到群 G' 的映射, A, B 分别为 G 与 G' 的非空子集. 记

$$\phi(A) = \{\phi(x) \mid x \in A\},$$
$$\phi^{-1}(B) = \{x \in G \mid \phi(x) \in B\},$$

则 $\phi(A)$ 与 $\phi^{-1}(B)$ 分别是 G' 与 G 的非空子集 ($\phi^{-1}(B)$ 仅仅是一个集合的记号, 并不表示映射 ϕ 是可逆的). $\phi(A)$ 与 $\phi^{-1}(B)$ 分别称为子集 A 与 B 在 ϕ 下的象集与原象集.

定理 84

设 ϕ 是群 G 到 G' 的同态映射, H 与 K 分别是 G 与 G' 的子群, 则

(1) $\phi(H)$ 是 G' 的子群;
(2) $\phi^{-1}(K)$ 是 G 的子群;
(3) 如果 H 是 G 的正规子群, 则 $\phi(H)$ 是 $\phi(G)$ 的正规子群;
(4) 如果 K 是 G' 的正规子群, 则 $\phi^{-1}(K)$ 是 G 的正规子群.

同态的性质

定理 84

设 ϕ 是群 G 到 G' 的同态映射, H 与 K 分别是 G 与 G' 的子群, 则

(1) $\phi(H)$ 是 G' 的子群;
(2) $\phi^{-1}(K)$ 是 G 的子群;
(3) 如果 H 是 G 的正规子群, 则 $\phi(H)$ 是 $\phi(G)$ 的正规子群;
(4) 如果 K 是 G' 的正规子群, 则 $\phi^{-1}(K)$ 是 G 的正规子群.

证明: (1) 对任意的 $h_1, h_2 \in H$, 有 $h_1 h_2^{-1} \in H$, 所以

$$\phi(h_1)(\phi(h_2))^{-1} = \phi(h_1)\phi\left(h_2^{-1}\right) = \phi\left(h_1 h_2^{-1}\right) \in \phi(H),$$

所以 $\phi(H)$ 是 G' 的子群.

证明 (续)

(2) 对任意的 $a, b \in \phi^{-1}(K)$, 有 $\phi(a), \phi(b) \in K$, 则

$$\phi\left(ab^{-1}\right) = \phi(a)\phi\left(b^{-1}\right) = \phi(a)\phi(b)^{-1} \in K,$$

于是 $ab^{-1} \in \phi^{-1}(K)$, 所以 $\phi^{-1}(K)$ 是 G 的子群.

证明 (续)

(2) 对任意的 $a, b \in \phi^{-1}(K)$, 有 $\phi(a), \phi(b) \in K$, 则
$$\phi\left(ab^{-1}\right) = \phi(a)\phi\left(b^{-1}\right) = \phi(a)\phi(b)^{-1} \in K,$$
于是 $ab^{-1} \in \phi^{-1}(K)$, 所以 $\phi^{-1}(K)$ 是 G 的子群.(3) 由 (1) 知, $\phi(H)$ 是 $\phi(G)$ 的子群. 又对任意的 $a' \in \phi(G), h' \in \phi(H)$, 存在 $a \in G, h \in H$ 使得 $\phi(a) = a', \phi(h) = h'$, 则 $aha^{-1} \in H$. 于是
$$\begin{aligned} a'h'a'^{-1} &= \phi(a)\phi(h)(\phi(a))^{-1} = \phi(a)\phi(h)\phi\left(a^{-1}\right) \\ &= \phi\left(aha^{-1}\right) \in \phi(H), \end{aligned}$$
所以 $\phi(H)$ 是 $\phi(G)$ 的正规子群.

证明 (续)

(2) 对任意的 $a, b \in \phi^{-1}(K)$, 有 $\phi(a), \phi(b) \in K$, 则

$$\phi\left(ab^{-1}\right) = \phi(a)\phi\left(b^{-1}\right) = \phi(a)\phi(b)^{-1} \in K,$$

于是 $ab^{-1} \in \phi^{-1}(K)$, 所以 $\phi^{-1}(K)$ 是 G 的子群.(3) 由 (1) 知, $\phi(H)$ 是 $\phi(G)$ 的子群. 又对任意的 $a' \in \phi(G), h' \in \phi(H)$, 存在 $a \in G, h \in H$ 使得 $\phi(a) = a', \phi(h) = h'$, 则 $aha^{-1} \in H$. 于是

$$\begin{aligned} a'h'a'^{-1} &= \phi(a)\phi(h)(\phi(a))^{-1} = \phi(a)\phi(h)\phi\left(a^{-1}\right) \\ &= \phi\left(aha^{-1}\right) \in \phi(H), \end{aligned}$$

所以 $\phi(H)$ 是 $\phi(G)$ 的正规子群.(4) 由 (2) 知, $\phi^{-1}(K)$ 是 G 的子群. 又对任意的 $a \in G, h \in \phi^{-1}(K)$, 则 $\phi(h) \in K$, 而 K 是 G' 的正规子群, 故

$$\phi\left(aha^{-1}\right) = \phi(a)\phi(h)\phi(a)^{-1} \in K.$$

从而 $aha^{-1} \in \phi^{-1}(K)$, 所以 $\phi^{-1}(K)$ 是 G 的正规子群.

同态的核

定义 85

设 ϕ 是群 G 到 G' 的同态映射, e' 是 G' 的单位元, 则称 e' 在 G 中的原象集

$$\phi^{-1}\left(\{e'\}\right) = \{a \in G \mid \phi(a) = e'\}$$

为同态映射 ϕ 的**核** (kernel), 记作 $\operatorname{Ker}\phi$.

同态的核

定义 85

设 ϕ 是群 G 到 G' 的同态映射, e' 是 G' 的单位元, 则称 e' 在 G 中的原象集

$$\phi^{-1}\left(\{e'\}\right) = \{a \in G \mid \phi(a) = e'\}$$

为同态映射 ϕ 的**核** (kernel), 记作 $\operatorname{Ker}\phi$.

定理 86

设 ϕ 是群 G 到 G' 的同态映射, 则 $\operatorname{Ker}\phi$ 是 G 的正规子群.

同态的核

定义 85

设 ϕ 是群 G 到 G' 的同态映射, e' 是 G' 的单位元, 则称 e' 在 G 中的原象集

$$\phi^{-1}\left(\{e'\}\right) = \{a \in G \mid \phi(a) = e'\}$$

为同态映射 ϕ 的核 (kernel), 记作 $\operatorname{Ker}\phi$.

定理 86

设 ϕ 是群 G 到 G' 的同态映射, 则 $\operatorname{Ker}\phi$ 是 G 的正规子群.

证明: 易知 $\{e'\}$ 是 G' 的正规子群. 从而由定理 84 第 (4) 条知 $\operatorname{Ker}\phi$ 是 G 的正规子群.

同态的核

定义 85

设 ϕ 是群 G 到 G' 的同态映射, e' 是 G' 的单位元, 则称 e' 在 G 中的原象集

$$\phi^{-1}\left(\{e'\}\right) = \{a \in G \mid \phi(a) = e'\}$$

为同态映射 ϕ 的**核** (kernel), 记作 $\operatorname{Ker}\phi$.

定理 86

设 ϕ 是群 G 到 G' 的同态映射, 则 $\operatorname{Ker}\phi$ 是 G 的正规子群.

证明: 易知 $\{e'\}$ 是 G' 的正规子群. 从而由定理 84 第 (4) 条知 $\operatorname{Ker}\phi$ 是 G 的正规子群.

例 87

例 72 至例 75 中的同态映射的核分别是

$$G,\ 2\mathbb{Z},\ \mathbb{R},\ H.$$

例 88

试求 $(\mathbb{Z}_{12},+)$ 到 $(\mathbb{Z}_{18},+)$ 的所有同态映射, 并求每一个同态映射的核.

例 88

试求 $(\mathbb{Z}_{12},+)$ 到 $(\mathbb{Z}_{18},+)$ 的所有同态映射, 并求每一个同态映射的核.

证明: 设 ϕ 是 $\mathbb{Z}_{12}$ 到 $\mathbb{Z}_{18}$ 的任一同态映射. 因为 $\mathbb{Z}_{12}$ 是循环群, 所以 ϕ 由 $\phi(\overline{1})$ 完全确定. 因 $\operatorname{ord}\overline{1}=12$, 从而由定理 79 第 (4) 条知 $\operatorname{ord}\phi(\overline{1}) \mid 12$.

例 88

试求 $(\mathbb{Z}_{12},+)$ 到 $(\mathbb{Z}_{18},+)$ 的所有同态映射, 并求每一个同态映射的核.

证明: 设 ϕ 是 $\mathbb{Z}_{12}$ 到 $\mathbb{Z}_{18}$ 的任一同态映射. 因为 $\mathbb{Z}_{12}$ 是循环群, 所以 ϕ 由 $\phi(\overline{1})$ 完全确定. 因 $\operatorname{ord}\overline{1}=12$, 从而由定理 79 第 (4) 条知 $\operatorname{ord}\phi(\overline{1})\mid 12$. 又因为 $\operatorname{ord}\phi(\overline{1})||\mathbb{Z}_{18}|=18$, 所以

$$\operatorname{ord}\phi(\overline{1})\mid(12,18)=6,$$

所以 $\phi(\overline{1})$ 的可能的取值为

$$\overline{0},\overline{9},\overline{6},\overline{12},\overline{3},\overline{15}.$$

例 88

试求 $(\mathbb{Z}_{12},+)$ 到 $(\mathbb{Z}_{18},+)$ 的所有同态映射，并求每一个同态映射的核.

证明: 设 ϕ 是 $\mathbb{Z}_{12}$ 到 $\mathbb{Z}_{18}$ 的任一同态映射. 因为 $\mathbb{Z}_{12}$ 是循环群，所以 ϕ 由 $\phi(\bar{1})$ 完全确定. 因 $\operatorname{ord}\bar{1}=12$，从而由定理 79 第 (4) 条知 $\operatorname{ord}\phi(\bar{1})\mid 12$. 又因为 $\operatorname{ord}\phi(\bar{1})||\mathbb{Z}_{18}|=18$，所以

$$\operatorname{ord}\phi(\bar{1})\mid(12,18)=6,$$

所以 $\phi(\bar{1})$ 的可能的取值为

$$\bar{0},\bar{9},\bar{6},\overline{12},\bar{3},\overline{15}.$$

由此得对应的同态映射与相应的核分别为

$$\begin{aligned}
\phi_1(\bar{x})&=\bar{0}, &\quad \operatorname{Ker}\phi_1&=\mathbb{Z}_{12};\\
\phi_2(\bar{x})&=9\bar{x}, &\quad \operatorname{Ker}\phi_2&=2\mathbb{Z}_{12};\\
\phi_3(\bar{x})&=6\bar{x}, &\quad \operatorname{Ker}\phi_3&=3\mathbb{Z}_{12};\\
\phi_4(\bar{x})&=12\bar{x}, &\quad \operatorname{Ker}\phi_4&=3\mathbb{Z}_{12};\\
\phi_5(\bar{x})&=3\bar{x}, &\quad \operatorname{Ker}\phi_5&=6\mathbb{Z}_{12};\\
\phi_6(\bar{x})&=15\bar{x}, &\quad \operatorname{Ker}\phi_6&=6\mathbb{Z}_{12}.
\end{aligned}$$

定理 89 (群同态基本定理)

设 ϕ 是群 G 到群 G' 的满同态, $K = \operatorname{Ker}\phi$, 则
$$G/K \cong G'.$$

定理 89 (群同态基本定理)

设 ϕ 是群 G 到群 G' 的满同态, $K = \operatorname{Ker}\phi$, 则
$$G/K \cong G'.$$

证明: 由定理 86 知, K 是 G 的正规子群, 所以有商群 G/K. 令
$$\begin{array}{rccc} \tilde{\phi}: & G/K & \longrightarrow & G', \\ & aK & \longmapsto & \phi(a). \end{array}$$

(1) 如果 $aK = bK$, 则 $a^{-1}b \in K$, 于是 $\phi\left(a^{-1}b\right) = e'$, 所以 $\phi(a) = \phi(b)$, 即 $\widetilde{\phi}(aK) = \widetilde{\phi}(bK)$. 这说明, $\widetilde{\phi}$ 的定义与代表元的选取无关, 从而 $\widetilde{\phi}$ 为 G/K 到 G' 的映射.

证明 (续)

(2) 对任意的 $a' \in G'$, 因为 ϕ 是满映射, 所以存在 $a \in G$ 使得 $\phi(a) = a'$. 从而

$$\widetilde{\phi}(aK) = \phi(a) = a',$$

因此, $\widetilde{\phi}$ 是 G/K 到 G' 的满映射.

(3) 如果 $\phi(a) = \phi(b)$, 则

$$\phi\left(a^{-1}b\right) = (\phi(a))^{-1}\phi(b) = e'.$$

于是 $a^{-1}b \in K$, 由此得 $aK = bK$. 所以 $\widetilde{\phi}$ 是 G/K 到 G' 的单映射.

