第 1 章 基础概念

1.1 二元运算

定义 1.1 (数域)

设 P 是由一些复数组成的集合, 其中包括 0 和 1. 如果 P 中任意两个数的和、差、积、商 (除数不为 0) 仍然是 P 中的数, 那么 P 就称为一个**数域**.

♣

定义 1.2

设 A 是一个集合. $A\times A$ 到 A 的一个映射 φ, 称为 A 的一个**二元运算**.

若记 $\varphi(a,b)=ab$, 则称 ab 为 a 与 b 的**积**. 若记 $\varphi(a,b)=a+b$, 则称 $a+b$ 为 a 与 b 的**和**.

若 A 上的二元运算 $\varphi(a,b)=ab$ 满足结合律

$$(ab)c=a(bc),\quad \forall a,b,c\in A,$$

则此二元运算称为**结合的**.

若 A 上的二元运算 $\varphi(a,b)=ab$ 满足交换律

$$ab=ba,\quad \forall a,b\in A,$$

则此二元运算称为**交换的**. 一般地, 若 $c,d\in A$ 有 $cd=dc$, 则称 c 与 d 是**交换的**.

♣

定义 1.3

设集合 A 有二元运算 $(a,b)\to ab$ 且满足结合律, 则对 $\forall n\in\mathbb{N}$ ($\mathbb{N}$ 表示自然数, 即正整数的集合), 定义

$$a^1=a,\quad a^{n+1}=a^n\cdot a,\quad \forall a\in A,$$

a^n 称为 a 的 ***n* 次乘幂**, 也简称 ***n* 次幂**.

在 A 中也可以定义**连乘积**

$$\prod_{i=1}^{n}a_i=\left(\prod_{i=1}^{n-1}a_i\right)a_n,\quad a_i\in A, i=1,2,\cdots,n.$$

♣

命题 1.1

1. $a^na^m=a^{n+m}, (a^m)^n=a^{nm}(\forall a\in A, m,n\in\mathbb{N})$.
2. 若 $a,b\in A$ 且 $ab=ba$, 则 $(ab)^n=a^nb^n(\forall n\in\mathbb{N})$.
3. 若有

$$0=n_0<n_1<\cdots<n_r=n,$$

则

$$\prod_{j=1}^{r}\left(\prod_{k=n_{j-1}+1}^{n_j}a_k\right)=\prod_{i=1}^{n}a_i.$$

♠

证明 证明是显然的.

□

定义 1.4

如果将二元运算记为加法且满足结合律, 于是可定义**倍数**与**连加**如下:

$$1 \cdot a = a, \quad (n+1)a = na + a,$$
$$\sum_{i=1}^{n} a_i = \left(\sum_{i=1}^{n-1} a_i\right) + a_n.$$

♣

命题 1.2

1. $na + ma = (n+m)a, \quad n(ma) = (nm)a, \quad \forall a \in A, m, n \in \mathbb{N}.$
2. 若 $a + b = b + a$, 则
$$n(a+b) = na + nb, \quad \forall n \in \mathbb{N},$$
3. 若有
$$0 = n_0 < n_1 < \cdots < n_r = n,$$
则
$$\sum_{j=1}^{r}\left(\sum_{k=n_{j-1}+1}^{n_j} a_k\right) = \sum_{i=1}^{n} a_i.$$

♠

证明 证明是显然的.

□

1.2 幺半群和群

定义 1.5 ((幺) 半群)

设 S 是非空集合. 在 S 中定义了二元运算称为乘法, 满足结合律, 即

$$(ab)c = a(bc), \quad \forall a, b, c \in S,$$

则称 S 为**半群**.

如果在半群 M 中存在元素 1, 使得

$$1a = a1 = a, \quad \forall a \in M, \tag{1.1}$$

则称 M 为幺半群, 1 称为**幺元素**或**幺元**或**单位元**.

如果一个幺半群 M(或半群 S) 的乘法还满足交换律, 即

$$ab = ba, \quad \forall a, b \in M\,(\text{或}S),$$

则称 M(或 S) 为**交换幺半群** (或**交换半群**), 也简单地称 M(或 S) 为**可换的**.

对于交换幺半群, 有时把二元运算记为加法, 此时幺元素记为 0, 改称**零元素**或**零**.

♣

例题 1.1

(1) $\mathbb{N}$ 对乘法是幺半群, 对加法是半群而不是幺半群. 非负整数集对加法与乘法均为幺半群.

(2) 令 $M(X)$ 为非空集 X 的所有变换 (即 X 到 X 的映射) 的集合, 则对于变换的乘法, $M(X)$ 是一个幺半群, id_X 是一个幺元素. 当 $|X| \geqslant 2$ 时, $M(X)$ 不是可换的.

(3) 设 $P(X)$ 为非空集合 X 的所有子集的集合. 空集 $\varnothing$ 也是 X 的一个子集, 则 $P(X)$ 对集合的并的运算是一个幺半群, $\varnothing$ 为幺元素. 同样, $P(X)$ 对集合的交的运算是一个幺半群, X 为幺元素, 这两种幺半群都是可换的.

命题 1.3

幺半群中的幺元素是唯一的.

♠

证明 如果 1 与 $1'$ 都是幺半群 M 的幺元素, 则由条件 (1.1)可知 $1 = 1'$.

□

定义 1.6 (群)

在非空集合 G 中定义了二元运算, 称为乘法. 若满足下列条件:

(1) 结合律成立, 即 $(ab)c = a(bc)(\forall a, b, c \in G)$;

(2) 存在**左幺元**, 即 $\exists e \in G$, 使 $ea = a(\forall a \in G)$;

(3) 对 $\forall a \in G$ 有**左逆元**, 即有 $b \in G$, 使 $ba = e$,

则称 $(G, \cdot)$ 或 G 是一个**群**. 若 G 的乘法还满足交换律, 则称 G 为**交换群**或 **Abel 群**.

有时将 Abel 群的运算记作加法. 这时左幺元改称**零元**, 以 0 表示; a 的左逆元改称 a 的**负元**, 记为 $-a$.

♣

注 数域 $\mathbb{P}$ 对加法构成一个群, 左幺元为 0, a 的左逆元为 $-a$. $\mathbb{P}$ 对乘法是幺半群, 不是群. 但是 $\mathbb{P}$ 中非零元素的集合 $\mathbb{P}^*$ 对乘法是群, 1 为左幺元, $1/a$ 为 a 的左逆元.

定理 1.1

设 m 是大于 1 的正整数, 记

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

则 $U(m)$ 关于剩余类的乘法构成群. 群 $(U(m), \cdot)$ 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

$$\mathbb{Z}_p^* = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}.$$

♡

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

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

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

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

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

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

$$(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{ab} \cdot \overline{c} = \overline{(ab)c} = \overline{a(bc)} = \overline{a} \cdot \overline{bc} = \overline{a} \cdot (\overline{b} \cdot \overline{c}).$$

所以结合律成立.

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

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

所以 $\overline{1}$ 为 $U(m)$ 的单位元.

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

$$au + mv = 1.$$

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

$$\overline{a} \cdot \overline{u} = \overline{au} = \overline{au + mv} = \overline{1},$$

$$\overline{u}\cdot\overline{a}=\overline{ua}=\overline{au}=\overline{1}.$$

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

这就证明了,$U(m)$ 关于剩余类的乘法构成群.

□

定理 1.2 (群的基本性质)

设 $(G,\cdot)$ 是一个群,$a\in G$,1 是 G 的左幺元, 则

(1) 若 b 为 a 的左逆元, 则 b 也是 a 的**右逆元**, 即有 $ab=1$, 故称 b 为 a 的**逆元**.

(2) 任一元素 a 的逆元唯一, 记为 a^{-1}, 并且 $1^{-1}=1,(a^{-1})^{-1}=a,(ab)^{-1}=b^{-1}a^{-1},(a^n)^{-1}=(a^{-1})^n$.

(3) 若 $a_1,a_2,\cdots,a_r\in G$, 则

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

(4) 1 也是 G 的**右幺元**, 即 $a\cdot 1=a\ (\forall a\in G)$, 故 1 为 G 的**幺元**. 故 G 为幺半群, 幺元唯一.

(5) 群运算满足**消去律**, 即

$$ax=bx \text{ 或 } xa=xb,\ \text{则}a=b,\ \forall a,b,x\in G.$$

(6) 对 $\forall a,b\in G$, 群中方程 $ax=b$ 与 $xa=b$ 的解都存在且唯一.

♡

证明

(1) 事实上, 设 c 是 b 的左逆元, 则有

$$ab=1\cdot(ab)=(cb)(ab)=c(ba)b=c(1\cdot b)=1.$$

(2) 设 b_1,b_2 均为 a 的逆元, 则有

$$b_1=b_1\cdot 1=b_1(ab_2)=(b_1a)b_2=1\cdot b_2=b_2.$$

其余各式显然.

(3) 只需注意到 $(a_1a_2\cdots a_r)(a_r^{-1}a_{r-1}^{-1}\cdots a_1^{-1})=1$ 即可.

(4) 设 b 为 a 的逆元, 则有

$$a\cdot 1=a(ba)=(ab)a=1\cdot a=a.$$

(5) 两边同乘 x^{-1} 即得.

(6) 事实上, $x=a^{-1}b$ 和 $x=ba^{-1}$ 分别为两个方程的解, 由性质 (5)知解唯一.

□

定理 1.3

设 G 是一个具有乘法运算 (对乘法封闭) 且满足结合律的非空集合, 则 G 构成群的充分必要条件是对任意的 $a,b\in G$, 方程

$$ax=b \quad 与 \quad ya=b$$

在 G 中都有解. 并且当 G 为群时, 上述方程的解存在且唯一.

♡

证明 **必要性**: 由定理 1.2(6)立得.

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

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

从而知 e 是 G 的左单位元.

其次, 对每个 $a\in G$,$ya=e$ 有解, 设为 a'. 于是

$$a'a=e,$$

从而知 a 有左逆元. 故 G 构成群.

□

命题 1.4

设 G 是群.

(1) 如果对任意的 $x \in G$, 都有 $x^2 = e$, 则 G 是一个交换群.

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

♠

证明

(1) 对任意的 $x, y \in G$, 有

$$yx = eyx = (xy)^2yx = xyxyyx = xyexx = xyxx = xy.$$

所以 G 是一个交换群.

(2) **必要性**: 如果 G 为交换群, 则对任意的 $a, b \in G$, 有

$$(ab)^2 = abab = aabb = a^2b^2.$$

充分性: 如果对任意的 $a, b \in G$, 有 $(ab)^2 = a^2b^2$, 则

$$ba = (a^{-1}a)ba(bb^{-1}) = a^{-1}(abab)b^{-1} = a^{-1}(ab)^2b^{-1} = a^{-1}a^2b^2b^{-1} = ab.$$

所以 G 为交换群.

□

例题 1.2 设 G 是有限群. 证明: G 中使 $x^3 = e$ 的元素 x 的个数是奇数.

证明 令 $S = \{x \in G \mid x^3 = e\}$. 由于 G 是有限群, 所以 S 为有限集. 又因为 $e^3 = e$, 所以 $e \in S$, 从而 S 不是空集. 如果另有 $x \neq e$, 使 $x^3 = e$, 则 $(x^{-1})^3 = e$. 因为 $x \neq e$, 所以 $x \neq x^{-1}$. 这说明 S 中的非单位元 (如果有的话) 总是成对出现, 又因为 $e^{-1} = e$, 所以 G 中使 $x^3 = e$ 的元素 x 的个数是奇数.

□

定义 1.7

设 a 是群 G 的元素, 可定义 a 的**非正整数次乘幂**如下:

$$a^0 = 1, \quad a^{-n} = (a^{-1})^n, \quad \forall n \in \mathbb{N}.$$

♣

定理 1.4

设 G 是一个群, 则对 $\forall m, n \in \mathbb{Z}, a, b \in G$ 有

$$a^m \cdot a^n = a^{m+n}, \quad (a^m)^n = a^{mn}, \quad 1^m = 1.$$

又若 $ab = ba$, 则有 $(ab)^m = a^mb^m$.

♡

证明

□

定义 1.8

群 G 中所含元素个数 $|G|$ 称为 G 的**阶**. 若 $|G|$ 有限, 则称 G 为**有限群**; 若 $|G|$ 无限, 则称 G 为**无限群**.

有限群 G 的乘法可列表给出, 此表称为 G 的**群表**. 设 $G = \{1, a_1, a_2, \cdots, a_{n-1}\}$ 为 n 阶群, 则 G 的群表为

	1	a_1	a_2	$\cdots$	a_{n-1}
1	1	a_1	a_2	$\cdots$	a_{n-1}
a_1	a_1	a_1^2	a_1a_2		a_1a_{n-1}
a_2	a_2	a_2a_1	a_2^2		a_2a_{n-1}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
a_{n-1}	a_{n-1}	$a_{n-1}a_1$	$a_{n-1}a_2$	$\cdots$	a_{n-1}^2

同样, 可定义半群与幺半群的阶, 对于有限半群与幺半群, 其运算也可列表给出.

命题 1.5

设 G 是一个群且 $|G| = n$, 若 $A \subseteq G$ 且 $|A| = n$, 则 $A = G$.

命题 1.6

(1) 设 G 是一个具有乘法运算 (对乘法封闭) 的非空有限集合. 如果 G 满足结合律, 有左单位元, 且右消去律成立, 则 G 是一个群.

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

证明

(1) 只需证 G 中每个元素有左逆即可. 设 $G = \{a_1, a_2, \cdots, a_n\}$, 则对任意的 $a \in G$,

$$Ga = \{a_1a, a_2a, \cdots, a_na\} \subseteq G.$$

当 $i \neq j$ 时, 有 $a_ia \neq a_ja$. 否则, 由右消去律得 $a_i = a_j$ 矛盾! 从而 $|Ga| = |G|$, 所以 $Ga = G$. 于是, 对 G 中任一元素 a 及 G 的左单位元 e, 因 $e \in G = Ga$, 所以必存在 $a_i \in G$, 使 $a_ia = e$. 于是 a 有左逆元 a_i. 故由群的定义知 G 为群.

(2) 只需证 e 是 G 的单位元,$a \in G$ 的右逆元 a' 是 a 的逆元即可. 由已知,$a' \in G$, 因此 a' 也有右逆元, 设为 a'', 则

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

于是

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

且

$$ea = (aa')a = a(a'a) = ae = a.$$

于是 e 是 G 的单位元,a' 是 a 的逆元. 从而, 由群的定义知 G 为群.

□

定义 1.9

设 a 是群 G 的元素. 若 $\forall k \in \mathbb{N}, a^k \neq 1$, 则称 a 的**阶为无穷**, 记作 $\operatorname{ord} a = \infty$. 若 $\exists k \in \mathbb{N}$, 使得 $a^k = 1$, 则 $r = \min\{k | k \in \mathbb{N}, a^k = 1\}$ 称为 a 的**阶**, 记作 $\operatorname{ord} a = r$.

定理 1.5 (群的阶的基本性质)

设 $(G, \cdot)$ 是一个群,$a \in G$, 则

(1) a 的阶为无穷当且仅当 $\forall m, n \in \mathbb{Z}$ 且 $m \neq n$ 时, $a^m \neq a^n$.

(2) 设 a 的阶为 d, 则

$$a^m = a^n \iff m \equiv n \pmod{d}. \tag{1.2}$$

特别地, 如果有 $m \in \mathbb{Z}$, 使 $a^m = 1$, 则 $d \mid m$.

(3) a 与 a^{-1} 阶相同.

证明

(1) 事实上, 若 a 的阶为无穷, 而有 $m \neq n$, 使 $a^m = a^n$. 设 $m > n$, 于是 $a^m(a^n)^{-1} = 1$, 而 $a^m(a^n)^{-1} = a^{m-n} = 1$, 自然 $m - n \in \mathbb{N}$. 矛盾.

反之, $\forall m,n\in\mathbb{Z}$ 且 $m\neq n$, 有 $a^m\neq a^n$, 则 $a^{m-n}=a^m(a^n)^{-1}=1$, 即 $\forall k\in\mathbb{N}$ 有 $a^k\neq 1$, 故 a 的阶为无穷.

(2) 设 a 的阶为 d, $m,n\in\mathbb{N}$, 由带余除法知, 一定能找到整数 t_1,t_2,r_1,r_2, 使 $m=dt_1+r_1(0\leqslant r_1<d)$, $n=dt_2+r_2(0\leqslant r_2<d)$. 于是 $a^m=(a^d)^{t_1}a^{r_1}=a^{r_1}$, $a^n=(a^d)^{t_2}a^{r_2}=a^{r_2}$, 因而

$$a^m=a^n\iff a^{r_1}=a^{r_2}\iff a^{r_1-r_2}=a^{r_2-r_1}=1.$$

又 $|r_1-r_2|<d$, 故上式也等价于 $r_1-r_2=0$, 即式 (1.2) 成立.

(3) 由 $(a^n)^{-1}=(a^{-1})^n$ 知 $a^k=1$ 当且仅当 $(a^{-1})^k=1$, 故 a^{-1} 与 a 同阶.

□

1.3 子群与商群

定义 1.10

设 A,B 是群 G 的两个子集, 约定

$$AB=\{ab|a\in A,b\in B\},A^{-1}=\{a^{-1}|a\in A\}.$$

特别地, 当 $A=\{a\}$ 为单点集时, 记 $AB=aB,BA=Ba$. 当然这些符号对半群与幺半群可同样使用.

♣

命题 1.7

设有限群 $N_1,N_2,\cdots,N_k$ 满足

$$N_i\cap N_j=\{1\},\ i\neq j.$$

则

$$|N_1N_2\cdots N_k|=|N_1||N_2|\cdots|N_k|.$$

♠

证明 因为 N_i 都是有限群, 所以设

$$N_i=\{n_1^i,n_2^i,\cdots,n_{|N_i|}^i\},\quad i=1,2,\cdots,k.$$

其中 $n_1^i=1$, $i=1,2,\cdots,k$. 由 $N_i\cap N_j=\{1\}(i\neq j)$ 知当 $i\neq j$ 时, 有

$$n_s^i\neq n_t^j,\quad \forall s,t\in\{1,2,\cdots,k\}.$$

于是

$$N_1N_2\cdots N_k=\{n_{j_1}^1n_{j_2}^2\cdots n_{j_k}^k\mid j_i\in\{1,2,\cdots,|N_i|\},i=1,2,\cdots,k\}.$$

因此直接计算 $N_1N_2\cdots N_k$ 的元素个数可得

$$|N_1N_2\cdots N_k|=|N_1||N_2|\cdots|N_k|.$$

若 $G=N_1\otimes N_2\otimes\cdots\otimes N_k$, 则当 $i\neq j$ 时, 有 $N_i\cap N_j\subseteq N_i\cap\prod\limits_{j\neq i}N_j=\{1\}$, 故此时有

$$|G|=|N_1||N_2|\cdots|N_k|.$$

□

定义 1.11

群 G 的非空子集 H 若对 G 的运算也构成一个群, 则称为 G 的**子群**, 记作 $H<G$.

♣

注 显然, $H=\{1\}$(1 为 G 的幺元) 与 $H=G$ 均为 G 的子群, 称为 G 的**平凡子群**, 其他的子群称为**非平凡子群**.

定理 1.6

设 H 是群 G 的非空子集, 则下列条件等价:

(1) H 是 G 的子群;

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

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

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

♡

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

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

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

(2) $\Rightarrow$ (3). 这是显然的.

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

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

□

推论 1.1

设 H 是群 G 的非空子集, 则下列条件等价:

(1) H 是 G 的子群;

(2) $HH = H, H^{-1} = H$;

(3) $H^{-1}H = H$.

♡

证明

(1)

(2)

(3)

□

命题 1.8

(1) 设 H 是群 G 的非空有限子集. 证明:H 是 G 的子群的充分必要条件是 H 关于 G 的运算封闭.

(2) 若 G 是一个群, 则 G 的任意子群的交 $\bigcap\limits_{H<G} H$ 也是 G 的子群.

(3) 若 H_1, H_2 都是群 G 的子群且 $H_2 \subseteq H_1$, 则 H_2 也是 H_1 的子群.

(4) 设 H, K 是群 G 的两个子群. 则 $H \cup K$ 是 G 的子群的充要条件是 $H \subseteq K$ 或 $K \subseteq H$. 并且群 G 不能被它的两个真子群所覆盖.

♠

注 在这个命题 1.8(4)中, 群 G 可能被它的三个真子群所覆盖. 例如, 群

$$U(8) = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}.$$

易知

$$H = \{\overline{1}, \overline{3}\}, \quad J = \{\overline{1}, \overline{5}\}, \quad K = \{\overline{1}, \overline{7}\}$$

都是 $U(8)$ 的真子群, 且 $U(8) = H \cup J \cup K$.

证明

(1) 必要性显然, 下证充分性. 因为 H 关于 G 的运算封闭, 所以 G 的运算是 H 的代数运算. 又因为 G 的运算满足结合律, 所以 H 的运算也满足结合律.

设 $H=\{a_1,a_2,\cdots,a_n\}$. 对任意的 $a\in H$, 记 $Ha=\{a_1a,a_2a,\cdots,a_na\}$, 则 $Ha\subseteq H$. 于是 $a_ia\neq a_ja(i\neq j)$. 否则, 由 $a_ia=a_ja(i\neq j)$ 可得

$$a_i=a_i(aa^{-1})=(a_ia)a^{-1}=(a_ja)a^{-1}=a_j(aa^{-1})=a_j,$$

显然矛盾! 由此推出 $|Ha|=n=|H|$, 于是 $Ha=H$. 这样, 对任意的 $a,b\in H$, 因为 $Ha=H$, 所以必有 $a_i\in H$, 使 $a_ia=b$. 这说明, 对任意的 $a,b\in H$, 方程 $xa=b$ 在 H 中必有解. 同理可证, 方程 $ay=b$ 在 H 中也有解. 从而, 由定理 1.3知 H 为群.

(2) 设 I 为任一 (有限或无限的) 指标集, $\{H_i\mid i\in I\}$ 为群 G 的一些子群的集合, 令

$$J=\bigcap_{i\in I}H_i,$$

因为 $e\in H_i(\forall i\in I)$, 所以 $e\in\bigcap\limits_{i\in I}H_i$, 从而 J 非空; 对 $\forall a,b\in J$, 有 $a,b\in H_i(\forall i\in I)$. 由于 $H_i<G$, 因此 $ab^{-1}\in H_i(\forall i\in I)$, 于是 $ab^{-1}\in J$. 这就证明了 $\bigcap\limits_{i\in I}H_i$ 为 G 的子群.

(3) 由 H_2 是 G 的子群知 $ab^{-1}\in H_2,\forall a,b\in H_2$. 又 $H_2\subseteq H_1$, 故 H_2 也是 H_1 的子群.

(4) 充分性显然, 下证必要性. 设 $H\cup K$ 是 G 的子群. 如果 $H\subseteq K$, 则结论成立. 如果 $H\nsubseteq K$, 则存在 $h\in H$, 使 $h\notin K$. 由于 $H\cup K$ 为 G 的子群, 因此对任意的 $k\in K$, 有 $hk\in H\cup K$. 从而必有 $hk\in H$ 或 $hk\in K$. 如果 $hk\in K$, 则 $h=hk\cdot k^{-1}\in K$, 这与 h 的选取矛盾. 从而必有 $hk\in H$, 由此推出 $k=h^{-1}\cdot hk\in H$. 由 k 的任意性知 $K\subseteq H$. 这就证明了必要性.

设 H,K 是群 G 的两个子群. 如果 $G=H\cup K$, 由前面所证, 应有 $H\subseteq K$ 或 $K\subseteq H$, 于是有 $G=K$ 或 $G=H$. 这说明 H,K 不可能都是 G 的真子群. 因此群 G 不能被它的两个真子群所覆盖.