(4) 对任意的 $aK, bK \in G/K$, 有

$$\begin{aligned}\widetilde{\phi}(aK \cdot bK) &= \widetilde{\phi}(abK) = \phi(ab) = \phi(a)\phi(b) \\ &= \widetilde{\phi}(aK)\widetilde{\phi}(bK).\end{aligned}$$

所以

$$\widetilde{\phi}: \quad G/K \cong G'.$$

例 90

设 m 是任一大于 1 的正整数. 令

$$\begin{array}{rccc} \phi: & \mathbb{Z} & \longrightarrow & \mathbb{Z}_m, \\ & a & \longmapsto & \bar{a}. \end{array}$$

例 90

设 m 是任一大于 1 的正整数. 令

$$\begin{array}{rrcl} \phi: & \mathbb{Z} & \longrightarrow & \mathbb{Z}_m, \\ & a & \longmapsto & \bar{a}. \end{array}$$

(1) 显然 ϕ 为 $\mathbb{Z}$ 到 $\mathbb{Z}_m$ 的映射.

例 90

设 m 是任一大于 1 的正整数. 令

$$\begin{array}{rccc} \phi: & \mathbb{Z} & \longrightarrow & \mathbb{Z}_m, \\ & a & \longmapsto & \bar{a}. \end{array}$$

(1) 显然 ϕ 为 $\mathbb{Z}$ 到 $\mathbb{Z}_m$ 的映射. (2) 对任意的 $\bar{a} \in \mathbb{Z}_m$, 有 $a \in \mathbb{Z}$, 使 $\phi(a) = \bar{a}$, 所以 ϕ 为 $\mathbb{Z}$ 到 $\mathbb{Z}_m$ 的满映射.

例 90

设 m 是任一大于 1 的正整数. 令

$$\begin{array}{rccc} \phi: & \mathbb{Z} & \longrightarrow & \mathbb{Z}_m, \\ & a & \longmapsto & \bar{a}. \end{array}$$

(1) 显然 ϕ 为 $\mathbb{Z}$ 到 $\mathbb{Z}_m$ 的映射. (2) 对任意的 $\bar{a} \in \mathbb{Z}_m$, 有 $a \in \mathbb{Z}$, 使 $\phi(a) = \bar{a}$, 所以 ϕ 为 $\mathbb{Z}$ 到 $\mathbb{Z}_m$ 的满映射. (3) 对任意的 $a, b \in \mathbb{Z}$, 有

$$\phi(a+b) = \overline{a+b} = \bar{a} + \bar{b} = \phi(a) + \phi(b)$$

所以 ϕ 为 $\mathbb{Z}$ 到 $\mathbb{Z}_m$ 的满同态.

例 90

设 m 是任一大于 1 的正整数. 令

$$\begin{array}{rccc} \phi: & \mathbb{Z} & \longrightarrow & \mathbb{Z}_m, \\ & a & \longmapsto & \bar{a}. \end{array}$$

(1) 显然 ϕ 为 $\mathbb{Z}$ 到 $\mathbb{Z}_m$ 的映射. (2) 对任意的 $\bar{a} \in \mathbb{Z}_m$, 有 $a \in \mathbb{Z}$, 使 $\phi(a) = \bar{a}$, 所以 ϕ 为 $\mathbb{Z}$ 到 $\mathbb{Z}_m$ 的满映射. (3) 对任意的 $a, b \in \mathbb{Z}$, 有

$$\phi(a+b) = \overline{a+b} = \bar{a} + \bar{b} = \phi(a) + \phi(b)$$

所以 ϕ 为 $\mathbb{Z}$ 到 $\mathbb{Z}_m$ 的满同态. (4) 同态的核

$$\begin{aligned} \operatorname{Ker}\phi &= \{x \in \mathbb{Z} \mid \phi(x) = \bar{0}\} \\ &= \{x \in \mathbb{Z} \mid \bar{x} = \bar{0}\} \\ &= \{x \in \mathbb{Z} | m | x\} = \langle m \rangle. \end{aligned}$$

从而由同态基本定理得

$$\tilde{\phi}: \quad \mathbb{Z}/\langle m \rangle \cong \mathbb{Z}_m.$$

证明同构的基本步骤

应用群同态基本定理证明群的同构, 一般有以下五个步骤:

证明同构的基本步骤

应用群同态基本定理证明群的同构, 一般有以下五个步骤:

第一步 建立群 G 与群 G' 的元素之间的对应关系 ϕ, 并证明 ϕ 为 G 到 G' 的映射;

证明同构的基本步骤

应用群同态基本定理证明群的同构, 一般有以下五个步骤:

第一步 建立群 G 与群 G' 的元素之间的对应关系 ϕ, 并证明 ϕ 为 G 到 G' 的映射;

第二步 证明 ϕ 为 G 到 G' 的满映射;

证明同构的基本步骤

应用群同态基本定理证明群的同构, 一般有以下五个步骤:

第一步 建立群 G 与群 G' 的元素之间的对应关系 ϕ, 并证明 ϕ 为 G 到 G' 的映射;

第二步 证明 ϕ 为 G 到 G' 的满映射;

第三步 证明 ϕ 为 G 到 G' 的同态映射;

证明同构的基本步骤

应用群同态基本定理证明群的同构, 一般有以下五个步骤:

第一步 建立群 G 与群 G' 的元素之间的对应关系 ϕ, 并证明 ϕ 为 G 到 G' 的映射;

第二步 证明 ϕ 为 G 到 G' 的满映射;

第三步 证明 ϕ 为 G 到 G' 的同态映射;

第四步 计算同态的核 $\mathrm{Ker}\,\phi$;

证明同构的基本步骤

应用群同态基本定理证明群的同构, 一般有以下五个步骤:

第一步 建立群 G 与群 G' 的元素之间的对应关系 ϕ, 并证明 ϕ 为 G 到 G' 的映射;

第二步 证明 ϕ 为 G 到 G' 的满映射;

第三步 证明 ϕ 为 G 到 G' 的同态映射;

第四步 计算同态的核 $\mathrm{Ker}\,\phi$;

第五步 应用群同态基本定理得 $G/\mathrm{Ker}\phi \cong G'$.

例

例 91

设群 $U_4 = \{1, -1, \mathrm{i}, -\mathrm{i}\}$ 是 4 次单位根群, $K = \{e, a, b, ab\}$ (Klein 四元群, 它是最小的非循环群) 是由元素 a, b 及关系 $a^2 = b^2 = e$ 和 $ab = ba$ 所定义的群. 问 U_4 与 K 是否同构, 为什么?

例 91

设群 $U_4 = \{1, -1, \mathrm{i}, -\mathrm{i}\}$ 是 4 次单位根群, $K = \{e, a, b, ab\}$ (Klein 四元群, 它是最小的非循环群) 是由元素 a, b 及关系 $a^2 = b^2 = e$ 和 $ab = ba$ 所定义的群. 问 U_4 与 K 是否同构, 为什么?

证明: 如果 U_4 与 K 同构, 设 ϕ 是 U_4 到 K 的同构映射. 令 $\phi(\mathrm{i}) = x$. 易知, $x^2 = e$. 从而

$$\phi(-1) = \phi\left(\mathrm{i}^2\right) = (\phi(\mathrm{i}))^2 = x^2 = e.$$

另一方面, $\phi(1) = e$. 由于 ϕ 是单映射, 所以 $-1 = 1$. 这是一个矛盾. 从而知 U_4 与 K 不同构.

例 92

4 阶群必同构于 U_4 或 Klein 四元群 $K = \{e, a, b, ab\}$.

例 92

4 阶群必同构于 U_4 或 Klein 四元群 $K=\{e,a,b,ab\}$.

证明: 设 H 为一个 4 阶群.

(1) 如果 H 有 4 阶元, 则 H 为 4 阶循环群, 从而 H 与 U_4 同构.

(2) 如果 H 不含有 4 阶元, 则除单位元 e 外, H 的其余三个元素的阶都是 2, 不妨设这三个元素为 $a, b, ab = ba$. 显然 H 是交换群. 从而 H 的元素与 K 的元素一一对应, 且有完全一致的运算关系. 所以 H 与 K 同构.

§2.5 群的同态和同构

- 同态与同构
- 同态的性质
- 同构的性质
- 同态的核
- 同态基本定理
- 同构的证明步骤

§2.6 循环群

- 循环群的定义
- 循环群的例子
- 循环群的生成元
- 循环群的子群
- 循环群的结构

循环群的定义

定义 93

设 G 是群, 如果存在 $a \in G$, 使得 $G = \langle a \rangle$, 则称 G 为**一个循环群** (cyclic group), 并称 a 为 G 的**一个生成元** (generator). 当 G 的元素个数无限时, 称 G 为**无限循环群**; 当 G 的元素个数为 n 时, 称 G 为 n **阶循环群**.

循环群的定义

定义 93

设 G 是群, 如果存在 $a \in G$, 使得 $G = \langle a \rangle$, 则称 G **为一个循环群** (cyclic group), 并称 a 为 G **的一个生成元** (generator). 当 G 的元素个数无限时, 称 G 为**无限循环群**; 当 G 的元素个数为 n 时, 称 G 为 n **阶循环群**.

注 93.1

由循环群的定义易见以下结论:

(1) 如果 $G = \langle a \rangle$ 是 n 阶循环群, 则 $G = \left\{e, a, a^2, a^3, \cdots, a^{n-1}\right\}$. 显然有 $\operatorname{ord} a = n$ 并且 $a^{k+tn} = a^k a^{tn} = a^k e = a^k$, 其中 $k, t \in \mathbb{Z}$. 进一步, 对任意 $k, l \in \mathbb{Z}$, 若有 $a^k = a^l$, 则 $a^{k-l} = e$. 由定理 *49* 第 *(2)* 条知 $n \mid k - l$, 于是 $a^k = a^l \Leftrightarrow n \mid k - l$.

(2) 如果 G 为无限循环群, 则由定理 *33* 知 $G = \left\{e, a, a^{-1}, a^2, a^{-2}, a^3, a^{-3}, \cdots\right\}$, 并且 $\operatorname{ord} a = \infty$. 对任意 $k, l \in \mathbb{Z}$, 若有由 $a^k = a^l$, 则 $a^{k-l} = e$, 于是 $k = l$.

例 94

整数加群 $\mathbb{Z}$ 是无限循环群.

例 94

整数加群 $\mathbb{Z}$ 是无限循环群.

证明: 显然, $\mathbb{Z}$ 是无限群. 又因为

$$\mathbb{Z} = \{n \cdot 1 \mid n \in \mathbb{Z}\},$$

所以 $\mathbb{Z} = \langle 1 \rangle$. 容易看出, $\mathbb{Z} = \langle -1 \rangle$, 所以 1 与 -1 都是 $\mathbb{Z}$ 的生成元. 并且对任意的 $d \in \mathbb{Z}, d \neq \pm 1$, 显然有 $1 \notin \langle d \rangle$, 所以 $\langle d \rangle \neq \mathbb{Z}$. 从而知, 1 与 -1 是群 $\mathbb{Z}$ 的仅有的两个生成元.

例 95

设 m 为正整数, 则模 m 剩余类加群

$$\begin{aligned}\mathbb{Z}_m &= \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{m-1}\} \\ &= \{0 \cdot \overline{1}, 1 \cdot \overline{1}, 2 \cdot \overline{1}, \cdots, (m-1) \cdot \overline{1}\} = \langle \overline{1} \rangle,\end{aligned}$$

所以 $\mathbb{Z}_m$ 是 m 阶循环群.

例 95

设 m 为正整数, 则模 m 剩余类加群

$$\begin{aligned}\mathbb{Z}_m &= \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{m-1}\} \\ &= \{0\cdot\overline{1}, 1\cdot\overline{1}, 2\cdot\overline{1}, \cdots, (m-1)\cdot\overline{1}\} = \langle\overline{1}\rangle,\end{aligned}$$

所以 $\mathbb{Z}_m$ 是 m 阶循环群.

例 96

容易计算在 $\mathbb{Z}_5^*$ 中, $\operatorname{ord} 2 = \operatorname{ord} 3 = |\mathbb{Z}_5^*| = 4$, 所以 $\mathbb{Z}_5^*$ 是 4 阶循环群, 且 2 与 3 是 $\mathbb{Z}_5^*$ 的两个生成元 (显然是 $\mathbb{Z}_5^*$ 的两个仅有的生成元).

例 97

对 n 次单位根群

$$U_n = \left\{\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} \mid k = 0, 1, 2, \cdots, n-1\right\}.$$

令

$$\omega = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

则

$$U_n = \langle\omega\rangle = \left\{1, \omega, \omega^2, \cdots, \omega^{n-1}\right\},$$

所以 U_n 是一个 n 阶循环群. 由定理 49 第 (3) 条知当 $(k, n) = 1$ 时, $\operatorname{ord}\omega^k = n$, 因此当 $(k, n) = 1$ 时 ω^k 都是 U_n 的生成元.

定理 98

设 p 为素数, 则 $\mathbb{Z}_p^*$ 是 $p-1$ 阶循环群.

例

定理 98

设 p 为素数, 则 $\mathbb{Z}_p^*$ 是 $p-1$ 阶循环群.

例 99

$U(15)$ 是否是循环群?