□

定义 1.12

1. 设 V 是数域 $\mathbb{P}$ 上的 n 维线性空间.S_V 为 V 上的全变换群, $GL(V)$ 表示 V 上所有可逆线性变换的集合, 则 $GL(V)$ 为 S_V 的子群, 称为线性空间 V 的**一般线性群**.
   又设 $SL(V)$ 为 V 上所有行列式等于 1 的线性变换的集合, 则 $SL(V)$ 是 $GL(V)$(同时也是 S_V) 的子群, 称为**特殊线性群**.
2. 设 V 是 n 维 Euclid 空间. 以 $O(V)$ 表示 V 上所有正交变换的集合, $SO(V)$ 表示所有行列式等于 1 的正交变换的集合, 则 $O(V)$ 是 $GL(V)$ 的子群, $SO(V)$ 是 $O(V)$ 的子群. $O(V)$ 称为 V 的**正交变换群**, 简称**正交群**, $SO(V)$ 称为**转动群** (或**特殊正交变换群、特殊正交群**).

♣

注 将上述 S_V 换成数域 $\mathbb{P}$ 上的全体方阵构成的乘法群, 线性变换换成方阵, 结论也成立.

证明

□

定义 1.13 (全变换群/置换群)

设 X 是非空集合. 以 S_X 表示 X 的所有可逆变换 (即 X 到 X 的一一对应) 的集合, 则 S_X 对变换的乘法构成一个群, id_X 为左幺元, f^{-1} 为 f 的左逆元. S_X 称 X 的**全变换群**.S_X 的子群称为 X 上的**变换群**.
如果集合 X 所含元素的个数 $|X|=n<+\infty$. 此时 S_X 记为 S_n, 称为 n 个文字的**对称群**或 n 个文字的**置换群**, 其元素称为**置换**.

♣

注 往后, 如果我们不加说明的话,S_n 就表示 $\{1,2,\cdots,n\}$ 的对称群.

定义 1.14

假定集合 $X=\{1,2,\cdots,n\}$, 记 S_n 为 X 的对称群, 设 $\sigma\in S_n$, 则 $\sigma(1),\sigma(2),\cdots,\sigma(n)$ 是 $1,2,\cdots,n$ 的一个排列. 常用下面记法:

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

更一般地, 若 $i_1,i_2,\cdots,i_n$ 是 $1,2,\cdots,n$ 的一个排列, 则可记

$$\sigma=\begin{pmatrix}i_1 & i_2 & \cdots & i_n\\ \sigma(i_1) & \sigma(i_2) & \cdots & \sigma(i_n)\end{pmatrix}$$

易知 S_n 中有 $n!$ 个元素, S_n 中一个元素可以有 $n!$ 种表示法.

例如, $\sigma\in S_3$, 满足 $\sigma(1)=2,\sigma(2)=3,\sigma(3)=1$, 则可记

$$\sigma=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}=\begin{pmatrix}1 & 3 & 2\\ 2 & 1 & 3\end{pmatrix}=\begin{pmatrix}2 & 1 & 3\\ 3 & 2 & 1\end{pmatrix}=\cdots$$

♣

定理 1.7

设 n 个不定元 $x_1,x_2,\cdots,x_n$ 的多项式

$$A=\prod_{1\leqslant i<j\leqslant n}(x_i-x_j)\in\mathbb{C}[x_1,x_2,\cdots,x_n].$$

记 S_n 为 $\{1,2,\cdots,n\}$ 的对称群, 对于 $\sigma\in S_n$, 令

$$A_\sigma=\prod_{1\leqslant i<j\leqslant n}(x_{\sigma(i)}-x_{\sigma(j)}),$$

则 $A_\sigma=\pm A$. 若 $A_\sigma=A$, 则称 σ 为**偶置换**, 并记 $\operatorname{sgn}\sigma=1$; 若 $A_\sigma=-A$, 则称 σ 为**奇置换**, 并记 $\operatorname{sgn}\sigma=-1$, $\operatorname{sgn}\sigma$ 称为 σ 的**符号**. 故有 sgn 是 S_n 到 $\{-1,1\}$ 的同态且

$$A_\sigma=\operatorname{sgn}\sigma A.$$

令 A_n 为 S_n 中偶置换集合, 即

$$A_n\triangleq\{\sigma\in S_n|\operatorname{sgn}\sigma=1\},$$

则 A_n 为 S_n 的子群.A_n 称为 n 个文字的**交错群**.

♡

证明 先证明 $A_\sigma=\pm A$. 注意到 A 中没有 x_i-x_j 的重因式, 因而只需说明 A_σ 中没有重因式即可. 设有 $\{\sigma(i),\sigma(j)\}=\{\sigma(k),\sigma(l)\}$, 则有如下两种可能:

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

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

因而都有 $\{i,j\}=\{k,l\}$, 由此知 $A_\sigma=\pm A$.

事实上, 若 $\tau,\sigma\in S_n$, 则有

$$A_{\sigma\tau}=\prod_{1\leqslant i<j\leqslant n}(x_{\sigma\tau(i)}-x_{\sigma\tau(j)}).$$

将 $A_{\sigma\tau}$ 与 A_σ 进行比较. 若 $\tau(i)<\tau(j)$, 则 $x_{\sigma\tau(i)}-x_{\sigma\tau(j)}$ 仍是 A_σ 中一个因子; 若 $\tau(i)>\tau(j)$, 则 $x_{\sigma\tau(j)}-x_{\sigma\tau(i)}=-(x_{\sigma\tau(i)}-x_{\sigma\tau(j)})$ 为 A_σ 中一因子, 因而将 A_σ 变成 $A_{\sigma\tau}$ 时改变因子符号的次数与将 A 变成 A_τ 时改变因子符号的次数相同, 因而有

$$A_{\sigma\tau}=\operatorname{sgn}\tau\cdot\prod_{1\leqslant i<j\leqslant n}(x_{\sigma(i)}-x_{\sigma(j)})=\operatorname{sgn}\sigma\operatorname{sgn}\tau A.$$

于是

$$\operatorname{sgn}(\sigma\tau)=\operatorname{sgn}\sigma\operatorname{sgn}\tau,\quad\forall\sigma,\tau\in S_n.$$

故 sgn 是 S_n 到 $\{-1,1\}$ 的同态. 又注意到 $\mathrm{sgn}\tau^{-1}=\mathrm{sgn}\tau, \forall \tau\in S_n$, 故

$$\mathrm{sgn}(\sigma\tau^{-1})=\mathrm{sgn}\sigma\mathrm{sgn}\tau^{-1}=\mathrm{sgn}\sigma\mathrm{sgn}\tau=1\Longrightarrow \sigma\tau^{-1}\in A_n,\quad \forall\sigma,\tau\in A_n.$$

由此知 A_n 为 S_n 的子群.

□

定义 1.15

设 H 是群 G 的子群, 又 $a\in G$. 集合 aH 与 Ha 分别称为以 a 为代表的 H 的**左陪集**与**右陪集**.

命题 1.9

设 H 是群 G 的子群, 又 $a,b\in G$, 则 aH, Ha, H, aHb 的阶都相同.

证明 设 $H=\{h_1,h_2,\cdots\}$, 则

$$aH=\{ah_1,ah_2,\cdots\},\quad Ha=\{h_1a,h_2a,\cdots\},\quad aHb=\{ah_1b,ah_2b,\cdots\},$$

故 aH, Ha, H 中所含元素的个数都相同, 即阶相同.

□

定理 1.8

设 H 是群 G 的子群, 则由

$$aRb,\ 若\ a^{-1}b\in H$$

所确定的 G 中的关系 R 是一个等价关系, 并且 a 所在的等价类为 $\{aH:a\in G\}$, 故 H 的左陪集族 $\{aH:a\in G\}$(集合无相同元素) 是 G 的一个分划.

证明 由 $a^{-1}a\in H$ 知 $aRa(\forall a\in G)$. 又设 aRb, 即 $a^{-1}b\in H$, 故 $(a^{-1}b)^{-1}=b^{-1}a\in H$, 即 bRa. 再设 aRb, cRb, 即 $a^{-1}b, b^{-1}c\in H$, 故 $a^{-1}c=(a^{-1}b)(b^{-1}c)\in H$, 即 aRc. 这样知 R 是等价关系. 又由 $b=a(a^{-1}b)$ 知

$$aRb\iff a^{-1}b\in H\iff b\in aH,$$

故 a 所在的等价类为 aH. 由定理 1.18知 $\{aH:a\in G\}$ 为 G 的一个分划.

□

推论 1.2

设 H 是群 G 的子群, 则下列条件等价:

(1) $aH\cap bH\neq\varnothing$;

(2) $aH=bH$;

(3) $a^{-1}b\in H$,

而且 $G=\bigcup\limits_{a\in G}aH$ 为不相交的并.

证明

□

定义 1.16

设 H 是群 G 的子群, 由定理 1.8定义 G 中的等价关系 R 为

$$aRb,\ 若\ a^{-1}b\in H.$$

将 G 对等价关系 R 的商集合, 即以左陪集 aH, $a\in G$ 为元素的集合记为 $G/H=\{aH:a\in G\}$, 称为 G 对 H 的**左陪集空间**. G/H 中元素个数 $|G/H|$ 称为 H 在 G 中的**指数**, 记为 $[G:H]$. 相应可定义**右陪集空间**.

注 $\{1\}$ 作为 G 的子群, 在 G 中指数显然为 $|G|$. 故也记 $|G|=[G:1]$.

例题 1.3 设 V 是数域 $\mathbb{P}$ 上的 n 维线性空间, $GL(V)$ 有子群 $SL(V)$. 在 V 中取定一组基, 任何一个线性变换由它在这组基下的矩阵完全确定, 可把它们等同起来.$\forall \lambda \in \mathbb{P}, \lambda \neq 0$, 令 $D(\lambda) = \mathrm{diag}(\lambda, 1, \cdots, 1)$, 于是 $D(\lambda) \in GL(V)$, 对于 $A \in GL(V)$ 有

$$ASL(V) = D(\lambda)SL(V) \iff \det A = \lambda.$$

于是

$$GL(V) = \bigcup_{\lambda \neq 0} D(\lambda)SL(V),$$

因而

$$[GL(V) : SL(V)] = +\infty.$$

证明

□

例题 1.4 设 V 是 n 维 Euclid 空间. 由 $A \in O(V)$ 有 $\det A = \pm 1$, 令 $D(\lambda) = \mathrm{diag}(\lambda, 1, \cdots, 1)$, 于是

$$O(V) = SO(V) \bigcup D(-1)SO(V), \quad [O(V) : SO(V)] = 2.$$

证明

□

例题 1.5 设 σ 是 S_n 中任一奇置换, 则有 $S_n = A_n \cup \sigma A_n$, 故 $[S_n : A_n] = 2$.

证明

□

定理 1.9 (Lagrange 定理)

设 H 是有限群 G 的子群, 记 1 为 G, H 的幺元, 则有

$$[G : 1] = [G : H][H : 1] \tag{1.3}$$

因而子群 H 的阶是群 G 的阶的因子.

♡

注 这个结论对无限群 G 也正确, 此时等式两边都是 $+\infty$.

证明 设 $a \in G$. 显然, 映射 $h \to ah$ 是 H 到 aH 上的一一对应, 因而 $|aH| = |H| = [H : 1]$. 又由推论 1.2知 $G = \bigcup_{a \in G} aH$ 为不相交的并, $\{aH : a \in G\}$ 的不同左陪集个数为 $[G : H]$, 故式 (1.3) 成立.

□

定理 1.10

设 H 是群 G 的子群, 则 G 中由

$$aRb, \text{ 若 } a^{-1}b \in H$$

所定义的关系 R 为同余关系的充分必要条件是

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

此时称 H 为 G 的**正规子群**, 记为 $H \lhd G$. 同时, 商集合 G/H 对同余关系 R 导出的运算

$$aH \cdot bH = abH, \quad \forall a, b \in G$$

也构成一个群, 称为 G 对 H 的**商群**. 商群 G/H 的幺元为 $1 \cdot H = H$. 为方便计, 常将商群 G/H 中元素记为 $\overline{g} = gH$. 有时也将商群 G/H 记作 $\dfrac{G}{H}$.

♡

证明 设 R 为同余关系. 又 $g \in G, h \in H$, 于是有

$$gRgh, \quad g^{-1}Rg^{-1},$$

因而 $gg^{-1}R(ghg^{-1})$, 即 $1Rghg^{-1}$, 亦即 $ghg^{-1} \in H$.

反之, 设 $\forall g \in G, h \in H$ 有 $ghg^{-1} \in H$. 设 aRb, cRd, 则 $a^{-1}b, c^{-1}d \in H$, 即 $\exists h_1, h_2 \in H$, 使 $b = ah_1, d = ch_2$, 从而 $c^{-1} = h_2 d^{-1}$. 因而 $(ac)^{-1}(bd) = c^{-1}a^{-1}ah_1 d = h_2\left(d^{-1}h_1 d\right) \in H$, 则有 $(ac)R(bd)$, 即 R 为同余关系.

设 R 为同余关系. 因 a 所在等价类为 aH, 由定理 1.20 知 G/H 中的乘法为

$$aH \cdot bH = abH, \quad \forall a, b \in G. \tag{1.4}$$

显然有 $(aH \cdot bH)cH = abcH = aH(bH \cdot cH)$, $1H \cdot aH = aH$, $a^{-1}H \cdot aH = 1 \cdot H$, 故 G/H 为群.

□

推论 1.3

(1) 若 G 为有限群, $H \lhd G$, 商群 G/H 的阶 $[G/H : H] = [G : H] = \dfrac{[G : 1]}{[H : 1]}$.

(2) 若 G 为无限群, $H \lhd G$, 商群 G/H 的阶 $[G/H : H] = [G : H]$.

♡

证明 这是Lagrange 定理的直接推论.

□

定理 1.11

设 H 是群 G 的子群, 则下列条件等价:

(1) $H \lhd G$;

(2) $gHg^{-1} = H, \forall g \in G$;

(3) $gH = Hg, \forall g \in G$;

(4) $g_1Hg_2H = g_1g_2H, \forall g_1, g_2 \in G$.

♡

证明 (1) $\Rightarrow$ (2). $g \in G, h \in H$, 则由 $H \lhd G$ 有 $ghg^{-1} \in H$, 又 $h = g(g^{-1}hg)g^{-1} \in gHg^{-1}$, 故有 $gHg^{-1} = H$.

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

(3) $\Rightarrow$ (4). 设 $g_1, g_2 \in G, h_1, h_2, h \in H$. 由条件 (3) 成立知 $\exists h_1', h' \in H$, 使 $h_1g_2 = g_2h_1'$, $g_2h = h'g_2$. 于是 $g_1h_1g_2h_2 = g_1g_2h_1'h_2 \in g_1g_2H$, $g_1g_2h = g_1h'g_2 \cdot 1 \in g_1H \cdot g_2H$, 故 $g_1H \cdot g_2H = g_1g_2H$.

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

□

命题 1.10

(1) Abel 群 G 的任一子群 H 都是正规子群, 商群 G/H 也是 Abel 群.

(2) 若 H 是群 G 的子群且 $H \supseteq N$, $N \lhd G$, 则 $N \lhd H$.

(3) 若 G 是一个群, 则 G 的任意正规子群的交 $\bigcap\limits_{H \lhd G} H$ 也是 G 的子群.

(4) 设 G 是一个群, 且 $N_1, N_2, \cdots, N_k \lhd G$, 则

$$N_1N_2 \cdots N_k \lhd G.$$

♠

证明

(1)

(2) 由命题 1.8(3)知 N 是 H 的子群. 又由 $N \lhd G$ 知

$$gng^{-1} \in H, \ \forall n \in N, \ g \in H \subseteq G.$$

故 $N \lhd H$.

(3)

(4) 由 $N_i \lhd G, i = 1, 2, \cdots, k$ 知

$$gn_ig^{-1} \in N_i, \quad \forall n_i \in N_i, g \in G.$$

于是对 $\forall n_1n_2\cdots n_k\in N_1N_2\cdots N_k, g\in G$, 有

$$g(n_1n_2\cdots n_k)g^{-1}=\left(gn_1g^{-1}\right)\left(gn_2g^{-1}\right)\cdots\left(gn_kg^{-1}\right)\in N_1N_2\cdots N_k.$$

故 $N_1N_2\cdots N_k\lhd G$.

□

例题 1.6 将商群 G/H 中元素记为 $\overline{g}=gH$, 则

(1) $SL(V)\lhd GL(V)$, $GL(V)/SL(V)=\{\overline{D(\lambda)}|\lambda\neq 0\}$ 且 $\overline{D(\lambda)D(\mu)}=\overline{D(\lambda\mu)}$;

(2) $SO(V)\lhd O(V)$, $O(V)/SO(V)=\{\overline{D(1)},\overline{D(-1)}\}$;

(3) $A_n\lhd S_n$, $S_n/A_n=\{\overline{1},\overline{\sigma}|\sigma$ 奇置换$\}$ 且

$$\overline{1}\cdot\overline{\sigma}=\overline{\sigma}\cdot\overline{1}=\overline{\sigma},\quad \overline{\sigma}\cdot\overline{\sigma}=\overline{1}\cdot\overline{1}=\overline{1}.$$

证明

□

定义 1.17 (极大正规子群)

设 G 是一个群,$H\lhd G$, 如果 H 满足以下两个条件:

(1) $H\subset G$, 即 $H\neq G$.

(2) 若 $K\lhd G$ 且 $H\subseteq K\subseteq G$, 则必有 $K=H$ 或 $K=G$.

则称 H 是 G 的**极大正规子群**.

♣

定义 1.18

若半群 S 的非空子集 S_1 对 S 的运算也是半群, 则称 S_1 为 S 的**子半群**.

若幺半群 M 的子集 Q 对 M 的运算也是幺半群且 M 的幺元 $1\in Q$, 则称 Q 为 M 的**子幺半群**.

♣

定理 1.12

如果关系 $\sim$ 是幺半群 (或半群)G 中的同余关系, 那么商集合 $G/\sim$ 对导出的运算 (见定理 1.20) 也是幺半群 (或半群), 称之为**商幺半群** (或**商半群**).

若 G 是交换幺半群 (或交换半群), 则商集合 $G/\sim$ 对导出的运算也是交换幺半群 (或交换半群).

♡

证明

□

1.4 环与域

定义 1.19 (环)

若在非空集合 R 中定义了加法和乘法两种二元运算, 并满足下列条件:

(1) R 对加法为 Abel 群;

(2) R 对乘法为半群;

(3) 加法与乘法间有分配律, 即 $\forall a,b,c\in R$,

$$a(b+c)=ab+ac,\quad (b+c)a=ba+ca,$$

则称 R 是一个**环**. 也记为 $(R,+,\cdot)$.

♣

命题 1.11

一切数域都是环.

♠

证明

□

例题 1.7

(1) $\mathbb{Z}$ 对加法与乘法是环, 称为**整数环**.

(2) 数域 P 上的 n 元多项式集合 $P[x_1, x_2, \cdots, x_n]$ 对多项式的加法和乘法是环, 称为 P 上的 $\boldsymbol{n}$ **元多项式环**.

(3) $R^{n\times n}$ 表示以环 R 中元素为矩阵元的 n 阶方阵的集合, 即 $\alpha \in R^{n\times n}$ 可写成

$$\alpha = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}, \quad a_{ij} \in R.$$

记 $a_{ij} = \mathrm{ent}_{ij}(\alpha)$. 由下面的两个关系:

(i) $\mathrm{ent}_{ij}(\alpha + \beta) = \mathrm{ent}_{ij}(\alpha) + \mathrm{ent}_{ij}(\beta)$;

(ii) $\mathrm{ent}_{ij}(\alpha\beta) = \sum_{k=1}^{n} \mathrm{ent}_{ik}(\alpha)\mathrm{ent}_{kj}(\beta)$

定义的 $R^{n\times n}$ 加法与乘法使其成为一个环, 称为 R 上的 $\boldsymbol{n}$ **阶方阵环**.

(4) 设 $C([a,b])$ 是闭区间 $[a,b]$ 上的连续函数的集合, 它对函数的加法与乘法是一个环, 称为 $[a,b]$ 上的**连续函数环**.

(5) 设 A 是一个 Abel 群, A 的运算是加法. 在 A 中定义乘法运算为 $ab = 0(\forall a, b \in A)$, 则 A 为一环, 这种环称为**零环**.

注 (5) 说明, 任何 Abel 群均可作为零环的加法群, 但是并非所有 Abel 群都可成为非零环的加法群.

证明

□

定理 1.13 (环的基本性质)

(1) 在环 R 中可定义任何整数的倍数及正整数次乘幂, 并且满足

(i) $\forall m, n \in \mathbb{Z}, a, b \in R$,

$$(m+n)a = ma + na,$$

$$(mn)a = m(na),$$

$$m(a+b) = ma + mb;$$

(ii) $a^m \cdot a^n = a^{m+n}, (a^m)^n = a^{mn}, \forall m, n \in \mathbb{N}, a \in R$;

(iii) 若 $a, b \in R$ 且 $ab = ba$, 则 $(ab)^m = a^m b^m, \forall m \in \mathbb{N}$.

(2) 由分配律成立有

$$\sum_{i=1}^{m}\sum_{j=1}^{n} a_i b_j = \sum_{j=1}^{n}\sum_{i=1}^{m} a_i b_j.$$

(3) $\forall a, b \in R$ 有 $a0 = 0a = 0, (-a)b = a(-b) = -ab, (-a)(-b) = ab$.

♡

证明

(1)

(2)

(3) 事实上, 由 $a \cdot 0 + ab = a(0+b) = ab$ 知 $a \cdot 0 = 0$. 同样 $0 \cdot a = 0, a(-b) = a(-b) + ab + (-ab) = -ab$. 最后 $(-a)(-b) = -(a(-b)) = -(-ab) = ab$.

□

定义 1.20

1. **交换环:** 乘法是交换半群的环.
2. **幺环:** 乘法是幺半群的环, 通常记幺元为 1.
3. **交换幺环:** 乘法是交换幺半群的环.
4. **无零因子环:** 任意两个非零元的积不为零的环.
5. 设 R 是环. $a,b\in R$ 且 $a\neq 0,b\neq 0$. 若 $ab=0$, 则称 a 是 R 的一个**左零因子**, b 是 R 的一个**右零因子**, 都简称为**零因子**. 有时为方便也将 0 称为零因子.
6. **整环:** 无零因子的幺环. 即若 $a,b\in\mathbb{R}\setminus\{0\}$, 则 $ab\neq 0$. 也即若 $a,b\in\mathbb{R}$ 且 $ab=0$, 则 $a=0$ 或 $b=0$.
7. **体:** 非零元素集合对乘法构成群的环, 即非零元素都可逆的幺环.
8. **域:** 交换的除环, 即非零元素集合对乘法为 Abel 群的环.

♣

注 当 $n>1$ 时, R 上的 n 阶方阵环 $R^{n\times n}$ 就不是无零因子环.

显然, 一切数域 P 都是域, 因而也是体.

定义 1.21

1. 设 R 是一个体, 若 R_1 对 R 中的加法和乘法也构成体且 $R_1\subseteq R$, 则称 R_1 是 R 的**子体**.
2. 设 R 是一个域, 若 R_1 对 R 中的加法和乘法也构成域且 $R_1\subseteq R$, 则称 R_1 是 R 的**子域**.

   若 R 是域 F 的子域, 则称 F 是 R 的**扩域**.

♣

定理 1.14

设 R 是一个环,S 是 R 的一个非空子集, 则 S 是 R 的子环的充分必要条件是满足下面任何一个条件:

(1) S 是 R 的加法子群; 且 S 关于 R 的乘法封闭, 即对 $\forall a,b\in S$, 有 $ab\in S$.