例

定理 98

设 p 为素数, 则 $\mathbb{Z}_p^*$ 是 $p-1$ 阶循环群.

例 99

$U(15)$ 是否是循环群?

证明: $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$. 容易算出

$$2^4 = 4^4 = 7^4 = 8^4 = 11^4 = 13^4 = 14^4 = 1.$$

所以 $U(15)$ 中每一个元素的阶都小于 $U(15)$ 的阶 8, 从而 $U(15)$ 不是循环群.

循环群的生成元

定理 100

设 $G=\langle a\rangle$ 为循环群, 则

(1) 如果 $|G|=\infty$, 则 a 与 a^{-1} 是 G 的两个仅有的生成元;
(2) 如果 $|G|=n$, 则 G 恰有 $\phi(n)$ 个生成元, 且 a^r 是 G 的生成元的充分必要条件是 $(n,r)=1$, 其中 $\phi(n)$ 是欧拉函数.

循环群的生成元

定理 100

设 $G=\langle a\rangle$ 为循环群, 则

(1) 如果 $|G|=\infty$, 则 a 与 a^{-1} 是 G 的两个仅有的生成元;
(2) 如果 $|G|=n$, 则 G 恰有 $\phi(n)$ 个生成元, 且 a^r 是 G 的生成元的充分必要条件是 $(n,r)=1$, 其中 $\phi(n)$ 是欧拉函数.

证明: (1) 显然, a 与 a^{-1} 都是 G 的生成元. 若 a^k 是 G 的任一生成元, 则存在 $n\in\mathbb{Z}$, 使得 $\left(a^k\right)^n=a^{kn}=a$. 由注 93.1 第 (2) 条得 $kn=1$, 从而 $k=\pm 1$. 这就证明了 (1).

定理 100

设 $G=\langle a\rangle$ 为循环群, 则

(1) 如果 $|G|=\infty$, 则 a 与 a^{-1} 是 G 的两个仅有的生成元;

(2) 如果 $|G|=n$, 则 G 恰有 $\phi(n)$ 个生成元, 且 a^r 是 G 的生成元的充分必要条件是 $(n,r)=1$, 其中 $\phi(n)$ 是欧拉函数.

证明: (1) 显然, a 与 a^{-1} 都是 G 的生成元. 若 a^k 是 G 的任一生成元, 则存在 $n\in\mathbb{Z}$, 使得 $\left(a^k\right)^n=a^{kn}=a$. 由注 93.1 第 (2) 条得 $kn=1$, 从而 $k=\pm1$. 这就证明了 (1).(2) 由定理 49 第 (3) 条知 $\operatorname{ord}a^r=\frac{n}{(n,r)}$, 从而

$$a^r\text{ 为 }G\text{ 的生成元}\iff\operatorname{ord}a^r=n\iff\frac{n}{(n,r)}=n$$

$$\iff(n,r)=1,$$

故由欧拉函数的知 G 的生成元的个数为 $\phi(n)$.

例 101

求 $\mathbb{Z}_{12}$ 的全部生成元.

例 101

求 $\mathbb{Z}_{12}$ 的全部生成元.

解: 因 $\mathbb{Z}_{12} = \langle \bar{1} \rangle$, 所以 $\bar{r} = r \cdot \bar{1}$ 是 $\mathbb{Z}_{12}$ 的生成元的充分必要条件是

$$(r, 12) = 1, \text{ 且 } 0 < r < 12.$$

由此得 $\mathbb{Z}_{12}$ 的全部生成元为

$$\bar{1}, \bar{5}, \bar{7}, \overline{11}.$$

循环群的子群

定理 102

循环群的任一子群也是循环群.

定理 102

循环群的任一子群也是循环群.

证明: 设 $G=\langle a\rangle$ 为循环群, H 为 G 的一个子群. 如果 $H=\{e\}$, 则 $H=\langle e\rangle$ 是循环群. 如果 $H\neq\{e\}$, 则 H 必含有某个 $a^l, l\neq 0$, 因而 H 也含有 a^{-l}, 从而 H 必含有 a 的某些正整数幂. 设 r 是使 $a^r\in H$ 的最小正整数, 下面证明

$$H=\langle a^r\rangle.$$

定理 102

循环群的任一子群也是循环群.

证明: 设 $G=\langle a\rangle$ 为循环群, H 为 G 的一个子群. 如果 $H=\{e\}$, 则 $H=\langle e\rangle$ 是循环群. 如果 $H\neq\{e\}$, 则 H 必含有某个 $a^l, l\neq 0$, 因而 H 也含有 a^{-l}, 从而 H 必含有 a 的某些正整数幂. 设 r 是使 $a^r\in H$ 的最小正整数, 下面证明

$$H=\langle a^r\rangle.$$

对任意的 $a^k\in H, r\leq k\in\mathbb{Z}$, 存在 $s,t\in\mathbb{Z}, 0\leq t<r$ 使得 $k=sr+t$, 则

$$a^t=a^{k-sr}=a^k\cdot(a^r)^{-s}\in H.$$

因为 $t<r$, 所以由 r 的选取知 $t=0$. 于是对任意 $a^k\in H$ 有

$$a^k=a^{sr}=(a^r)^s\in\langle a^r\rangle,\text{ 即 } H\subseteq\langle a^r\rangle.$$

又显然有 $\langle a^r\rangle\subseteq H$. 所以 $H=\langle a^r\rangle$ 为循环群.

推论 103

设 $G = \langle a \rangle$ 为循环群, $\operatorname{ord} a = n$, $r \in \mathbb{Z}$. 如果 $(n, r) = d$, 则 $\langle a^r \rangle = \left\langle a^d \right\rangle$.

循环群的子群

推论 103

设 $G=\langle a\rangle$ 为循环群, $\operatorname{ord} a=n$, $r\in\mathbb{Z}$. 如果 $(n,r)=d$, 则 $\langle a^r\rangle=\left\langle a^d\right\rangle$.

证明: 因为 $(n,r)=d$, 所以存在 $u,v\in\mathbb{Z}$ 使得 $d=un+vr$. 于是 $a^d=a^{un+vr}=a^{vr}\in\langle a^r\rangle$. 另一方面, 同样由于 $(n,r)=d$, 所以 $d\mid r$, 从而又有 $a^r\in\left\langle a^d\right\rangle$. 由此得 $\langle a^r\rangle=\left\langle a^d\right\rangle$.

推论 103

设 $G=\langle a\rangle$ 为循环群, $\operatorname{ord} a=n$, $r\in\mathbb{Z}$. 如果 $(n,r)=d$, 则 $\langle a^r\rangle=\langle a^d\rangle$.

证明: 因为 $(n,r)=d$, 所以存在 $u,v\in\mathbb{Z}$ 使得 $d=un+vr$. 于是 $a^d=a^{un+vr}=a^{vr}\in\langle a^r\rangle$. 另一方面, 同样由于 $(n,r)=d$, 所以 $d\mid r$, 从而又有 $a^r\in\langle a^d\rangle$. 由此得 $\langle a^r\rangle=\langle a^d\rangle$.

推论 104

设 $G=\langle a\rangle$ 为循环群,

(1) 如果 $|G|=\infty$, 则 G 的全部子群为

$$\left\{\left\langle a^d\right\rangle \mid d=0,1,2,\cdots\right\}.$$

(2) 如果 $|G|=n$, 则 G 的全部子群为

$$\left\{\left\langle a^d\right\rangle \mid d \text{ 为 } n \text{ 的正因子 }\right\}.$$

证明

由定理 102 知, 循环群的任一子群必形如 $\langle a^r \rangle$ $(r \in \mathbb{Z})$. 显然, $\langle a^r \rangle = \langle a^{-r} \rangle$. 因此, 循环群的任一子群必形如 $\langle a^r \rangle$ $(r \in \mathbb{Z}$ 且 $r \geqslant 0)$.

证明

由定理 102 知, 循环群的任一子群必形如 $\langle a^r \rangle$ ($r \in \mathbb{Z}$). 显然, $\langle a^r \rangle = \langle a^{-r} \rangle$. 因此, 循环群的任一子群必形如 $\langle a^r \rangle$ ($r \in \mathbb{Z}$ 且 $r \geqslant 0$).

(1) 如果 $|G| = \infty$, 因为对任意的 $r_1 > r_2 > 0$, 有 $r_1 \nmid r_2$, 所以 $a^{r_2} \notin \langle a^{r_1} \rangle$, 于是 $\langle a^{r_1} \rangle \neq \langle a^{r_2} \rangle$. 另一方面, 对任意的 $r > 0$, 显然 $a^r \notin \left\langle a^0 \right\rangle = \langle e \rangle$, 所以又有 $\langle a^r \rangle \neq \langle e \rangle$. 由此得 G 的全部子群为

$$\left\{ \left\langle a^d \right\rangle \mid d = 0, 1, 2, \cdots \right\}.$$

证明

由定理 102 知, 循环群的任一子群必形如 $\langle a^r \rangle$ $(r \in \mathbb{Z})$. 显然, $\langle a^r \rangle = \langle a^{-r} \rangle$. 因此, 循环群的任一子群必形如 $\langle a^r \rangle$ $(r \in \mathbb{Z}$ 且 $r \geqslant 0)$.

(1) 如果 $|G| = \infty$, 因为对任意的 $r_1 > r_2 > 0$, 有 $r_1 \nmid r_2$, 所以 $a^{r_2} \notin \langle a^{r_1} \rangle$, 于是 $\langle a^{r_1} \rangle \neq \langle a^{r_2} \rangle$. 另一方面, 对任意的 $r > 0$, 显然 $a^r \notin \left\langle a^0 \right\rangle = \langle e \rangle$, 所以又有 $\langle a^r \rangle \neq \langle e \rangle$. 由此得 G 的全部子群为

$$\left\{ \left\langle a^d \right\rangle \mid d = 0, 1, 2, \cdots \right\}.$$

(2) 如果 $|G| = n$, 由推论 103 可知, 对任意的正整数 r, 存在 n 的正因子 $d = (n, r)$, 有 $\langle a^r \rangle = \left\langle a^d \right\rangle$. 又如果 $d_1 > d_2$ 为 n 的两个不同的正因子, 则 $d_1 \nmid d_2$, 因此不存在非负整数 s, t 使得 $d_2 = sd_1 - tn$, 于是 $a^{d_2} \notin \left\langle a^{d_1} \right\rangle$, 从而 $\left\langle a^{d_1} \right\rangle \neq \left\langle a^{d_2} \right\rangle$. 另一方面, 对 n 的任一正因子 $d < n$, 显然 $a^d \neq e$, 所以又有 $\left\langle a^d \right\rangle \neq \langle e \rangle$, 而 $\langle e \rangle = \langle a^n \rangle$, 由此得 G 的全部子群为 $\{\left\langle a^d \right\rangle \mid d$ 为 n 的正因子$\}$.

例 105

求 $\mathbb{Z}_{12}$ 的全部子群.

例 105

求 $\mathbb{Z}_{12}$ 的全部子群.

解: 因 12 的全部正因子为

$$1, 2, 3, 4, 6, 12,$$

所以 $\mathbb{Z}_{12}$ 的子群共有以下 6 个:

$$\begin{aligned}
\langle\overline{1}\rangle &= \mathbb{Z}_{12},\\
\langle\overline{2}\rangle &= 2\mathbb{Z}_{12} = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\},\\
\langle\overline{3}\rangle &= 3\mathbb{Z}_{12} = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\},\\
\langle\overline{4}\rangle &= 4\mathbb{Z}_{12} = \{\overline{0}, \overline{4}, \overline{8}\},\\
\langle\overline{6}\rangle &= 6\mathbb{Z}_{12} = \{\overline{0}, \overline{6}\},\\
\langle\overline{12}\rangle &= 12\mathbb{Z}_{12} = \{\overline{0}\}.
\end{aligned}$$

循环群的结构定理

定理 106

设 G 为循环群.

(1) 如果 $G = \langle a \rangle$ 是无限循环群, 则 $G \cong (\mathbb{Z}, +)$;

(2) 如果 $G = \langle a \rangle$ 是 n 阶循环群, 则 $G \cong (\mathbb{Z}_n, +)$.

循环群的结构定理

定理 106

设 G 为循环群.

(1) 如果 $G = \langle a \rangle$ 是无限循环群, 则 $G \cong (\mathbb{Z}, +)$;

(2) 如果 $G = \langle a \rangle$ 是 n 阶循环群, 则 $G \cong (\mathbb{Z}_n, +)$.

证明: (1) 令

$$\phi : \mathbb{Z} \longrightarrow G,$$

$$k \longmapsto a^k, \quad \forall k \in \mathbb{Z}.$$

(i) 显然 ϕ 是 $\mathbb{Z}$ 到 G 的映射;

(ii) 设 $k, l \in \mathbb{Z}$, 如果 $a^k = a^l$, 则由注 93.1 第 (2) 条得 $k = l$, 所以 ϕ 为 $\mathbb{Z}$ 到 G 的单映射;

证明 (续)

(ii) 设 $k, l \in \mathbb{Z}$, 如果 $a^k = a^l$, 则由注 93.1 第 (2) 条得 $k = l$, 所以 ϕ 为 $\mathbb{Z}$ 到 G 的单映射; (iii) 对任意的 $a^k \in G$, 有 $k \in \mathbb{Z}$, 使 $\phi(k) = a^k$, 所以 ϕ 是 $\mathbb{Z}$ 到 G 的满映射;

证明 (续)

(ii) 设 $k, l \in \mathbb{Z}$, 如果 $a^k = a^l$, 则由注 93.1 第 (2) 条得 $k = l$, 所以 ϕ 为 $\mathbb{Z}$ 到 G 的单映射; (iii) 对任意的 $a^k \in G$, 有 $k \in \mathbb{Z}$, 使 $\phi(k) = a^k$, 所以 ϕ 是 $\mathbb{Z}$ 到 G 的满映射; (iv) 对任意的 $k, l \in \mathbb{Z}$,

$$\phi(k+l) = a^{k+l} = a^k \cdot a^l = \phi(k) \cdot \phi(l),$$

所以 ϕ 是 $\mathbb{Z}$ 到 G 的同构映射. 因此, $G \cong (\mathbb{Z}, +)$.

证明 (续)

(ii) 设 $k, l \in \mathbb{Z}$, 如果 $a^k = a^l$, 则由注 93.1 第 (2) 条得 $k = l$, 所以 ϕ 为 $\mathbb{Z}$ 到 G 的单映射; (iii) 对任意的 $a^k \in G$, 有 $k \in \mathbb{Z}$, 使 $\phi(k) = a^k$, 所以 ϕ 是 $\mathbb{Z}$ 到 G 的满映射; (iv) 对任意的 $k, l \in \mathbb{Z}$,

$$\phi(k+l) = a^{k+l} = a^k \cdot a^l = \phi(k) \cdot \phi(l),$$

所以 ϕ 是 $\mathbb{Z}$ 到 G 的同构映射. 因此, $G \cong (\mathbb{Z}, +)$. (2) 令

$$\begin{aligned} \phi: \quad \mathbb{Z}_n &\longrightarrow G, \\ \bar{k} &\longmapsto a^k, \quad \forall \bar{k} \in \mathbb{Z}_n. \end{aligned}$$

(ii) 设 $k,l\in\mathbb{Z}$, 如果 $a^k=a^l$, 则由注 93.1 第 (2) 条得 $k=l$, 所以 ϕ 为 $\mathbb{Z}$ 到 G 的单映射; (iii) 对任意的 $a^k\in G$, 有 $k\in\mathbb{Z}$, 使 $\phi(k)=a^k$, 所以 ϕ 是 $\mathbb{Z}$ 到 G 的满映射; (iv) 对任意的 $k,l\in\mathbb{Z}$,

$$\phi(k+l)=a^{k+l}=a^k\cdot a^l=\phi(k)\cdot\phi(l),$$

所以 ϕ 是 $\mathbb{Z}$ 到 G 的同构映射. 因此, $G\cong(\mathbb{Z},+)$. (2) 令

$$\begin{aligned}\phi:\quad \mathbb{Z}_n &\longrightarrow G,\\ \bar{k} &\longmapsto a^k,\quad \forall\bar{k}\in\mathbb{Z}_n.\end{aligned}$$

(i) 设 $\bar{k}=\bar{l}$, 则 $n\mid k-l$, 于是 $a^{k-l}=e$, 从而 $a^k=a^l$, 所以 ϕ 是 $\mathbb{Z}_n$ 到 G 的映射;

证明 (续)

(ii) 设 $\bar{k}, \bar{l} \in \mathbb{Z}_n$, 如果 $\phi(\bar{k}) = \phi(\bar{l})$, 即 $a^k = a^l$, 则 $n \mid k - l$, 从而 $\bar{k} = \bar{l}$, 所以 ϕ 是 $\mathbb{Z}_n$ 到 G 的单映射;

(iii) 对任意的 $a^k \in G$, 有 $\bar{k} \in \mathbb{Z}_n$, 使 $\phi(\bar{k}) = a^k$, 所以 ϕ 是 $\mathbb{Z}_n$ 到 G 的满映射;

证明 (续)

(ii) 设 $\bar{k}, \bar{l} \in \mathbb{Z}_n$, 如果 $\phi(\bar{k}) = \phi(\bar{l})$, 即 $a^k = a^l$, 则 $n \mid k - l$, 从而 $\bar{k} = \bar{l}$, 所以 ϕ 是 $\mathbb{Z}_n$ 到 G 的单映射;

(iii) 对任意的 $a^k \in G$, 有 $\bar{k} \in \mathbb{Z}_n$, 使 $\phi(\bar{k}) = a^k$, 所以 ϕ 是 $\mathbb{Z}_n$ 到 G 的满映射; (iv) 对任意的 $\bar{k}, \bar{l} \in \mathbb{Z}_n$, 有

$$\phi(\bar{k} + \bar{l}) = \phi(\overline{k + l}) = a^{k+l} = a^k \cdot a^l = \phi(\bar{k}) \cdot \phi(\bar{l}).$$

(ii) 设 $\bar{k}, \bar{l} \in \mathbb{Z}_n$, 如果 $\phi(\bar{k}) = \phi(\bar{l})$, 即 $a^k = a^l$, 则 $n \mid k - l$, 从而 $\bar{k} = \bar{l}$, 所以 ϕ 是 $\mathbb{Z}_n$ 到 G 的单映射;

(iii) 对任意的 $a^k \in G$, 有 $\bar{k} \in \mathbb{Z}_n$, 使 $\phi(\bar{k}) = a^k$, 所以 ϕ 是 $\mathbb{Z}_n$ 到 G 的满映射; (iv) 对任意的 $\bar{k}, \bar{l} \in \mathbb{Z}_n$, 有

$$\phi(\bar{k} + \bar{l}) = \phi(\overline{k + l}) = a^{k+l} = a^k \cdot a^l = \phi(\bar{k}) \cdot \phi(\bar{l}).$$

注 106.1

由定理 *106* 可知, 从同构的观点看, 循环群仅有两类, 即整数加群 $(\mathbb{Z}, +)$ 和模 n 剩余类加群 $(\mathbb{Z}_n, +)$, 所以掌握了这两类群, 也就等于把一切循环群都弄清楚了.

§2.6 循环群

- 循环群的定义
- 循环群的例子
- 循环群的生成元
- 循环群的子群
- 循环群的结构

§2.7 对称群

- 对称群
- 凯莱定理
- 轮换与对换
- 置换的轮换表示
- 置换的对换分解
- 奇 (偶) 置换
- 交错群

对称群的定义

定义 107

设 A 为非空集合. 记 A 的所有置换构成的集合为 $S(A)$, 则 $S(A)$ 在映射的复合作为乘法运算下是群, 我们称 $S(A)$ 为 A 的**对称群** (symmetric group), $S(A)$ 的任一子群称为**置换群** (permutation group). 如果 A 是有 n 个元素的有限集, 则将 A 表示为 $[n]=\{1,2,3,\cdots,n\}$, 并且对任意 $\sigma\in S(A)$ 记为 $\sigma=\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$; 此时将 $S(A)$ 记为 S_n, 并称为 n **次对称群**.

例 108

写出 S_3 的全部元素.

例 108

写出 S_3 的全部元素.

解: 易得 S_3 有 6 个元素, 它们是

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

例 109

设置换 $\sigma \in S_5$ 为
$\sigma(1)=3, \sigma(2)=5, \sigma(3)=2, \sigma(4)=4, \sigma(5)=1$, 则

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

该置换也可以写成

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

等.

例 109

设置换 $\sigma \in S_5$ 为
$\sigma(1)=3, \sigma(2)=5, \sigma(3)=2, \sigma(4)=4, \sigma(5)=1$, 则

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

该置换也可以写成

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

等.

注 109.1

由于置换的乘法本质上是映射的合成, 所以置换的乘法是从右往左的. 此外, 对于 $\sigma \in S_n$ 以及 1 到 n 中的 r $(r \geq 2)$ 个不同的数 $i_1, i_2, \cdots, i_r$, 若有 $\sigma(i_1)=i_2, \sigma(i_2)=i_3, \cdots, \sigma(i_{r-1})=i_r$, 则可表示为 $i_1 \rightarrow i_2 \rightarrow i_3 \rightarrow \cdots \rightarrow i_r$.

例

例 110

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$, 其中 σ 以下列顺序作用于集合 $\{1,2,3,4,5\}$: $1 \to 3 \to 1$, $2 \to 1 \to 2$, $3 \to 2 \to 3$, $4 \to 4 \to 4$.

凯莱定理

定理 111

n 次对称群 S_n 的阶是 $n!$.

凯莱定理

定理 111

n 次对称群 S_n 的阶是 $n!$.

定理 112 (凯莱定理 (Cayley, 1854))

每一个群都同构于一个置换群.

定理 111

n 次对称群 S_n 的阶是 $n!$.

定理 112 (凯莱定理 (Cayley, 1854))

每一个群都同构于一个置换群.

证明: 设 G 是群, $a \in G$, 定义 ϕ_a 为 $\phi_a(x) = ax$, $\forall x \in G$, 则 ϕ_a 是 G 的一个置换. 令

$$G_l = \{\phi_a \mid a \in G\}.$$

易证 G_l 关于映射的合成构成群 $S(G)$ 的一个子群.

凯莱定理

定理 111

n 次对称群 S_n 的阶是 $n!$.

定理 112 (凯莱定理 (Cayley, 1854))

每一个群都同构于一个置换群.

证明: 设 G 是群, $a \in G$, 定义 ϕ_a 为 $\phi_a(x) = ax$, $\forall x \in G$, 则 ϕ_a 是 G 的一个置换. 令

$$G_l = \{\phi_a \mid a \in G\}.$$

易证 G_l 关于映射的合成构成群 $S(G)$ 的一个子群. 进一步, 令

$$\rho : G \longrightarrow G_l,$$

$$a \longmapsto \phi_a, \quad \forall a \in G.$$

易证 ρ 是 G 到 G_l 的同构.

轮换与对换

定义 113

设 σ 是一个 n 阶置换. 如果存在 1 到 n 中的 r 个不同的数 $i_1, i_2, \cdots, i_r$, 使

$$\sigma\left(i_1\right)=i_2, \sigma\left(i_2\right)=i_3, \cdots, \sigma\left(i_{r-1}\right)=i_r, \sigma\left(i_r\right)=i_1,$$

并且 σ 保持其余的元素不变, 则称 σ 是一个长度为 r 的**轮换** (cycle), 简称 r 轮换, 记作 $\sigma=\left(i_1 i_2 \cdots i_r\right)$, 其中集合 $\left\{i_1, i_2, \cdots, i_r\right\}$ 记为 $I(\sigma)$. 特别地, 2 轮换称为**对换** (transposition).

定义 113

设 σ 是一个 n 阶置换. 如果存在 1 到 n 中的 r 个不同的数 $i_1, i_2, \cdots, i_r$, 使

$$\sigma(i_1) = i_2, \sigma(i_2) = i_3, \cdots, \sigma(i_{r-1}) = i_r, \sigma(i_r) = i_1,$$

并且 σ 保持其余的元素不变, 则称 σ 是一个长度为 r 的**轮换** (cycle), 简称 r 轮换, 记作 $\sigma = (i_1 i_2 \cdots i_r)$, 其中集合 $\{i_1, i_2, \cdots, i_r\}$ 记为 $I(\sigma)$. 特别地, 2 轮换称为**对换** (transposition).

定义 114

设 $\sigma = (i_1 i_2 \cdots i_r)$ 与 $\tau = (j_1 j_2 \cdots j_s)$ 是两个轮换, 如果对任意 $k \in [r], l \in [s]$ 均有 $i_k \neq j_l$, 则称 σ 与 τ 为两个**不相交的轮换**.

轮换与对换

定义 113

设 σ 是一个 n 阶置换. 如果存在 1 到 n 中的 r 个不同的数 $i_1, i_2, \cdots, i_r$, 使

$$\sigma(i_1) = i_2, \sigma(i_2) = i_3, \cdots, \sigma(i_{r-1}) = i_r, \sigma(i_r) = i_1,$$

并且 σ 保持其余的元素不变, 则称 σ 是一个长度为 r 的**轮换** (cycle), 简称 r 轮换, 记作 $\sigma = (i_1 i_2 \cdots i_r)$, 其中集合 $\{i_1, i_2, \cdots, i_r\}$ 记为 $I(\sigma)$. 特别地, 2 轮换称为**对换** (transposition).

定义 114

设 $\sigma = (i_1 i_2 \cdots i_r)$ 与 $\tau = (j_1 j_2 \cdots j_s)$ 是两个轮换, 如果对任意 $k \in [r], l \in [s]$ 均有 $i_k \neq j_l$, 则称 σ 与 τ 为两个**不相交的轮换**.

- 一般地, 恒等置换常写为 (1). 若一个置换不是恒等置换, 则在它的分解式中, 常将出现的 1 轮换省略不写.

例 115

将 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 6 & 1 & 5 & 2 \end{pmatrix}$ 表为不相交轮换的乘积.