(2) 对 $\forall a,b\in S$, 有 $a-b\in S$; 且对 $\forall a,b\in S$, 有 $ab\in S$.

♡

注 这就是说, 环 R 的子环 S 是 R 的关于减法与乘法封闭的非空子集.

证明

(1) **必要性**: 因为 S 是环, 由环的定义知 S 是 R 的加法子群; 且 S 关于 R 的乘法封闭.

充分性: 设 S 是 R 的加法子群,S 关于 R 的乘法封闭, 则 S 对加法和乘法都封闭. 又因为 R 对加法构成 Abel 群, 对乘法构成半群, 乘法对加法满足分配律, 而 $S\subseteq R$, 且 S 的运算就是 R 的运算, 所以 S 也对加法构成 Abel 群, 对乘法构成半群, 乘法对加法满足分配律. 因此 S 是 R 的子环.

(2) 由定理 1.6(4)知 S 是 R 的加法子群的充要条件是对 $\forall a,b\in S$, 有 $a-b\in S$. 再由结论 (1) 知 (2) 就是 S 是 R 的子环的充要条件.

□

命题 1.12

(1) 体一定是整环, 进而域也一定是整环.

(2) 若 R 是一个体, 则 G 的任意子体的交也是 R 的子体.

(3) 若 R 是一个域, 则 G 的任意子体的交也是 R 的子域.

♠

证明

(1) 设 R 是一个体,$a,b\in\mathbb{R}$ 且 $ab=0$. 若 $a\neq 0$, 则 $b=a^{-1}(ab)=0$; 若 $b\neq 0$, 则 $a=(ab)b^{-1}=0$. 故 R 是整环.

(2)

(3)

□

命题 1.13

(1) 环 R 为整环的充要条件是 R 的非零元素集合 $R^* = R \setminus \{0\}$ 是乘法幺半群 R 的子幺半群.

(2) 若 R 是交换整环, 则 $R^* = R \setminus \{0\}$ 对乘法构成交换幺半群且消去律成立, 即

$$ax = bx \ (\text{或} xa = xb), \ \text{则} a = b, \ \forall a, b, x \in R^*$$

(3) 若 R 是整环且 $\prod_{i=1}^{k} a_i = 0, a_i \in R$, 则存在 $i_0 \in [1, k] \cap \mathbb{N}$, 使 $a_{i_0} = 0$.

♠

证明

(1)

(2) 因为 R 是交换整环且 $R^* \subseteq R$, 所以 R 对乘法构成交换幺半群. 设 $a, b, x \in R^*$ 且 $ax = bx$, 则 $(a - b)x = 0$. 由于 R 是整环且 $x \neq 0$, 故 $a - b = 0$, 即 $a = b$.$xa = xb$ 的情况同理可证.

(3) 由整环定义易得.

□

命题 1.14

设 p 是一个素数, 则 $\mathbb{Z}_p = \{0, 1, \cdots, \overline{p-1}\}$ 是只含 p 个元素的域且非数域.

♠

证明 由 p 是一个素数易知 $\mathbb{Z}$ 中关系 $a \equiv b (\mathrm{mod}\ p)$ 对加法及乘法都是同余关系, 因而在 $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ 中有加法运算, 使 $\mathbb{Z}_p$ 为 Abel 群, 而且在 $\mathbb{Z}_p$ 中有乘法运算, 使 $\mathbb{Z}_p$ 为交换幺半群. $\mathbb{Z}_p = \{0, 1, \cdots, \overline{p-1}\}$. 又 $\forall \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_p$ 有

$$\overline{a}(\overline{b} + \overline{c}) = \overline{a(b + c)} = \overline{ab + ac} = \overline{ab} + \overline{ac} = \overline{ab} + \overline{ac},$$

即分配律成立. 故 $\mathbb{Z}_p$ 是交换幺环. 又对 $a \in \mathbb{N}, a < p$, 由 p 为素数知有 $m, n \in \mathbb{Z}$, 使 $ma + np = 1$, 因而 $\overline{m} \cdot \overline{a} = \overline{1}$, 即 $\mathbb{Z}_p$ 中每个非零元素可逆, 因而 $\mathbb{Z}_p$ 是只含 p 个元素的域且非数域.

□

定理 1.15

设 $\mathbb{C}$ 为复数域. 考虑 $\mathbb{C}^{2\times 2}$ 中子集

$$H = \left\{ \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \middle| \alpha, \beta \in \mathbb{C} \right\}.$$

证明 H 是体, 称 H 为 $\mathbb{R}$ 上的**四元数体**.

♡

证明 容易验证 H 对矩阵的加法为 Abel 群. 又对 $\forall \alpha, \beta, \gamma, \delta \in \mathbb{C}$ 有

$$\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \begin{pmatrix} \gamma & \delta \\ -\overline{\delta} & \overline{\gamma} \end{pmatrix} = \begin{pmatrix} \alpha\gamma - \beta\overline{\delta} & \alpha\delta + \beta\overline{\gamma} \\ -\overline{\alpha}\overline{\delta} - \overline{\beta}\gamma & \overline{\alpha}\overline{\gamma} - \overline{\beta}\delta \end{pmatrix} \in H,$$

故 H 对矩阵乘法为幺半群. 显然加法与乘法间有分配律, 故 H 为幺环. 又若

$$\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \neq 0,$$

则

$$\begin{vmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{vmatrix} = \alpha\overline{\alpha} + \beta\overline{\beta} > 0.$$

此时有

$$\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}^{-1} = (\alpha\overline{\alpha} + \beta\overline{\beta})^{-1} \begin{pmatrix} \overline{\alpha} & -\beta \\ \overline{\beta} & \alpha \end{pmatrix} \in H,$$

即 $H^* = H \setminus \{0\}$ 为群, 因而 H 是体. 又 H 中有元素

$$\boldsymbol{A} = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \quad \boldsymbol{B} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

由 $\boldsymbol{AB} \neq \boldsymbol{BA}$, 故 H 是体, 但不是域.

□

命题 1.15

设 $\mathbf{H}$ 为四元数体, 令

$$\mathbf{i} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{i} = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix},$$
$$\mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{k} = \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}.$$

则

$$\mathbf{i} \cdot \mathbf{j} = \mathbf{k}, \quad \mathbf{i} \cdot \mathbf{k} = -\mathbf{j},$$
$$\mathbf{j} \cdot \mathbf{i} = -\mathbf{k}, \quad \mathbf{j} \cdot \mathbf{k} = \mathbf{i},$$
$$\mathbf{k} \cdot \mathbf{i} = \mathbf{j}, \quad \mathbf{k} \cdot \mathbf{j} = -\mathbf{i},$$
$$\mathbf{i}^2 = \mathbf{i}, \quad \mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{i},$$
$$\mathbf{i} \cdot \mathbf{i} = \mathbf{i} \cdot \mathbf{i} = \mathbf{i}, \quad \mathbf{i} \cdot \mathbf{j} = \mathbf{j} \cdot \mathbf{i} = \mathbf{j}, \quad \mathbf{i} \cdot \mathbf{k} = \mathbf{k} \cdot \mathbf{i} = \mathbf{k}.$$

并且有下面结论:

(1) $\forall \alpha \in \mathbf{H}$, 存在唯一的一组 $(a, b, c, d) \in \mathbb{R}^{1\times 4}$, 使得 $\alpha = a\mathbf{i} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$. 进而

$$\mathbf{H} = \{a\mathbf{i} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in \mathbb{R}\}.$$

(2) $\mathbf{H}$ 的变换 σ:

$$\sigma(a\mathbf{i} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) = a\mathbf{i} - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$$

是 $\mathbf{H}$ 的一个对合.

♠

注 我们一般省略不写 $\mathbf{i}$, 即将 $a\mathbf{i}$ 简写成 a.

证明

(1) 根据定理 1.15,$\alpha \in \mathbf{H}$ 有 $a, b, c, d \in \mathbb{R}$, 使得

$$\alpha = \begin{pmatrix} a + b\sqrt{-1} & c + d\sqrt{-1} \\ -c + d\sqrt{-1} & a - b\sqrt{-1} \end{pmatrix} = a\mathbf{i} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}.$$

由

$$\begin{pmatrix} a + b\sqrt{-1} & c + d\sqrt{-1} \\ -c + d\sqrt{-1} & a - b\sqrt{-1} \end{pmatrix} = \begin{pmatrix} a_1 + b_1\sqrt{-1} & c_1 + d_1\sqrt{-1} \\ -c_1 + d_1\sqrt{-1} & a_1 - b_1\sqrt{-1} \end{pmatrix},$$

知当且仅当 $a_1 = a, b_1 = b, c_1 = c, d_1 = d$ 结论 (1) 成立.

(2) 再设 $\beta = a_1\mathbf{i} + b_1\mathbf{i} + c_1\mathbf{j} + d_1\mathbf{k}, a_1, b_1, c_1, d_1 \in \mathbb{R}$, 则

$$\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta), \quad \forall \alpha, \beta \in \mathbf{H}.$$

$$\begin{aligned}
\sigma(\alpha\beta) &= \sigma\left((a\mathbf{i} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})(a_1\mathbf{i} + b_1\mathbf{i} + c_1\mathbf{j} + d_1\mathbf{k})\right) \\
&= \sigma\left((aa_1 - bb_1 - cc_1 - dd_1)\mathbf{i} + (ab_1 + ba_1 + cd_1 - dc_1)\mathbf{i} + (ac_1 + ca_1 + db_1 - bd_1)\mathbf{j} + (ad_1 + da_1 + bc_1 - cb_1)\mathbf{k}\right) \\
&= (aa_1 - bb_1 - cc_1 - dd_1)\mathbf{i} - (ab_1 + ba_1 + cd_1 - dc_1)\mathbf{i} - (ac_1 + ca_1 + db_1 - bd_1)\mathbf{j} - (ad_1 + da_1 + bc_1 - cb_1)\mathbf{k} \\
&= (a_1\mathbf{i} - b_1\mathbf{i} - c_1\mathbf{j} - d_1\mathbf{k})(a\mathbf{i} - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}) = \sigma(\beta)\sigma(\alpha).
\end{aligned}$$

因此 σ 是 $\mathbf{H}$ 的反自同构. 又因

$$\sigma^2(\alpha)=\sigma(a\mathbf{i}-b\mathbf{i}-c\mathbf{j}-d\mathbf{k})=a\mathbf{i}+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}=\alpha,$$

故 σ 是对合.

□

定义 1.22

若环 R 的非空子集 R_1 对 R 的加法与乘法也构成环, 则称 R_1 为 R 的**子环**. 若 R_1 还满足 $RR_1\subseteq R_1$ (或 $R_1R\subseteq R_1$), 则称 R_1 为 R 的***左理想*** (或***右理想***). 若环 R 的非空子集 I 既是左理想又是右理想, 也即 $RR_1R\subseteq R_1$, 则称 I 为 R 的**双边理想**, 简称**理想**.

♣

注 $\{0\}$ 与 R 都是 R 的理想, 称为**平凡理想**. 在交换环中, 左理想、右理想与理想这三个概念是一致的.

定理 1.16

(1) 一个环中任意多个理想之交还是理想.

(2) 若 A 是环 R 的理想,B 是环 R 的子环且 $B\supseteq A$, 则 A 也是环 B 的理想.

(3) 若 A 是环 R 的非空子集, 则所有包含 A 的理想之交仍是一个包含 A 的理想, 称为**由 A 生成的理想**, 记为 $\langle A\rangle$.

♡

证明

(1)

(2)

(3)

□

定义 1.23

设 R 是一个环, 对于 $a\in R$, 我们定义 $\langle a\rangle=\langle\{a\}\rangle$ 为**由 a 生成的主理想**.

对于 $a_1,\cdots,a_n\in R$, 我们定义

$$\langle a_1,\cdots,a_n\rangle=\langle\{a_1,\cdots,a_n\}\rangle.$$

为**由 $a_1,a_2,\cdots,a_n$ 有限生成的理想**. 一般地, 若一个理想能被有限个元素生成, 我们就称其为**有限生成的理想**.