例 115

将 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 6 & 1 & 5 & 2 \end{pmatrix}$ 表为不相交轮换的乘积.

解. 容易看出, σ 以下列顺序作用于 $\{1,2,3,4,5\}$ 的元素:

$$\begin{array}{ccccccc} 1 & \longmapsto & 4 & \longmapsto & 1, & & \\ 2 & \longmapsto & 3 & \longmapsto & 6 & \longmapsto & 2, \\ 5 & \longmapsto & 5. & & & & \end{array}$$

所以 $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 6 & 1 & 5 & 2 \end{pmatrix} = (14)(236)(5) = (14)(236).$

例 115

将 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 6 & 1 & 5 & 2 \end{pmatrix}$ 表为不相交轮换的乘积.

解. 容易看出, σ 以下列顺序作用于 $\{1,2,3,4,5\}$ 的元素:

$$\begin{array}{ccccccc} 1 & \longmapsto & 4 & \longmapsto & 1, & & \\ 2 & \longmapsto & 3 & \longmapsto & 6 & \longmapsto & 2, \\ 5 & \longmapsto & 5. & & & & \end{array}$$

所以 $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 6 & 1 & 5 & 2 \end{pmatrix} = (14)(236)(5) = (14)(236).$

例 116

三次对称群 S_3 的 6 个元素的轮换表示为

$$\begin{array}{lll} \sigma_1 = (1); & \sigma_2 = (12); & \sigma_3 = (13); \\ \sigma_4 = (23); & \sigma_5 = (123); & \sigma_6 = (132). \end{array}$$

轮换的性质

定理 117

任何两个不相交轮换的乘积是可以交换的.

定理 117

任何两个不相交轮换的乘积是可以交换的.

证明: 设 $\sigma = (i_1 i_2 \cdots i_r)$ 与 $\tau = (j_1 j_2 \cdots j_s)$ 是两个不相交的轮换, a 是 $\{1, 2, \cdots, n\}$ 中的任意一个数.

(1) 如果 $a \neq i_k, j_l$ $(k \in [r], l \in [s])$, 则

$$\sigma\tau(a) = \sigma(a) = a, \ \tau\sigma(a) = \tau(a) = a,$$

所以 $\sigma\tau(a) = \tau\sigma(a)$.

(2) 如果 $a = i_k$ $(k \in [r])$, 则 $\sigma(a) \neq j_l$ $(l \in [s])$. 从而

$$\sigma\tau(a) = \sigma(a), \ \tau\sigma(a) = \tau(\sigma(a)) = \sigma(a),$$

所以 $\sigma\tau(a) = \tau\sigma(a)$.

(3) 同理可证, 如果 $a = j_l$ $(l \in [s])$, 也有 $\sigma\tau(a) = \tau\sigma(a)$.

综上定理得证.

置换的轮换表示

定理 118

S_n 中每一个置换可表为一些不相交轮换的乘积.

定理 118

S_n 中每一个置换可表为一些不相交轮换的乘积.

证明: 设置换为 $\sigma \in S_n$. 任意选取 $i_1 \in [n]$. 不妨设轮换 $\sigma_1 = (i_1 i_2 \cdots i_r)$, 任意选取 $j_1 \in [n] \backslash I(\sigma_1)$, 可得一轮换 $\sigma_2 = (j_1 j_2 \cdots j_s)$. 显然$I(\sigma_1) \cap I(\sigma_2) = \emptyset$. 由于 n 有限, 以此类推可得一系列不相交轮换 $\sigma_1, \sigma_2, \cdots, \sigma_t$, 并且 $\cup_{k=1}^{t} I(\sigma_k) = [n]$. 进一步, 可验证 $\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_t$. 于是定理得证.

注 118.1

设 $\sigma \in S_n$. 则对任意 $i \in [n]$, 由 σ 是置换易知包含 i 的轮换在不考虑初始值时是唯一确定的. 从而由定理 *117* 和定理 *118* 知将 σ 分解为不相交轮换的乘积, 如果不考虑轮换内的整数次序和不相交轮换之间的次序, 以及乘积中 1 轮换的个数, 则这个分解式是唯一的.

注 118.1

设 $\sigma \in S_n$. 则对任意 $i \in [n]$, 由 σ 是置换易知包含 i 的轮换在不考虑初始值时是唯一确定的. 从而由定理 *117* 和定理 *118* 知将 σ 分解为不相交轮换的乘积, 如果不考虑轮换内的整数次序和不相交轮换之间的次序, 以及乘积中 1 轮换的个数, 则这个分解式是唯一的.

例 119

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 1 & 6 \end{pmatrix} = (12345);$$
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 5 & 4 & 3 & 1 \end{pmatrix} = (126)(35).$$

例 120

将下列轮换的乘积表示为不相交轮换的乘积:

$$(3654)(3241)(31524).$$

例 120

将下列轮换的乘积表示为不相交轮换的乘积:

$$(3654)(3241)(31524).$$

解. 设 $\sigma = (3654)\,, \delta = (3241)\,, \eta = (31524)$, 则有

$$\begin{array}{ccccccc}
1 & \xmapsto{\eta} & 5 & \xmapsto{\delta} & 5 & \xmapsto{\sigma} & 4, \\
4 & \xmapsto{\eta} & 3 & \xmapsto{\delta} & 2 & \xmapsto{\sigma} & 2, \\
2 & \xmapsto{\eta} & 4 & \xmapsto{\delta} & 1 & \xmapsto{\sigma} & 1, \\
3 & \xmapsto{\eta} & 1 & \xmapsto{\delta} & 3 & \xmapsto{\sigma} & 6, \\
6 & \xmapsto{\eta} & 6 & \xmapsto{\delta} & 6 & \xmapsto{\sigma} & 5, \\
5 & \xmapsto{\eta} & 2 & \xmapsto{\delta} & 4 & \xmapsto{\sigma} & 3.
\end{array}$$

由此得 $(3654)(3241)(31524) = (142)(365)$.

轮换的阶

定理 121

如果 $\sigma \in S_n$ 是一个 r 轮换, 则 $\operatorname{ord}\sigma = r$.

轮换的阶

定理 121

如果 $\sigma \in S_n$ 是一个 r 轮换, 则 $\operatorname{ord} \sigma = r$.

证明: 直接计算可知 $\sigma^r = (1)$, 且对任意的 $0 < s < r, \sigma^s \neq e$, 所以 $\operatorname{ord} \sigma = r$.

轮换的阶

定理 121

如果 $\sigma \in S_n$ 是一个 r 轮换, 则 $\operatorname{ord}\sigma = r$.

证明: 直接计算可知 $\sigma^r = (1)$, 且对任意的 $0 < s < r, \sigma^s \neq e$, 所以 $\operatorname{ord}\sigma = r$.

定理 122

如果 $\sigma \in S_n$ 是一些不相交轮换的乘积

$$\sigma = \sigma_1\sigma_2\cdots\sigma_s,$$

其中 σ_i 是 r_i 轮换, 则 $\operatorname{ord}\sigma = [r_1, r_2, \cdots, r_s]$.

轮换的阶

定理 121

如果 $\sigma \in S_n$ 是一个 r 轮换, 则 $\operatorname{ord}\sigma = r$.

证明: 直接计算可知 $\sigma^r = (1)$, 且对任意的 $0 < s < r, \sigma^s \neq e$, 所以 $\operatorname{ord}\sigma = r$.

定理 122

如果 $\sigma \in S_n$ 是一些不相交轮换的乘积

$$\sigma = \sigma_1\sigma_2\cdots\sigma_s,$$

其中 σ_i 是 r_i 轮换, 则 $\operatorname{ord}\sigma = [r_1, r_2, \cdots, r_s]$.

证明: 设 $m = [r_1, r_2, \cdots, r_s]$. 由于不相交轮换的乘积是可以互相交换的, 因此

$$\sigma^m = \sigma_1^m\sigma_2^m\cdots\sigma_s^m = e,$$

从而 $\operatorname{ord}\sigma \mid m$.

证明 (续)

另一方面, 设 $\sigma_1 = (i_1 i_2 \cdots i_{r_1})$, 则对任意的 $i_j \in \{i_1, i_1, \cdots, i_{r_1}\}$, 由于 σ_1, $\sigma_2, \cdots, \sigma_s$ 为互不相交的轮换, 因此

$$\begin{aligned}\sigma_1^{\text{ord } \sigma}(i_j) &= \sigma_1^{\operatorname{ord}\sigma} \sigma_2^{\operatorname{ord}\sigma} \cdots \sigma_s^{\text{ord } \sigma}(i_j) \\ &= \sigma^{\operatorname{ord}\sigma}(i_j) = i_j.\end{aligned}$$

由此推出 $\sigma_1^{\operatorname{ord}\sigma} = e$, 从而 $r_1 \mid \operatorname{ord}\sigma$. 同理可证 $r_i \mid \operatorname{ord}\sigma \ (i = 1, 2, \cdots, s)$. 于是

$$m = [r_1, r_2, \cdots, r_s] \mid \operatorname{ord}\sigma.$$

所以

$$\operatorname{ord}\sigma = [r_1, r_2, \cdots, r_s]$$

例 123

设 σ 是一个 7 阶置换, 已知 $\sigma^3 = (1437562)$, 试求 σ.

例 123

设 σ 是一个 7 阶置换, 已知 $\sigma^3 = (1437562)$, 试求 σ.

解法 1: 由已知, σ 是 $1 \sim 7$ 的一个置换. 因为 σ^3 是一个 7 轮换, 所以 σ 也是一个 7 轮换, 从而 ord $\sigma = 7$. 于是

$$\sigma = \left(\sigma^3\right)^5 = (1437562)^5 = (1674253)\,.$$

例 123

设 σ 是一个 7 阶置换, 已知 $\sigma^3 = (1437562)$, 试求 σ.

解法 1: 由已知, σ 是 $1 \sim 7$ 的一个置换. 因为 σ^3 是一个 7 轮换, 所以 σ 也是一个 7 轮换, 从而 ord $\sigma = 7$. 于是

$$\sigma = \left(\sigma^3\right)^5 = (1437562)^5 = (1674253).$$

解法 2: 本题也可按下面的方法求解:

易知, σ 是一个 7 轮换. 设 $\sigma = (i_1 i_2 i_3 i_4 i_5 i_6 i_7)$, 则

$$\sigma^3 = (i_1 i_4 i_7 i_3 i_6 i_2 i_5).$$

将这与 $\sigma^3 = (143756)$ 比较, 可得

$i_1 = 1, i_2 = 6, i_3 = 7, i_4 = 4, i_5 = 2, i_6 = 5, i_7 = 3$, 即

$\sigma = (167425)$.

置换的对换分解

定理 124

每个置换都可表为对换的乘积.

置换的对换分解

定理 124

每个置换都可表为对换的乘积.

证明: 首先, 设 $\sigma=(i_1i_2\cdots i_r)$ 是一个 r 轮换, 则

$$\sigma=(i_1i_2)(i_2i_3)\cdots(i_{r-2}i_{r-1})(i_{r-1}i_r).$$

所以每个轮换可以表示为对换的乘积. 由于每个置换可以表示为不相交轮换的乘积, 所以每个置换也可以表示为对换的乘积.

定理 124

每个置换都可表为对换的乘积.

证明: 首先, 设 $\sigma = (i_1 i_2 \cdots i_r)$ 是一个 r 轮换, 则

$$\sigma = (i_1 i_2)(i_2 i_3)\cdots(i_{r-2} i_{r-1})(i_{r-1} i_r).$$

所以每个轮换可以表示为对换的乘积. 由于每个置换可以表示为不相交轮换的乘积, 所以每个置换也可以表示为对换的乘积.

例 125

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 3 & 6 & 2 & 5 & 4 & 1 \end{pmatrix} = (17)(23)(36)(64)$$
$$= (71)(36)(25)(64)(45)(25).$$

逆序 (数)

定义 126

由 $1, 2, \cdots, n$ 这 n 个数排成的任一个有序数组 $i_1, i_2, \cdots, i_n$ 称为一个 n 级排列. 在一个排列中, 如果一对数的前后位置与大小顺序相反, 即前面的数大于后面的数, 那么就称它们构成一个**逆序**, 排列中的逆序总数称为这个排列的**逆序数**. 对任意 $\sigma \in S_n$, 则 $\sigma(1)\sigma(2)\sigma(3)\cdots\sigma(n)$ 可以看做是一个 n 级排列, 其逆序数记为 $\mathcal{N}(\sigma)$.

置换的对换分解唯一性

定理 127

将一个置换 $\sigma \in S_n$ 表为对换的乘积, 所用对换个数的奇偶性是唯一的.

置换的对换分解唯一性

定理 127

将一个置换 $\sigma \in S_n$ 表为对换的乘积，所用对换个数的奇偶性是唯一的.