♣

定理 1.17

(1) 若 R 是幺环,$a,a_1,a_2,\cdots,a_n\in R$, 则

$$\langle a\rangle=RaR\triangleq\left\{\sum_{i=1}^{m}x_iay_i\mid m\in\mathbb{N},x_i,y_i\in R\right\},$$

$$\langle a_1,\cdots,a_n\rangle=Ra_1R+\cdots+Ra_nR=\left\{\sum_{i=1}^{n}s_i\mid s_i\in Ra_iR\right\}=\{\sum_{i=1}^{n}\sum_{j=1}^{m_i}x_{ij}a_iy_{ij}\mid m_i\in\mathbb{N},x_{ij},y_{ij}\in R\}.$$

进而显然有 $\langle 1\rangle=R$. 若还有 I 是 R 的理想且 $a_1,a_2,\cdots,a_n\in I$, 则显然有 $\langle a_1,a_2,\cdots,a_n\rangle\subseteq I$.

(2) 若 R 是交换幺环,$a,a_1,a_2,\cdots,a_n\in R$, 则

$$\langle a\rangle=aR=Ra=\{xa\mid x\in R\}=\{ax\mid x\in R\},$$

$$\langle a_1,\cdots,a_n\rangle=Ra_1+\cdots+Ra_n=a_1R+\cdots+a_nR=\{\sum_{i=1}^{n}r_ia_i\mid r_i\in R\}=\{\sum_{i=1}^{n}a_ir_i\mid r_i\in R\}.$$

再设 U 是 R 中所有可逆元素构成的集合, 则当且仅当 $u\in U$ 时, 有 $\langle u\rangle=uR=R$.

若还有 I 是 R 的理想且 $a_1,a_2,\cdots,a_n\in I$, 则显然有 $\langle a_1,a_2,\cdots,a_n\rangle\subseteq I$.

♡

证明

(1) 只须证明第二个等式. 设 $\sum\limits_{i=1}^{n}\sum\limits_{j=1}^{m_1}x_{ij}a_iy_{ij},\sum\limits_{i=1}^{n}\sum\limits_{j=1}^{m_2}r_{ij}a_is_{ij}\in Ra_1R+\cdots+Ra_nR$, 记 $x_{i,m_1+j}=-r_{ij},y_{i,m_1+j}=s_{ij}(i=1,2,\cdots,n;j=1,2,\cdots,m_2)$, 则

$$\begin{aligned}&\sum_{i=1}^{n}\sum_{j=1}^{m_1}x_{ij}a_iy_{ij}-\sum_{i=1}^{n}\sum_{j=1}^{m_2}r_{ij}a_is_{ij}=\sum_{i=1}^{n}\left(\sum_{j=1}^{m_1}x_{ij}a_iy_{ij}+\sum_{j=1}^{m_2}(-r_{ij})a_is_{ij}\right)\\&=\sum_{i=1}^{n}\left(\sum_{j=1}^{m_1}x_{ij}a_iy_{ij}+\sum_{j=1}^{m_2}x_{i,m_1+j}a_iy_{i,m_1+j}\right)\\&=\sum_{i=1}^{n}\sum_{j=1}^{m_1+m_2}x_{ij}a_iy_{ij}\in Ra_1R+\cdots+Ra_nR.\end{aligned}$$

故 $Ra_1R+\cdots+Ra_nR$ 对加法构成 R 的子群. 又因为 R 对加法构成 Abel 群, 所以 $Ra_1R+\cdots+Ra_nR$ 也对加法构成 Abel 群.

注意到

$$\left(\sum_{i=1}^{n}\sum_{j=1}^{m_1}x_{ij}a_iy_{ij}\right)\left(\sum_{k=1}^{n}\sum_{l=1}^{m_2}r_{kl}a_ks_{kl}\right)$$

的每一项都形如 $(x_{ij}a_iy_{ij}r_{kl})a_ks_{kl}\in Ra_kR$, 故

$$\left(\sum_{i=1}^{n}\sum_{j=1}^{m_1}x_{ij}a_iy_{ij}\right)\left(\sum_{k=1}^{n}\sum_{l=1}^{m_2}r_{kl}a_ks_{kl}\right)\in Ra_1R+\cdots+Ra_nR.$$

因为 R 对乘法满足结合律, 所以 $Ra_1R+\cdots+Ra_nR$ 对乘法也满足结合律. 故 $Ra_1R+\cdots+Ra_nR$ 对乘法构成半群. 因此 $Ra_1R+\cdots+Ra_nR$ 是 R 的子环.

对 $\forall r\in R$, 都有

$$\begin{aligned}&r\left(\sum_{i=1}^{n}\sum_{j=1}^{m_1}x_{ij}a_iy_{ij}\right)=\sum_{i=1}^{n}\sum_{j=1}^{m_1}(rx_{ij})a_iy_{ij}\in Ra_1R+\cdots+Ra_nR,\\&\left(\sum_{i=1}^{n}\sum_{j=1}^{m_1}x_{ij}a_iy_{ij}\right)r=\sum_{i=1}^{n}\sum_{j=1}^{m_1}x_{ij}a_i(y_{ij}r)\in Ra_1R+\cdots+Ra_nR,\end{aligned}$$

故 $R(Ra_1R+\cdots+Ra_nR)\subseteq Ra_1R+\cdots+Ra_nR,(Ra_1R+\cdots+Ra_nR)R\subseteq Ra_1R+\cdots+Ra_nR$, 因此 $Ra_1R+\cdots+Ra_nR$ 是 R 的理想, 且显然有 $Ra_1R+\cdots+Ra_nR\supseteq\{a_1,a_2,\cdots,a_n\}$. 故 $Ra_1R+\cdots+Ra_nR\supseteq\langle a_1,\cdots,a_n\rangle$.

又设 I 也是 R 的理想且包含 $a_1,\cdots,a_n$, 则由理想的定义和加法的封闭性知

$$I\supseteq Ra_1R+\cdots+Ra_nR.$$

故故 $Ra_1R+\cdots+Ra_nR\subseteq\langle a_1,\cdots,a_n\rangle$. 综上可得 $\langle a_1,\cdots,a_n\rangle=Ra_1R+\cdots+Ra_nR$.

(2) 只须证明第二个等式. 设 $r_1a_1+\cdots+r_na_n,s_1a_1+\cdots+s_na_n\in Ra_1+\cdots+Ra_n(r_i,s_i\in R)$, 我们有

$$(r_1a_1+\cdots+r_na_n)-(s_1a_1+\cdots+s_na_n)=(r_1-s_1)a_1+\cdots+(r_n-s_n)a_n\in Ra_1+\cdots+Ra_n.$$

因此 $Ra_1+\cdots+Ra_n$ 对加法构成子群. 又因为 R 对加法构成 Abel 群, 所以 $Ra_1+\cdots+Ra_n$ 对加法构成 Abel 群.

注意到

$$(r_1a_1+\cdots+r_na_n)(s_1a_1+\cdots+s_na_n)=\left(\sum_{i=1}^{n}r_ia_i\right)\left(\sum_{j=1}^{n}s_ja_j\right)$$

的每一项都形如 $\left(r_i a_i s_j\right) a_j \in R a_j$. 因此

$$(r_1a_1+\cdots+r_na_n)(s_1a_1+\cdots+s_na_n)=\left(\sum_{i=1}^{n} r_ia_i\right)\left(\sum_{j=1}^{n} s_ja_j\right)\in Ra_1+\cdots+Ra_n.$$

又因为 R 对乘法满足结合律, 所以 $Ra_1+\cdots+Ra_n$ 对乘法也满足结合律. 故 $Ra_1+\cdots+Ra_n$ 对乘法构成半群. 因此 $Ra_1+\cdots+Ra_n$ 是 R 的子环.

对 $\forall r\in R$, 由 R 是交换幺环可得

$$r\left(r_1a_1+\cdots+r_na_n\right)=\left(r_1a_1+\cdots+r_na_n\right)r=rr_1a_1+\cdots+rr_na_n\in Ra_1+\cdots+Ra_n,$$

故 $R(Ra_1+\cdots+Ra_n)\subseteq Ra_1+\cdots+Ra_n$,$(Ra_1+\cdots+Ra_n)R\subseteq Ra_1+\cdots+Ra_n$. 因此 $Ra_1+\cdots+Ra_n$ 是个理想, 而且显然包含 $a_1,\cdots,a_n$. 故 $Ra_1+\cdots+Ra_n\supseteq\langle a_1,\cdots,a_n\rangle$.

设 I 是一个包含了 $a_1,\cdots,a_n$ 的理想, 那么根据理想的定义和加法的封闭性, 有

$$I\supseteq Ra_1+\cdots+Ra_n.$$

故 $Ra_1+\cdots+Ra_n\subseteq\langle a_1,\cdots,a_n\rangle$. 综上可得 $\langle a_1,\cdots,a_n\rangle=Ra_1+\cdots+Ra_n$.

若 $u\in U$, 设 $r\in R$, 则 $r=u(u^{-1}r)\in uR$, 故 $R\subseteq uR$. 又显然有 $uR\subseteq R$, 故 $uR=R$.

若 $uR=R$, 则由 $1\in R$ 知存在 $r\in R$, 使 $ur=1$, 又 R 可交换, 故 $r=u^{-1}$, 即 $u\in U$.

□

定理 1.18

设 I 为环 R 的子环. 在 R 中定义关系“$\sim$”,

$$a\sim b,\ \ a+(-b)=a-b\in I,$$

则关系“$\sim$”对加法为同余关系.a 所在的等价类为 $a+I$. 关系“$\sim$”对乘法也为同余关系的充分必要条件是 I 为 R 的理想.

若 I 为理想, 则将 R 对等价关系 I 的商集合记为 $R/\sim=R/I$, 并且 $R/\sim=R/I$ 中可定义加法、乘法为

$$(a+I)+(b+I)=(a+b)+I,\quad \forall a,b\in R, \tag{1.5}$$

$$(a+I)\cdot(b+I)=ab+I,\quad \forall a,b\in R. \tag{1.6}$$

R/I 对这种加法与乘法也构成环, 称为 R 对 I 的**商环**.

♡

证明 因 R 对加法为 Abel 群, 故 R 的加法子群 I 为正规子群. 由定理 1.10 知“$\sim$”对 R 的加法为同余关系, 再由命题 1.10知在 R/I 中有加法运算 (1.5) 且为 Abel 群.

现设“$\sim$”对乘法也是同余关系. 对 $\forall a\in I,b\in R$ 有 $a\sim 0,b\sim b$, 因而 $ab\sim 0,ba\sim 0$, 故 $ab,ba\in I$, 因而 I 为 R 的理想.

反之, 设 I 是 R 的理想, $a,b,c,d\in R$ 且 $a\sim b,c\sim d$, 即 $a-b,c-d\in I$. 此时有 $ac-bd=ac-ad+ad-bd=a(c-d)+(a-b)d\in I$, 即 $ac\sim bd$, 故“$\sim$”对乘法也是同余关系.

当 I 为理想时, 在 R/I 中可定义乘法如式 (1.6) 且对 $\forall a,b,c\in R$ 有

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

并且

$$\begin{aligned}((a+I)+(b+I))(c+I)&=((a+b)+I)(c+I)=(a+b)c+I\\&=(ac+bc)+I=(ac+I)+(bc+I)\\&=(a+I)(c+I)+(b+I)(c+I).\end{aligned}$$

类似有

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

即 R/I 为半群, 且对加法乘法的分配律成立. 故 R/I 是一个环.

□

推论 1.4

若 R 为交换环, 则 R/I 也是交换环.

♡

证明

□

推论 1.5

若 R 为幺环, 则 R/I 也是幺环且 $1+I$ 为幺元.

♡

证明

□

例题 1.8 从定理 1.18知 $m\mathbb{Z}$ 为 $\mathbb{Z}$ 的理想, 故 $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ 对剩余类 $(\mathrm{mod}\ m)$ 的加法与乘法是一个环.

当 p 为素数时, $\mathbb{Z}_p$ 为域.

若 m 是合数, 即 $m = m_1m_2(m_i \in \mathbb{Z}, |m_i| > 1, i = 1, 2)$, 则 $\mathbb{Z}_m$ 有零因子 $\overline{m_1}, \overline{m_2}$.

例题 1.9 设 R 是一个环. 考虑 $R^{n\times n}$ 中子集

$$A = \{\alpha \mid \alpha \in R^{n\times n}, j \neq 1 \text{ 时}, \mathrm{col}_j\alpha = 0\},$$

$$B = \{\alpha \mid \alpha \in R^{n\times n}, i \neq 1 \text{ 时}, \mathrm{row}_i\alpha = 0\},$$

则 A, B 分别为 $R^{n\times n}$ 的左理想与右理想. 当 $n \geqslant 2$ 时, 一般来说, A, B 都不是双边理想.

1.5 同态与同构

定义 1.24

设 G_1, G_2 是两个群 (或半群、幺半群), f 是 G_1 到 G_2 的映射. 如果 f 满足

$$f(xy) = f(x)f(y), \quad \forall x, y \in G_1,$$

则称 f 是 G_1 到 G_2 的一个**同态**.

若 f 还是满映射, 则称 f 为**满同态**, 或 G_1 到 G_2 上的同态, 这时也称 G_1 与 G_2 同态.

若 f 还是一一对应, 则称 f 为**同构**, 这时也称 G_1 与 G_2 同构, 记为 $G_1 \cong G_2$.

♣

定理 1.19

1. 设 H 是群 G 的正规子群. 记 G 到商群 G/H 的自然映射为

$$\pi : \pi(g) = gH, \quad \forall g \in G,$$

则 π 为 G 到 G/H 上的同态, 称 π 为**自然同态**.

2. 若 G 是一个半群 (或幺半群). “$\sim$” 是 G 中一个同余关系, 则 G 到商半群 (或商幺半群) $G/\sim$ 的自然映射 π 是同态, 也称**自然同态**.

♡

注 显然自然同态都是满同态.

证明

1.

2.

□

命题 1.16

设 N 是群 G 的子群, 记 G 到商集 G/N 的自然映射为 π, 则

(1) 若 H 是 G 的子群且 $H \supseteq N$, 则 $\pi(H) = H/N$.

♠

证明

(1) 由命题 1.8(3)知 N 也是 H 的子群, 故

$$H/N = \{hN : h \in H\} = \pi(H).$$

□

例题 1.10

(1) 容易看出 $\{1,-1\}$ 对乘法构成一个 2 阶群. 定义 S_n 到 $\{1,-1\}$ 的映射 $f : f(\sigma) = \mathrm{sgn}\sigma(\forall \sigma \in S_n)$, 则 f 为满同态.

(2) 设 V 是数域 P 上 n 维线性空间. $GL(V)$ 到 $P^* = P \setminus \{0\}$ 的映射

$$f : f(A) = \det A, \quad \forall A \in GL(V)$$

是 $GL(V)$ 到 P^* 上的同态.

(3) 设 exp 为实数加法群 $\mathbb{R}$ 到正实数乘法群 $\mathbb{R}^+ = \{x \in \mathbb{R} | x > 0\}$ 的映射,

$$\exp : \exp(x) = \mathrm{e}^x, \quad \forall x \in \mathbb{R},$$

其中, e 为自然对数的底, 则 exp 是同构.

(4) 设 V 是数域 P 上的 n 维线性空间, $GL(V)$ 是 V 上一般线性群, $GL(n,P)$ 是 P 上所有 n 阶可逆方阵的集合, 则 $GL(n,P)$ 对矩阵乘法构成群且 $GL(V) \cong GL(n,P)$.

类似地, 有

$$SL(V) \cong SL(n,P) = \{A \in GL(n,P) | \det A = 1\}.$$

又若 V 为 n 维 Euclid 空间, 则

$$O(V) \cong O(n,\mathbb{R}) = \{A \in GL(n,\mathbb{R}) | AA' = I_n\},$$

其中, A' 为 A 的转置, I_n 为 n 阶单位矩阵. 还有

$$SO(V) \cong SO(n,\mathbb{R}) = \{A \in O(n,\mathbb{R}) | \det A = 1\}.$$

证明

1.
2.
3.
4.
5.
6. 事实上, 在 V 中取定一组基 $\alpha_1, \alpha_2, \cdots, \alpha_n$, 简记为 $\{\alpha\}$. 对 $\forall A \in GL(V)$, A 在 $\{\alpha\}$ 下的矩阵 $M(A)$ 是唯一确定的. 反之, 对任一 $A \in P^{n\times n}$ 存在唯一的线性变换 A 满足 $M(A) = A$, 而且 $A \in GL(V)$ 当且仅当 $M(A) \in GL(n,P)$, 因而 $A \to M(A)$ 是 $GL(V)$ 到 $GL(n,P)$ 的一一对应, 又由

$$M(AB) = M(A)M(B), \quad \forall A, B \in GL(V)$$

知 $GL(V) \cong GL(n,P)$.

□

定理 1.20 (群同态与同构的基本性质)

(1) 若 f 是群 G_1 到群 G_2 的同态, g 是群 G_2 到群 G_3 的同态, 则

(i) gf 是 G_1 到 G_3 的同态 (图 1.1);

(ii) 若 f,g 都是满同态, 则 gf 也是满同态;

(iii) 若 f,g 都是同构, 则 gf 也是同构.

(2) 设 f 是群 G_1 到群 G_2 的同态, e_1,e_2 分别为 G_1,G_2 的幺元, 则

$$f(e_1)=e_2,\quad f(a^{-1})=f(a)^{-1},\quad \forall a\in G_1.$$

(3) 设 f 是群 G_1 到群 G_2 的同态, 则 $f(G_1)$ 是 G_2 的子群, 因而 f 可看成 G_1 到 $f(G_1)$ 上的同态.

(4) 群的同构关系是一个等价关系, 即对任何群 G 有 $G\cong G$; 若 $G_1\cong G_2$, 则 $G_2\cong G_1$; 若 $G_1\cong G_2, G_2\cong G_3$, 则 $G_1\cong G_3$.

♡

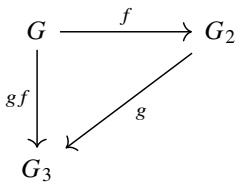

图 1.1

证明

(1) 事实上, $\forall a,b\in G_1$ 有 $gf(a),gf(b)\in G_3$ 且

$$gf(ab)=g(f(ab))=g(f(a)f(b))=gf(a)gf(b).$$

故 gf 为 G_1 到 G_3 的同态. 又由 $f(G_1)=G_2, g(G_2)=G_3$, 即得 $gf(G_1)=G_3$. 又由 g,f 为一一对应, 则 gf 也是一一对应.

(2) 事实上, $f(e_1)=f(e_1^2)=f(e_1)f(e_1)$, 故有

$$f(e_1)=f(e_1)f(e_1)^{-1}=e_2.$$

又 $a\in G_1$ 有 $f(e_1)=f(aa^{-1})=f(a)f(a^{-1})$, 故

$$f(a^{-1})=f(a)^{-1}f(e_1)=f(a)^{-1}.$$

(3) 事实上, 由性质 (2) 知 $e_2=f(e_1)\in f(G_1)$, 又 $f(a),f(b)\in f(G_1)$ 有 $f(a)f(b)^{-1}=f(ab^{-1})\in f(G_1)$, 故 $f(G_1)$ 是 G_2 的子群.

(4) 对任何群 G 有 $G\cong G$ (只要取 $f=\mathrm{id}_G$); 若 $G_1\cong G_2$, 则 $G_2\cong G_1$ (若 $f:G_1\to G_2$ 为同构映射, 则 $f^{-1}:G_2\to G_1$ 也是同构映射); 若 $G_1\cong G_2, G_2\cong G_3$, 则 $G_1\cong G_3$ (参见性质 (1)).

□

定义 1.25

设 G 是群. 对于 $a\in G$, 可定义 G 的两个变换 L_a,R_a 如下:

$$L_a(x)=ax,\quad R_a(x)=xa,\quad \forall x\in G.$$

L_a,R_a 分别称为由 a 决定的**左平移**与**右平移**. 定义

$$L_G\triangleq\{L_a|a\in G\},\quad R_G\triangleq\{R_a|a\in G\}.$$

♣

命题 1.17

G 上由 a 决定的左平移, 右平移 L_a,R_a 都是 G 的一一对应, 即为 S_G 中元素且有

$$L_aL_b=L_{ab},\quad R_aR_b=R_{ba},\quad L_1=R_1=\mathrm{id}_G,$$
$$L_{a^{-1}}=L_a^{-1},\quad R_{a^{-1}}=R_a^{-1},\quad L_aR_b=R_bL_a,\quad \forall a,b\in G,$$

1 为 G 的幺元. 从这些等式可知 $L_G = \{L_a | a \in G\}$ 与 $R_G = \{R_a | a \in G\}$ 都是 S_G 的子群. ♠

证明

□

定理 1.21 (Cayley 定理)

设 G 是一个群, 则

$$G \cong L_G \cong R_G.$$

♡

注 左平移与右平移的概念对半群与幺半群也是适用的. 但应注意, 此时左右平移不一定是一一对应.Cayley 定理对半群是不成立的, 但对幺半群 G 仍有 $G \cong L_G$, 这时 L_G 是 $M(G)$ 的子幺半群 ($M(G)$ 的定义见例题 1.1).

证明 记 G 到 L_G 的映射 $L : L(a) = L_a$. 显然 L 是满映射. 又若 $L(a) = L(b)$, 即 $L_a = L_b$, 则有 $a = a \cdot 1 = L_a(1) = L_b(1) = b$, 因而 L 还是一一映射, 故 L 为一一对应. 又对 $\forall a, b \in G$ 有

$$L(ab) = L_{ab} = L_a L_b = L(a)L(b),$$

故 L 是 G 到 L_G 上的同构, 即 $G \cong L_G$.

类似地, 不难验证, 由 $R'(a) = R_{a^{-1}}$ 确定的 G 到 R_G 的映射 R' 也是一个同构, 即有 $G \cong L_G \cong R_G$.

□

定义 1.26

群 G 到自身的同构称为 G 的**自同构**, 群 G 的自同构的集合记为 $\mathrm{Aut}G$. ♣

定理 1.22

设 G 是一个群, 则有

(1) $\mathrm{Aut}G$ 对变换的乘法也是一个群, 称为 G 的**自同构群**;

(2) $\forall g \in G$, G 的变换 $\mathrm{ad}g = L_g R_{g^{-1}}$, 即 $\mathrm{ad}g(x) = gxg^{-1} (\forall g \in G)$ 是 G 的一个自同构, 称为由 g 决定的**内自同构**;

(3) G 的内自同构的集合 $\mathrm{Int}G$ (也记成 $\mathrm{ad}G$ 或 $\mathrm{Inn}(G)$) 是 $\mathrm{Aut}G$ 的正规子群, 称为 G 的**内自同构群**;

(4) $\mathrm{ad} : g \to \mathrm{ad}g$ 是群 G 到 $\mathrm{Int}G$ 上的同态.

(5) 若 $C(G) = \{1\}$, 则 $\mathrm{ad} : g \to \mathrm{ad}g$ 是群 G 到 $\mathrm{Int}G$ 上的同构, 即 $G \cong \mathrm{Int}G$.