证明: 设 $\sigma_1\sigma_2\cdots\sigma_r$ 是 σ 的任意一个对换的乘积表示，即

$$\sigma = \sigma_1\sigma_2\cdots\sigma_r,$$

其中 σ_i 都是对换. 由于排列 $\sigma(1)\sigma(2)\cdots\sigma(n)$ 可由自然排列 $123\cdots n$ 经过 r 次对换 $\sigma_1, \sigma_2, \cdots, \sigma_r$ 得到，而自然排列的逆序数为 0，是偶数. 因此，r 的奇偶性和排列 $\sigma(1)\sigma(2)\cdots\sigma(n)$ 的逆序数的奇偶性必然相同，于是可知 $\sigma \in S_n$ 表为对换的乘积时所用对换个数的奇偶性是由排列 $\sigma(1)\sigma(2)\cdots\sigma(n)$ 的逆序数的奇偶性唯一确定的.

奇 (偶) 置换

定义 128

可表成偶数个对换的乘积的置换叫**偶置换** (even permutation), 可表成奇数个对换的乘积的置换叫**奇置换** (odd permutation).

奇 (偶) 置换

定义 128

可表成偶数个对换的乘积的置换叫**偶置换** (even permutation), 可表成奇数个对换的乘积的置换叫**奇置换** (odd permutation).

注 128.1

由置换和排列的关系以及定义 *128* 可知*:*

(1) 任何两个偶 *(*奇*)* 置换之积是偶置换*;*

(2) 一个偶置换与一个奇置换之积是奇置换*;*

(3) 一个偶 *(*奇*)* 置换的逆置换仍是一个偶 *(*奇*)* 置换*.*

奇 (偶) 置换

定理 129

设 G 是置换群. 若 G 中存在奇置换, 则 G 中奇置换的个数与偶置换的个数相同.

奇 (偶) 置换

定理 129

设 G 是置换群. 若 G 中存在奇置换, 则 G 中奇置换的个数与偶置换的个数相同.

证明: 设 G 中有奇置换. 由于 G 是置换群, 所以 $(1) \in G$, 而 (1) 为偶置换. 所以 G 中既有奇置换又有偶置换. 以 O 与 E 分别表示 G 中奇置换与偶置换的集合. 设 σ 为 G 的任一奇置换, 则

$$\sigma O = \{\sigma\delta \mid \delta \in O\} \subseteq E,$$

$$\sigma E = \{\sigma\tau \mid \tau \in E\} \subseteq O.$$

因此

$$|O| = |\sigma O| \leq |E|, \; |E| = |\sigma E| \leq |O|,$$

由此得 $|O| = |E|$. 这就证明了结论.

奇 (偶) 置换

推论 130

当 $n > 1$ 时, 在全体 n 阶置换中, 奇置换与偶置换各有 $\frac{n!}{2}$ 个.

奇 (偶) 置换

推论 130

当 $n > 1$ 时, 在全体 n 阶置换中, 奇置换与偶置换各有 $\frac{n!}{2}$ 个.

定理 131

设 G 是置换群. 则 G 中所有偶置换的集合 H 是 G 的子群.

推论 130

当 $n > 1$ 时, 在全体 n 阶置换中, 奇置换与偶置换各有 $\frac{n!}{2}$ 个.

定理 131

设 G 是置换群. 则 G 中所有偶置换的集合 H 是 G 的子群.

证明: 因 $(1) \in G$ 为偶置换, 所以 $(1) \in H$, 从而 H 非空. 又由于两个偶置换的乘积仍是偶置换, 所以 H 关于置换的乘积封闭. 由注 128.1 第 (3) 条知 H 中每个偶置换的逆为偶置换, 仍然在 H 中. 由定理 25 知 H 为 G 的子群.

定义 132

由 S_n 的全体偶置换所构成的子群称为 n 次**交错群** (alternating group), 记作 A_n.

交错群

定义 132

由 S_n 的全体偶置换所构成的子群称为 n 次**交错群** (alternating group)，记作 A_n.

例 133

S_3 的交错群为

$$A_3 = \{(1), (123), (132)\}.$$

§2.7 对称群

- 对称群
- 凯莱定理
- 轮换与对换
- 置换的轮换表示
- 置换的对换分解
- 奇 (偶) 置换
- 交错群

§2.8 群的直积

- 群的外直积
- 外直积的性质
- 外直积元素的阶
- 循环群的外直积
- 群的内直积
- 内直积的性质
- 内直积的判定

定义 134

设 $G_1, G_2, \cdots, G_n$ 是有限多个群. 构造集合 $G_1, G_2, \cdots, G_n$ 的笛卡尔积

$$G = \{(g_1, g_2, \cdots, g_n) \mid g_i \in G_i, i = 1, 2, \cdots, n\},$$

并在 G 中定义运算

$$(g_1, g_2, \cdots, g_n) \cdot (g_1', g_2', \cdots, g_n') = (g_1 g_1', g_2 g_2', \cdots, g_n g_n'),$$

则 G 关于上述运算构成群, 称为群 $G_1, G_2, \cdots, G_n$ **的外直积** (external direct product), 记作 $G = G_1 \times G_2 \times \cdots \times G_n$.

注 134.1

设 $G = G_1 \times G_2 \times \cdots \times G_n$ 是群 $G_1, G_2, \cdots, G_n$ 的外直积，则

注 134.1

设 $G = G_1 \times G_2 \times \cdots \times G_n$ 是群 $G_1, G_2, \cdots, G_n$ 的外直积, 则

(1) 如果 $e_1, e_2, \cdots, e_n$ 分别是群 $G_1, G_2, \cdots G_n$ 的单位元, 则 $(e_1, e_2, \cdots, e_n)$ 是 G 的单位元. 进一步, 设 $(g_1, g_2, \cdots, g_n) \in G$, 则 $(g_1, g_2, \cdots, g_n)^{-1} = \left(g_1^{-1}, g_2^{-1}, \cdots, g_n^{-1}\right)$;

注 134.1

设 $G = G_1 \times G_2 \times \cdots \times G_n$ 是群 $G_1, G_2, \cdots, G_n$ 的外直积, 则

(1) 如果 $e_1, e_2, \cdots, e_n$ 分别是群 $G_1, G_2, \cdots G_n$ 的单位元, 则 $(e_1, e_2, \cdots, e_n)$ 是 G 的单位元. 进一步, 设 $(g_1, g_2, \cdots, g_n) \in G$, 则 $(g_1, g_2, \cdots, g_n)^{-1} = \left(g_1^{-1}, g_2^{-1}, \cdots, g_n^{-1}\right)$;

(2) G 是有限群的充分必要条件是 $G_1, G_2, \cdots, G_n$ 都是有限群. 并且, 当 G 是有限群时, 有 $|G| = |G_1|\,|G_2| \cdots |G_2|$;

注 134.1

设 $G = G_1 \times G_2 \times \cdots \times G_n$ 是群 $G_1, G_2, \cdots, G_n$ 的外直积, 则

(1) 如果 $e_1, e_2, \cdots, e_n$ 分别是群 $G_1, G_2, \cdots G_n$ 的单位元, 则 $(e_1, e_2, \cdots, e_n)$ 是 G 的单位元. 进一步, 设 $(g_1, g_2, \cdots, g_n) \in G$, 则 $(g_1, g_2, \cdots, g_n)^{-1} = (g_1^{-1}, g_2^{-1}, \cdots, g_n^{-1})$;

(2) G 是有限群的充分必要条件是 $G_1, G_2, \cdots, G_n$ 都是有限群. 并且, 当 G 是有限群时, 有 $|G| = |G_1|\,|G_2| \cdots |G_2|$;

(3) 当 $G_1, G_2, \cdots, G_n$ 都是加群时, 它们的外直积通常记作 $G_1 \oplus G_2 \oplus \cdots \oplus G_n$, 并称为**外直和**.

例

例 135

(1) $\mathbb{R}^n = \mathbb{R} \times \cdots \times \mathbb{R}$;

例 135

(1) $\mathbb{R}^n = \mathbb{R} \times \cdots \times \mathbb{R}$;

(2) 由例 92 知 4 阶群 $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ 必同构于 Klein 四元群 $G = \{e, a, b, ab\}$ 或 4 阶循环群.

例 135

(1) $\mathbb{R}^n = \mathbb{R} \times \cdots \times \mathbb{R}$;

(2) 由例 92 知 4 阶群 $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ 必同构于 Klein 四元群 $G = \{e, a, b, ab\}$ 或 4 阶循环群.注意到对任意 $(a, b) \in \mathbb{Z}_2 \oplus \mathbb{Z}_2$ 有 $(a, b) + (a, b) = (0, 0)$. 因此 $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ 不是循环群. 令 G 到 $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ 的映射 ϕ 为 $\phi(e) = (0, 0), \phi(a) = (1, 0), \phi(b) = (0, 1), \phi(ab) = (1, 1)$, 则 ϕ 是一同构映射. 事实上, G 到 $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ 的任意一个将 e 映射到零元 $(0, 0)$ 的一一映射都是一个同构映射.

定理 136

设 $G = G_1 \times G_2 \times \cdots \times G_n$ 是群 $G_1, G_2, \cdots, G_n$ 的外直积, 则 G 是交换群的充分必要条件是 $G_1, G_2, \cdots, G_n$ 都是交换群.

外直积的性质

定理 136

设 $G = G_1 \times G_2 \times \cdots \times G_n$ 是群 $G_1, G_2, \cdots, G_n$ 的外直积, 则 G 是交换群的充分必要条件是 $G_1, G_2, \cdots, G_n$ 都是交换群.

证明: 如果 $G_1, G_2, \cdots, G_n$ 都是交换群, 则对任意的 $(g_1, g_2, \cdots, g_n), (g_1', g_2', \cdots, g_n') \in G$ 有

$$\begin{aligned}(g_1, g_2, \cdots, g_n) \cdot (g_1', g_2', \cdots, g_n') &= (g_1 g_1', g_2 g_2', \cdots, g_n g_n') \\ &= (g_1' g_1, g_2' g_2, \cdots, g_n' g_n) \\ &= (g_1', g_2', \cdots, g_n') \cdot (g_1, g_2, \cdots, g_n),\end{aligned}$$

所以 G 是交换群.

外直积的性质

定理 136

设 $G = G_1 \times G_2 \times \cdots \times G_n$ 是群 $G_1, G_2, \cdots, G_n$ 的外直积, 则 G 是交换群的充分必要条件是 $G_1, G_2, \cdots, G_n$ 都是交换群.

证明: 如果 $G_1, G_2, \cdots, G_n$ 都是交换群, 则对任意的 $(g_1, g_2, \cdots, g_n), (g_1', g_2', \cdots, g_n') \in G$ 有

$$\begin{aligned}(g_1, g_2, \cdots, g_n) \cdot (g_1', g_2', \cdots, g_n') &= (g_1 g_1', g_2 g_2', \cdots, g_n g_n') \\ &= (g_1' g_1, g_2' g_2, \cdots, g_n' g_n) \\ &= (g_1', g_2', \cdots, g_n') \cdot (g_1, g_2, \cdots, g_n),\end{aligned}$$

所以 G 是交换群. 反之, 如果 G 是交换群, 那么对任意的 $(g_1, g_2, \cdots, g_n), (g_1', g_2', \cdots, g_n') \in G$ 有 $(g_1, g_2, \cdots, g_n) \cdot (g_1', g_2', \cdots, g_n') = (g_1', g_2', \cdots, g_n') \cdot (g_1, g_2, \cdots, g_n)$, 即 $(g_1 g_1', g_2 g_2', \cdots, g_n g_n') = (g_1' g_1, g_2' g_2, \cdots, g_n' g_n)$. 因此 $g_i g_i' = g_i' g_i$ 对任意 $1 \le i \le n$. 从而 $G_1, G_2, \cdots, G_n$ 都是交换群.

外直积的性质

定理 137

设 $G=G_1\times G_2\times\cdots\times G_n$ 是群 $G_1,G_2,\cdots,G_n$ 的外直积, 则对任意 $\sigma\in S_n$ 有 $G_1\times G_2\times\cdots\times G_n\cong G_{\sigma(1)}\times G_{\sigma(2)}\times\cdots\times G_{\sigma(n)}$.

外直积的性质

定理 137

设 $G = G_1 \times G_2 \times \cdots \times G_n$ 是群 $G_1, G_2, \cdots, G_n$ 的外直积, 则对任意 $\sigma \in S_n$ 有 $G_1 \times G_2 \times \cdots \times G_n \cong G_{\sigma(1)} \times G_{\sigma(2)} \times \cdots \times G_{\sigma(n)}$.

证明: 构造映射

$$\phi: G_1 \times G_2 \times \cdots \times G_n \longrightarrow G_{\sigma(1)} \times G_{\sigma(2)} \times \cdots \times G_{\sigma(n)},$$

$$(a_1, a_2, \cdots, a_n) \longmapsto \left(a_{\sigma(1)}, a_{\sigma(2)}, \cdots, a_{\sigma(n)}\right),$$

则 ϕ 是一一映射.

证明 (续)

注意到

$$
\begin{aligned}
&\phi\big((a_1,a_2,\cdots,a_n)\cdot(b_1,b_2,\cdots,b_n)\big)\\
&=\phi\,(a_1b_1,a_2b_2,\cdots,a_nb_n)\\
&=\big(a_{\sigma(1)}b_{\sigma(1)},a_{\sigma(2)}b_{\sigma(2)},\cdots,a_{\sigma(n)}b_{\sigma(n)}\big)\\
&=\big(a_{\sigma(1)},a_{\sigma(2)},\cdots,a_{\sigma(n)}\big)\cdot\big(b_{\sigma(1)},b_{\sigma(2),\cdots,b_{\sigma(n)}}\big)\\
&=\phi\big(a_1,a_2,\cdots,a_n\big)\phi\big(b_1,b_2,\cdots,b_n\big).
\end{aligned}
$$

证明 (续)

注意到

$$\begin{aligned}
&\phi\big((a_1,a_2,\cdots,a_n)\cdot(b_1,b_2,\cdots,b_n)\big)\\
=\,&\phi\,(a_1b_1,a_2b_2,\cdots,a_nb_n)\\
=\,&\big(a_{\sigma(1)}b_{\sigma(1)},a_{\sigma(2)}b_{\sigma(2)},\cdots,a_{\sigma(n)}b_{\sigma(n)}\big)\\
=\,&\big(a_{\sigma(1)},a_{\sigma(2)},\cdots,a_{\sigma(n)}\big)\cdot\big(b_{\sigma(1)},b_{\sigma(2),\cdots,b_{\sigma(n)}}\big)\\
=\,&\phi\big(a_1,a_2,\cdots,a_n\big)\phi\big(b_1,b_2,\cdots,b_n\big).
\end{aligned}$$

因此, ϕ 是 $G_1\times G_2\times\cdots\times G_n$ 到 $G_{\sigma(1)}\times G_{\sigma(2)}\times\cdots\times G_{\sigma(n)}$ 的同构映射, 从而

$$G_1\times G_2\times\cdots\times G_n\cong G_{\sigma(1)}\times G_{\sigma(2)}\times\cdots\times G_{\sigma(n)}.$$

外直积的性质

定理 138

设 $G=G_1\times G_2\times\cdots\times G_n$ 是群 $G_1,G_2,\cdots,G_n$ 的外直积, $e_1,e_2,\cdots,e_n$ 分别是群 $G_1,G_2,\cdots G_n$ 的单位元, 则

(1) 定义 $H_i=\{e_1\}\times\cdots\times\{e_{i-1}\}\times G_i\times\{e_{i+1}\}\times\cdots\times\{e_n\}$, 则 H_i 是 G 的一个正规子群, 且同构于 G_i;

(2) $G=H_1H_2\cdots H_n$;

(3) 如果 $h_1h_2\cdots h_n=h_1'h_2'\cdots h_n'$, 其中 $h_i,h_i'\in H_i$, 则对所有 $1\le i\le n$ 有 $h_i=h_i'$.

定理 138

设 $G = G_1 \times G_2 \times \cdots \times G_n$ 是群 $G_1, G_2, \cdots, G_n$ 的外直积, $e_1, e_2, \cdots, e_n$ 分别是群 $G_1, G_2, \cdots G_n$ 的单位元, 则

(1) 定义 $H_i = \{e_1\} \times \cdots \times \{e_{i-1}\} \times G_i \times \{e_{i+1}\} \times \cdots \times \{e_n\}$, 则 H_i 是 G 的一个正规子群, 且同构于 G_i;

(2) $G = H_1 H_2 \cdots H_n$;

(3) 如果 $h_1 h_2 \cdots h_n = h_1' h_2' \cdots h_n'$, 其中 $h_i, h_i' \in H_i$, 则对所有 $1 \leq i \leq n$ 有 $h_i = h_i'$.

证明: (1) 由于 e_i 和 G_i 都是 G 的正规子群, 由正规子群的定义和外直积的定义易验证 H_i 是 G 的正规子群.

证明 (续)

现证 H_i 同构于 G_i. 令

$$\begin{aligned} \phi: \quad G_i &\longrightarrow H_i, \\ g_i &\longmapsto (e_1, \cdots, e_{i-1}, g_i, e_{i+1}, \cdots, e_n), \end{aligned}$$

则易验证 ϕ 是 H_i 到 G_i 的同构映射.

证明 (续)

现证 H_i 同构于 G_i. 令

$$\begin{array}{rccl} \phi: & G_i & \longrightarrow & H_i, \\ & g_i & \longmapsto & (e_1, \cdots, e_{i-1}, g_i, e_{i+1}, \cdots, e_n), \end{array}$$

则易验证 ϕ 是 H_i 到 G_i 的同构映射.

(2) 设有 $g = (g_1, g_2, \cdots, g_n) \in G$, 其中 $g_i \in G_i$. 于是有
$g = (g_1, e_2, e_3, \cdots, e_{n-1}, e_n) \cdot (e_1, g_2, e_3, \cdots, e_{n-1}, e_n) \cdot \cdots \cdot$
$(e_1, e_2, e_3, \cdots, e_{n-1}, g_n) \in H_1 H_2 \cdots H_n$, 于是 $G \subseteq H_1 H_2 \cdots H_n$.
反之, 显然有 $H_1 H_2 \cdots H_n \subseteq G$. 因此, $G = H_1 H_2 \cdots H_n$.

现证 H_i 同构于 G_i. 令

$$\begin{array}{rccl}\phi: & G_i & \longrightarrow & H_i, \\ & g_i & \longmapsto & (e_1,\cdots,e_{i-1},g_i,e_{i+1},\cdots,e_n),\end{array}$$

则易验证 ϕ 是 H_i 到 G_i 的同构映射.

(2) 设有 $g=(g_1,g_2,\cdots,g_n)\in G$, 其中 $g_i\in G_i$. 于是有
$g=(g_1,e_2,e_3,\cdots,e_{n-1},e_n)\cdot(e_1,g_2,e_3,\cdots,e_{n-1},e_n)\cdot\cdots\cdot$
$(e_1,e_2,e_3,\cdots,e_{n-1},g_n)\in H_1H_2\cdots H_n$, 于是 $G\subseteq H_1H_2\cdots H_n$.
反之, 显然有 $H_1H_2\cdots H_n\subseteq G$. 因此, $G=H_1H_2\cdots H_n$.

(3) 显然对任意 $a\in H_i, b\in H_j$ 有 $ab=ba$, 其中 $i\neq j$. 设有
$h=h_1h_2\cdots h_n=h_1'h_2'\cdots h_n'\in H_1H_2\cdots H_n$, 其中
$h_i=(e_1,\cdots,e_{i-1},g_i,e_{i+1},\cdots,e_n)\in H_i$,
$h_i'=(e_1,\cdots,e_{i-1},g_i',e_{i+1},\cdots,e_n)\in H_i$, $g_i,g_i'\in G_i$. 可得
${h_1'}^{-1}h_1{h_2'}^{-1}h_2\cdots{h_n'}^{-1}h_n=e=({g_1'}^{-1}g_1,{g_2'}^{-1}g_2,\cdots,{g_n'}^{-1}g_n)$. 由
于 G 的单位元是 $e=(e_1,e_2,\cdots,e_n)$, 因此对所有 $1\leq i\leq n$ 有
$g_i=g_i'$, 于是有 $h_i=h_i'$.

例

例 139

设 $G_1 = \langle a \rangle, G_2 = \langle b \rangle$ 分别是 3 阶和 5 阶的循环群, 则 $G = G_1 \times G_2$ 是一个 15 阶的循环群.

例 139

设 $G_1 = \langle a \rangle, G_2 = \langle b \rangle$ 分别是 3 阶和 5 阶的循环群, 则 $G = G_1 \times G_2$ 是一个 15 阶的循环群.

解: 首先, 由定理 136 知, G 是一个 15 阶的交换群. 设 e_1, e_2 分别是 G_1, G_2 的单位元, 取 $c = (a, b) \in G$, 其中 $a \neq e_1, b \neq e_2$, 则

$$c^3 = \left(e_1, b^3\right), \quad c^5 = \left(a^2, e_2\right),$$

所以 c^3, c^5 都不等于 (e_1, e_2). 可知 $\operatorname{ord} c \neq 3, 5$. 由拉格朗日定理知, $\operatorname{ord} c = 15$. 即 $G = \langle c \rangle$ 是 15 阶循环群.

外直积元素的阶

定理 140

设 G_1, G_2 是两个群，a 和 b 分别是 G_1 和 G_2 中的有限阶元素，则对于 $(a,b) \in G_1 \times G_2$，有

$$\operatorname{ord}(a,b) = [\operatorname{ord} a, \operatorname{ord} b].$$

外直积元素的阶

定理 140

设 G_1, G_2 是两个群, a 和 b 分别是 G_1 和 G_2 中的有限阶元素, 则对于 $(a,b) \in G_1 \times G_2$, 有

$$\operatorname{ord}(a,b) = [\operatorname{ord} a, \operatorname{ord} b].$$

证明: 设 $\operatorname{ord} a = m, \operatorname{ord} b = n, s = [m,n]$, 则

$$(a,b)^s = (a^s, b^s) = (e_1, e_2)\,.$$

从而 (a,b) 的阶有限, 设其为 t, 则需证明 $t = s$. 由上式有 $t \mid s$. 下证 $s \mid t$. 因为

$$(e_1, e_2) = (a,b)^t = \left(a^t, b^t\right),$$

所以, $a^t = e_1, b^t = e_2$. 于是, $m \mid t$ 且 $n \mid t$, 从而 t 是 m 和 n 的公倍数. 而 s 是 m 和 n 的最小公倍数, 因此 $s \mid t$. 结合以上讨论得 $s = t$.

例 141

下面来确定 $\mathbb{Z}_{15} \oplus \mathbb{Z}_5$ 中 5 阶元素的个数. 由定理 140, 就是要确定 $\mathbb{Z}_{15} \oplus \mathbb{Z}_5$ 中满足 $5 = \operatorname{ord}(a, b) = [\operatorname{ord} a, \operatorname{ord} b]$ 的元素 (a, b) 的个数. 显然这就要求或者 $\operatorname{ord} a = 5$ 且 $\operatorname{ord} b = 1$ 或 5, 或者 $\operatorname{ord} a = 1$ 且 $\operatorname{ord} b = 5$. 下面分情况讨论.

例 141

下面来确定 $\mathbb{Z}_{15} \oplus \mathbb{Z}_5$ 中 5 阶元素的个数. 由定理 140, 就是要确定 $\mathbb{Z}_{15} \oplus \mathbb{Z}_5$ 中满足 $5 = \operatorname{ord}(a, b) = [\operatorname{ord} a, \operatorname{ord} b]$ 的元素 (a, b) 的个数. 显然这就要求或者 $\operatorname{ord} a = 5$ 且 $\operatorname{ord} b = 1$ 或 5, 或者 $\operatorname{ord} a = 1$ 且 $\operatorname{ord} b = 5$. 下面分情况讨论.

(1) $\operatorname{ord} a = \operatorname{ord} b = 5$. 此时 a 有 4 种选择 (即 $3, 6, 9, 12$), b 也有 4 种选择, 从而共有 16 个 5 阶元素;

例 141

下面来确定 $\mathbb{Z}_{15} \oplus \mathbb{Z}_5$ 中 5 阶元素的个数. 由定理 140, 就是要确定 $\mathbb{Z}_{15} \oplus \mathbb{Z}_5$ 中满足 $5 = \operatorname{ord}(a,b) = [\operatorname{ord} a, \operatorname{ord} b]$ 的元素 (a,b) 的个数. 显然这就要求或者 $\operatorname{ord} a = 5$ 且 $\operatorname{ord} b = 1$ 或 5, 或者 $\operatorname{ord} a = 1$ 且 $\operatorname{ord} b = 5$. 下面分情况讨论.

(1) $\operatorname{ord} a = \operatorname{ord} b = 5$. 此时 a 有 4 种选择 (即 $3, 6, 9, 12$), b 也有 4 种选择, 从而共有 16 个 5 阶元素;

(2) $\operatorname{ord} a = 5, \operatorname{ord} b = 1$. 此时 a 仍有 4 种选择, 而 b 只有一种选择, 故共有 4 个 5 阶元素;

例

例 141

下面来确定 $\mathbb{Z}_{15} \oplus \mathbb{Z}_5$ 中 5 阶元素的个数. 由定理 140, 就是要确定 $\mathbb{Z}_{15} \oplus \mathbb{Z}_5$ 中满足 $5 = \operatorname{ord}(a,b) = [\operatorname{ord} a, \operatorname{ord} b]$ 的元素 (a,b) 的个数. 显然这就要求或者 $\operatorname{ord} a = 5$ 且 $\operatorname{ord} b = 1$ 或 5, 或者 $\operatorname{ord} a = 1$ 且 $\operatorname{ord} b = 5$. 下面分情况讨论.

(1) $\operatorname{ord} a = \operatorname{ord} b = 5$. 此时 a 有 4 种选择 (即 $3, 6, 9, 12$), b 也有 4 种选择, 从而共有 16 个 5 阶元素;

(2) $\operatorname{ord} a = 5, \operatorname{ord} b = 1$. 此时 a 仍有 4 种选择, 而 b 只有一种选择, 故共有 4 个 5 阶元素;

(3) $\operatorname{ord} a = 1, \operatorname{ord} b = 5$. 此时 a 只有一种选择, 而 b 有 4 种选择, 故也有 4 个 5 阶元素.

于是, $\mathbb{Z}_{15} \oplus \mathbb{Z}_5$ 共有 24 个 5 阶元素.

循环群的外直积

定理 142

设 G_1 和 G_2 分别是 m 阶及 n 阶的循环群，则 $G_1 \times G_2$ 是循环群的充要条件是 $(m, n) = 1$.

定理 142

设 G_1 和 G_2 分别是 m 阶及 n 阶的循环群，则 $G_1 \times G_2$ 是循环群的充要条件是 $(m, n) = 1$.

证明: 设 $G_1 = \langle a \rangle, G_2 = \langle b \rangle$.

假设 $G_1 \times G_2$ 是循环群. 若 $(m, n) = t \neq 1$, 则由于 $\operatorname{ord} a = m$, ord $b = n$, 而 $a^{m/t}$ 和 $b^{n/t}$ 的阶都是 t, 因此 $\langle (a^{m/t}, e_2) \rangle$ 和 $\langle (e_1, b^{n/t}) \rangle$ 是循环群 $G_1 \times G_2$ 中的两个不同的 t 阶子群. 而这与推论 103 的第 (2) 条相矛盾, 所以 $(m, n) = 1$.

定理 142

设 G_1 和 G_2 分别是 m 阶及 n 阶的循环群，则 $G_1 \times G_2$ 是循环群的充要条件是 $(m,n)=1$.

证明: 设 $G_1=\langle a\rangle, G_2=\langle b\rangle$.

假设 $G_1 \times G_2$ 是循环群. 若 $(m,n)=t\neq 1$, 则由于 $\operatorname{ord} a=m$, ord $b=n$, 而 $a^{m/t}$ 和 $b^{n/t}$ 的阶都是 t, 因此 $\langle(a^{m/t},e_2)\rangle$ 和 $\langle(e_1,b^{n/t})\rangle$ 是循环群 $G_1\times G_2$ 中的两个不同的 t 阶子群. 而这与推论 103 的第 (2) 条相矛盾, 所以 $(m,n)=1$.

反之, 假设 $(m,n)=1$, 则

$$\begin{aligned}\operatorname{ord}(a,b)&=[m,n]=mn\\&=|G_1|\cdot|G_2|=|G_1\times G_2|\end{aligned}$$

所以 (a,b) 是 $G_1\times G_2$ 的生成元, 因此 $G_1\times G_2$ 是循环群.

群的内直积

定义 143

设 $H_1, \cdots, H_n$ 是 G 的子群. 如果群 G 满足下述三个条件:

(1) $H_1, \cdots, H_n$ 都是 G 的正规子群;

(2) $G = H_1 H_2 \cdots H_n$;

(3) 如果 $h_1 \cdots h_n = h'_1 \cdots h'_n$, 其中 $h'_i, h_i \in H_i$, 则对所有 $1 \leq i \leq n$ 有 $h_i = h'_i$,

则称 G 是 $H_1, \cdots, H_n$ 的**内直积** (internal direct product).

引理 144

如果群 G 是有限多个正规子群 $H_1, H_2, \cdots, H_n$ 的内直积, 则对任意 $a \in H_i, b \in H_j$ 有 $ab = ba$, 其中 $i \neq j$.

引理 144

如果群 G 是有限多个正规子群 $H_1, H_2, \cdots, H_n$ 的内直积, 则对任意 $a \in H_i, b \in H_j$ 有 $ab = ba$, 其中 $i \neq j$.

证明: 由于 $ab \in aH_j = H_j a$, 从而存在 $b' \in H_j$ 使得 $ab = b'a$. 同理, 由 $ab \in H_i b = bH_i$ 可知存在 $a' \in H_i$ 使得 $ab = ba'$. 于是可得 $b'a = ba'$. 由内直积中每个元素表示法唯一性可知
$b' = b, a' = a$.

注 144.1

设群 G 是有限多个正规子群 $H_1, H_2, \cdots, H_n$ 的内直积, 由定义 *143* 可得:

注 144.1

设群 G 是有限多个正规子群 $H_1, H_2, \cdots, H_n$ 的内直积, 由定义 *143* 可得*:*

(1) 定义 *143* 中的第 *(3)* 条即为对任意 $h \in G$ 时, 若有 $h = h_1 \cdots h_n$, 其中 $h_i \in H_i$, 则 h 的表示法唯一. 特别地, 若 G 的单位元 $e = h_1 \cdots h_n$, 其中 $h_i \in H_i$, 则有 $h_i = e$, 这是因为 $e = e \cdots e$;

注 144.1

设群 G 是有限多个正规子群 $H_1, H_2, \cdots, H_n$ 的内直积, 由定义 *143* 可得:

(1) 定义 *143* 中的第 *(3)* 条即为对任意 $h \in G$ 时, 若有 $h = h_1 \cdots h_n$, 其中 $h_i \in H_i$, 则 h 的表示法唯一. 特别地, 若 G 的单位元 $e = h_1 \cdots h_n$, 其中 $h_i \in H_i$, 则有 $h_i = e$, 这是因为 $e = e \cdots e$;

(2) 由引理 *144* 可得若有 $h = h_1 h_2 \cdots h_n$, $h' = h_1' h_2' \cdots h_n'$, 其中 $h_i, h_i' \in H_i$, 则 $hh' = h_1 h_1' h_2 h_2' \cdots h_n h_n'$;

注 144.1

设群 G 是有限多个正规子群 $H_1, H_2, \cdots, H_n$ 的内直积, 由定义 *143* 可得:

(1) 定义 *143* 中的第 *(3)* 条即为对任意 $h \in G$ 时, 若有 $h = h_1 \cdots h_n$, 其中 $h_i \in H_i$, 则 h 的表示法唯一. 特别地, 若 G 的单位元 $e = h_1 \cdots h_n$, 其中 $h_i \in H_i$, 则有 $h_i = e$, 这是因为 $e = e \cdots e$;

(2) 由引理 *144* 可得若有 $h = h_1 h_2 \cdots h_n$, $h' = h_1' h_2' \cdots h_n'$, 其中 $h_i, h_i' \in H_i$, 则 $hh' = h_1 h_1' h_2 h_2' \cdots h_n h_n'$;

(3) 定义 *143* 中的第 *(3)* 条可等价为单位元 e 的表示法唯一.

内直积的性质

定理 145

如果群 G 是有限多个正规子群 $H_1, H_2, \cdots, H_n$ 的内直积, 则 $G \cong H_1 \times H_2 \times \cdots \times H_n$.

内直积的性质

定理 145

如果群 G 是有限多个正规子群 $H_1, H_2, \cdots, H_n$ 的内直积, 则 $G \cong H_1 \times H_2 \times \cdots \times H_n$.

证明: 构造映射

$$\phi: \ H_1 \times H_2 \times \cdots \times H_n \longrightarrow G,$$

$$(h_1, h_2, \cdots, h_n) \longmapsto h_1 h_2 \cdots h_n.$$

定理 145

如果群 G 是有限多个正规子群 $H_1, H_2, \cdots, H_n$ 的内直积, 则 $G \cong H_1 \times H_2 \times \cdots \times H_n$.

证明: 构造映射

$$\phi: H_1 \times H_2 \times \cdots \times H_n \longrightarrow G,$$

$$(h_1, h_2, \cdots, h_n) \longmapsto h_1 h_2 \cdots h_n.$$

由定义 143 第 (3) 条知 ϕ 为单射, 由定义 143 第 (2) 条知 ϕ 为满射. 注意到对任意 $(h_1, \cdots, h_n), (h_1', \cdots, h_n') \in H_1 \times \cdots \times H_n$ 有

$$\begin{aligned}
\phi((h_1, \cdots, h_n) \cdot (h_1', \cdots, h_n')) &= \phi(h_1 h_1', h_2 h_2', \cdots, h_n h_n') \\
&= h_1 h_1' \cdots h_n h_n' \\
&= h_1 \cdots h_n h_1' \cdots h_n' \\
&= \phi(h_1, \cdots, h_n) \phi(h_1', \cdots, h_n').
\end{aligned}$$

因此, ϕ 是 $H_1 \times H_2 \times \cdots \times H_n$ 到 G 的同构映射.

注 145.1

外直积 $G = H_1 \times H_2 \times \cdots \times H_n$ 中的群 $H_1, H_2, \cdots, H_n$ 一般并不是 G 中的子群, 故有 "外直积" 之称, 而内直积 $G = H_1 H_2 \cdots H_n$ 中的 $H_1, H_2, \cdots, H_n$ 则都是 G 的子群. 根据定理 *138* 和定理 *145* 可见, 内外直积的概念本质上是一致的, 所以有时可不对内外直积加以区分, 而统称为群的直积.

内直积的判定

定理 146

设群 $G = H_1 H_2 \cdots H_n$, 其中每个 H_i 都是 G 的正规子群, 则下述三条等价:

(1) G 是 $H_i, H_2, \cdots, H_n$ 的内直积;

(2) $H_1 \cdots H_{i-1} \cap H_i = \{e\}$, 对任意 $i = 2, \cdots, n$;

(3) $H_1 \cdots H_{i-1} H_{i+1} \cdots H_n \cap H_i = \{e\}$, 对任意 $i = 2, \cdots, n$.

内直积的判定

定理 146

设群 $G = H_1 H_2 \cdots H_n$, 其中每个 H_i 都是 G 的正规子群, 则下述三条等价:

(1) G 是 $H_i, H_2, \cdots, H_n$ 的内直积;

(2) $H_1 \cdots H_{i-1} \cap H_i = \{e\}$, 对任意 $i = 2, \cdots, n$;

(3) $H_1 \cdots H_{i-1} H_{i+1} \cdots H_n \cap H_i = \{e\}$, 对任意 $i = 2, \cdots, n$.

证明: 我们按照 “(2) ⇒ (1) ⇒ (3) ⇒(2)” 的顺序来证明定理.

内直积的判定

定理 146

设群 $G = H_1 H_2 \cdots H_n$, 其中每个 H_i 都是 G 的正规子群, 则下述三条等价:

(1) G 是 $H_i, H_2, \cdots, H_n$ 的内直积;

(2) $H_1 \cdots H_{i-1} \cap H_i = \{e\}$, 对任意 $i = 2, \cdots, n$;

(3) $H_1 \cdots H_{i-1} H_{i+1} \cdots H_n \cap H_i = \{e\}$, 对任意 $i = 2, \cdots, n$.

证明: 我们按照 "(2) $\Rightarrow$ (1) $\Rightarrow$ (3) $\Rightarrow$(2)" 的顺序来证明定理.

"(2) $\Rightarrow$ (1)" 由定理 39 第 (2) 条知 $H_1 \cdots H_i < G$. 假设任意 $g \in G$ 有两种表示方法 $g = h_1 \cdots h_n = h_1' \cdots h_n'$, 其中 $h_i, h_i' \in H_i$, 其中 $h_i, h_i' \in H_i$, 则

$$(h_1' \cdots h_{n-1}')^{-1}(h_1 \cdots h_{n-1}) = h_n' h_n^{-1} \in H_1 \cdots H_{n-1} \cap H_n.$$

证明 (续)

由 (2) 可得 $h'_n h_n^{-1} = (h'_1 \cdots h'_{n-1})^{-1}(h_1 \cdots h_{n-1}) = e$. 因此 $h'_n = h_n, h'_1 \cdots h'_{n-1} = h_1 \cdots h_{n-1}$. 类似地, 由 $h'_1 \cdots h'_{n-1} = h_1 \cdots h_{n-1}$ 可得 $h'_{n-1} = h_{n-1}$. 以此类推可得 $h'_{n-2} = h_{n-2}, h'_{n-3} = h_{n-3}, \cdots, h'_1 = h_1$.

证明 (续)

由 (2) 可得 $h'_n h_n^{-1} = (h'_1 \cdots h'_{n-1})^{-1}(h_1 \cdots h_{n-1}) = e$. 因此 $h'_n = h_n, h'_1 \cdots h'_{n-1} = h_1 \cdots h_{n-1}$. 类似地, 由 $h'_1 \cdots h'_{n-1} = h_1 \cdots h_{n-1}$ 可得 $h'_{n-1} = h_{n-1}$. 以此类推可得 $h'_{n-2} = h_{n-2}, h'_{n-3} = h_{n-3}, \cdots, h'_1 = h_1$.

"(1) $\Rightarrow$ (3)" 对任意 $h_i \in H_1 \cdots H_{i-1}H_{i+1} \cdots H_n \cap H_i$ 可得 $h_1 \cdots h_{i-1}h_{i+1} \cdots h_n = h_i \in H_1 \cdots H_{i-1}H_{i+1} \cdots H_n \cap H_i$, 其中 $h_i \in H_i$. 于是

$$e = h_1 \cdots h_{i-1}h_{i+1} \cdots h_n h_i^{-1} = h_1 \cdots h_{i-1}h_i^{-1}h_{i+1} \cdots h_n.$$

当 G 是 $H_1, H_2, \cdots, H_n$ 的内直积时, 由 G 的单位元 e 表示法的唯一性可知 $h_i^{-1} = e$, 从而 $h_i = e$.

"(3) $\Rightarrow$ (2)" 显然.