♡

证明

(1) 显然有 $\mathrm{id}_G \in \mathrm{Aut}G \subseteq S_G$, 任取 $\theta_1, \theta_2 \in \mathrm{Aut}G$, 于是 $\theta_1\theta_2^{-1} \in S_G$ 且对 $\forall x, y \in G$,

$$\begin{aligned}\theta_1\theta_2^{-1}(xy) &= \theta_1(\theta_2^{-1}(xy)) = \theta_1(\theta_2^{-1}(\theta_2\theta_2^{-1}(x) \cdot \theta_2\theta_2^{-1}(y))) \\ &= \theta_1(\theta_2^{-1}\theta_2(\theta_2^{-1}(x)\theta_2^{-1}(y))) = \theta_1(\theta_2^{-1}(x)\theta_2^{-1}(y)) \\ &= \theta_1\theta_2^{-1}(x) \cdot \theta_1\theta_2^{-1}(y),\end{aligned}$$

即有 $\theta_1\theta_2^{-1} \in \mathrm{Aut}G$. 故 $\mathrm{Aut}G$ 是群.

(2) 对 $\forall g \in G$ 有 $L_g, R_{g^{-1}} \in S_G$, 因而 $\mathrm{ad}g = L_g R_{g^{-1}} \in S_G$, 又对 $\forall x, y \in G$, 有

$$\mathrm{ad}g(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = \mathrm{ad}g(x) \cdot \mathrm{ad}g(y).$$

故 $\mathrm{ad}g \in \mathrm{Aut}G$, 即 $\mathrm{ad}g$ 是 G 的自同构.

(3) 对 $\forall g_1, g_2 \in G$, 有

$$\begin{aligned}(\mathrm{ad}g_1)(\mathrm{ad}g_2)^{-1} &= L_{g_1}R_{g_1^{-1}}(L_{g_2}R_{g_2^{-1}})^{-1} \\ &= L_{g_1}R_{g_1^{-1}}R_{g_2}L_{g_2^{-1}} = L_{g_1}L_{g_2^{-1}}R_{g_1^{-1}}R_{g_2} \\ &= L_{(g_1g_2^{-1})}R_{(g_2g_1^{-1})} = \mathrm{ad}g_1g_2^{-1}.\end{aligned} \tag{1.7}$$

故 $\mathrm{Int}G$ 是 $\mathrm{Aut}G$ 的子群.

又对 $\forall g, a \in G, \forall \theta \in \mathrm{Aut}G$,

$$\theta(\mathrm{ad}g)\theta^{-1}(a) = \theta(g\theta^{-1}(a)g^{-1}) = \theta(g)a\theta(g)^{-1} = \mathrm{ad}\theta(g)(a),$$

因而

$$\theta(\mathrm{ad}g)\theta^{-1} = \mathrm{ad}\theta(g), \quad \forall g \in G, \theta \in \mathrm{Aut}G.$$

由此知 $\mathrm{Int}G$ 是 $\mathrm{Aut}G$ 的正规子群.

(4) 在式 (1.7) 中, 取 $g_1 = 1$, 则有

$$(\mathrm{ad}g_2)^{-1} = \mathrm{ad}g_2^{-1}.$$

一般由式 (1.7) 知

$$\mathrm{ad}g_1 \cdot \mathrm{ad}g_2 = (\mathrm{ad}g_1)(\mathrm{ad}g_2)^{-1})^{-1} = \mathrm{ad}g_1(g_2^{-1})^{-1} = \mathrm{ad}g_1g_2.$$

由此知 $\mathrm{ad} : G \to \mathrm{Int}G$ 为 G 到 $\mathrm{Int}G$ 上的同态映射.

(5) 由定理 1.22(4)可知 ad 是 G 到 $\mathrm{Int}G$ 的同态. 显然 ad 是满射.

设 $x, y \in G$, 若 $\mathrm{ad}(x) = \mathrm{ad}(y)$, 即 $\mathrm{ad}x = \mathrm{ad}y$, 则对 $\forall g \in G$, 有

$$xgx^{-1} = ygy^{-1} \Longleftrightarrow \left(y^{-1}x\right) g \left(x^{-1}y\right) = g \Longleftrightarrow \left(y^{-1}x\right) g \left(y^{-1}x\right)^{-1} = g.$$

故 $y^{-1}x \in C(G)$. 又 $C(G) = \{1\}$, 故 $y^{-1}x = 1$, 进而 $x = y$. 因此 ad 为单射. 故 ad 是 G 到 $\mathrm{Int}G$ 的同构.

□

定义 1.27

设 G 是一个群, $\mathrm{Aut}G, \mathrm{Int}G$ 分别为 G 的自同构群与内自同构群, 称商群 $\mathrm{Aut}G/\mathrm{Int}G$ 为 G 的**外自同构群**.

定义 1.28

设 R, R_1 是两个环, φ 是 R 到 R_1 的映射, 如果对 $\forall a, b \in R$,

$$\varphi(a+b) = \varphi(a) + \varphi(b),$$

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

那么称 φ 是 R 到 R_1 的一个**同态**.

若 φ 是满映射, 则称 φ 为**满同态**, 或称 φ 为 R 到 R_1 上的同态.

若 φ 还是一一对应, 则称 φ 为**同构**. 这时也称 R 与 R_1 同构, 记为 $R \cong R_1$.

命题 1.18

(1) 若 φ 是 R 到 R' 的同态, 则 $\varphi(R)$ 是 R' 的子环. 进而若 R_1 是 R 的子环, 则 $\varphi(R_1)$ 也是 R' 的子环.

(2) 环的同态的积还是环同态.

(3) 环的同构关系是等价关系, 即 $R \cong R; R \cong R_1 \Rightarrow R_1 \cong R; R_1 \cong R_2, R_2 \cong R_3 \Rightarrow R_1 \cong R_3$.

证明

(1) 注意到 $\varphi|_{R_1}$ 是 $R_1 \to R'$ 的环同态, 故由前面的结论知 $\varphi(R_1)$ 也是 R' 的子环.

(2)

(3)

□

定理 1.23

1. 设 R, R_1 是两个环. 定义 R 到 R_1 的映射 $\varphi : \varphi(x) = 0 (\forall x \in R)$, 则 φ 为 R 到 R_1 的同态, 这样的同态称为**零同态**.

2. 设 I 是环 R 的一个理想. R 到商环 R/I 的自然映射 $\pi:\pi(x)=x+I(\forall x\in R)$ 是 R 到 R/I 上的同态, 称为**自然同态**.

证明

1.

2.

□

命题 1.19

设 A 是环 R 的子环, 记 R 到商集 R/A 的自然映射为 π, 则

(1) 若 B 是环 R 的子环且 $B\supseteq A$, 则 $\pi(B)=B/A$.

证明

(1)

□

例题 1.11 设 V 是数域 P 上 n 维线性空间, 用 End$V$ 表示 V 上线性变换的集合, 显然, End$V$ 对线性变换的加法与乘法构成一环, 设 $\{\alpha\}=\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$ 是 V 的一组基, 则映射

$$\mathcal{A}\to M(\mathcal{A}),\quad \forall\mathcal{A}\in \mathrm{End}V$$

是 End$V$ 到 $P^{n\times n}$ 上的同构. 这里 $M(\mathcal{A})$ 表示线性变换基 $\{\alpha\}$ 下的矩阵.

证明

□

定义 1.29

设 R,R' 是两个环, 若 R 到 R' 的映射 φ, 对 $\forall a,b\in R$ 满足

$$\varphi(a+b)=\varphi(a)+\varphi(b),\quad \varphi(ab)=\varphi(b)\varphi(a),$$

则称 φ 是从 R 到 R' 的**反同态**. 又若 φ 还是一一对应, 则称 φ 为从 R 到 R' 的**反同构**.

一个环 R 到自身的反同构称为**反自同构**. 若环 R 的反自同构 η 满足 $\eta^2=\mathrm{id}_R$, 则称 η 为 R 的一个**对合**.

定理 1.24

对任一环 R, 一定有一个环 R' 与它反同构.

证明 事实上, 只需作一个与 R 一一对应的集合 R', 设映射 $x\to x'$ 为这个对应关系. 在 R' 中定义加法与乘法如下:

$$x'+y'=(x+y)',\quad x'y'=(yx)',\quad \forall x',y'\in R',$$

则 R' 成环且与 R 反同构.

□

例题 1.12 设 P 是一个数域, 在环 $P^{n\times n}$ 中定义映射 $\tau:A\to A'$, 则 τ 是 $P^{n\times n}$ 的对合.

证明

□

1.6 模

定义 1.30 (模)

设 R 是幺环, M 是 Abel 群, 其运算为加法. 若有 $R\times M$ 到 M 的映射: $(a,x)\to ax(a\in R,x\in M)$, 对 $\forall a,b\in R,x,y\in M$ 满足

(1) $a(x+y)=ax+ay$;

(2) $(a+b)x=ax+bx$;

(3) $(ab)x=a(bx)$;

(4) $1\cdot x=x$,

则称 M 为 R 上的一个**左模**, 或称 M 是**左 R 模**, ax 称为 a 与 x 的积, 相应地说, R 与 M 间有一个乘法.

类似地, 可定义**右 R 模**, 即有映射 $(x,a)\to xa(a\in R,x\in M)$, 对 $\forall a,b\in R,x,y\in M$ 满足

(1) $(x+y)a=xa+ya$;

(2) $x(a+b)=xa+xb$;

(3) $x(ab)=(xa)b$;

(4) $x\cdot 1=x$.

若 M 既是左 R 模, 又是右 R 模且满足

$$(ax)b=a(xb),\quad \forall a,b\in R,\ x\in M,$$

则称 M 是 **R 双模**, 或称 **R 模**.

♣

注 假设 R 交换环且 M 是左或右 R 模, 又对 $a\in R,x\in M$, 令 $xa=ax$, 则易证 M 是一个 R 模, 今后对于交换环 R 上的模都指这种意义下的模.

例题 1.13 数域 P 上的线性空间 V 就是一个 **P 模**. 一般地, 域 F 上的模都称为 F 上的**线性空间**.

证明

□

例题 1.14 设 R 是幺环, R 对加法是 Abel 群, 记为 R_+. 考虑 $R\times R_+$ 到 R_+ 的映射

$$(r,x)\to rx,\quad r\in R,x\in R_+$$

及 $R_+\times R$ 到 R_+ 的映射

$$(x,s)\to xs,\quad x\in R_+,s\in R,$$

使 R_+ 变成一个 R 模, 因而 R 可看成它自身上的模.

证明

□

例题 1.15 设 V 是数域 P 上的线性空间, $\mathcal{A}$ 是 V 的一个线性变换, 令 $R=P[\lambda]$ 为 P 上的一元多项式环, 则 $R\times V$ 到 V 的映射 $(f(\lambda),x)\to f(\mathcal{A})x, f(\lambda)\in R(x\in V)$, 使 V 成为一个左 R 模.

证明

□

例题 1.16 设 M 是一个 Abel 群, 运算为加法, 则 $\mathrm{End}M$ 为 M 的自同态环, 并且 $\mathrm{End}M\times M$ 到 M 的映射 $(\eta,x)\to\eta(x)(\eta\in\mathrm{End}M,x\in M)$, 使 M 成为一个左 $\mathrm{End}M$ 模.

证明

□

定理 1.25

设 M 是一个 R 模, 则

(1) $\forall a, a_i \in R, x, x_i \in M, 1 \leqslant i \leqslant n,$

$$a\left(\sum_{i=1}^{n} x_i\right) = \sum_{i=1}^{n} a x_i, \quad \left(\sum_{i=1}^{n} a_i\right) x = \sum_{i=1}^{n} a_i x.$$

(2) $\forall a \in R, x \in M,$

$$a0 = 0a = 0, \quad a(-x) = (-a)x = -ax.$$

♡

证明

(1)

(2)

□

定义 1.31

设 M 是一个 R 模, M 的子集 N 若满足

(1) N 是 M 的子群;

(2) $\forall a \in R, x \in N$ 有 $ax \in N$, 即对 $\forall x \in N$, 有 $Rx \subseteq N$

则称 N 为 M 的一个**子模**. 显然, $\{0\}$ 与 M 都是 M 的子模, 称为**平凡子模**.

♣

例题 1.17 设 V 是数域 P 上的线性空间, V 的子模即 V 的线性子空间. 一般域 F 上的线性空间的子模, 也称为 V 的线性子空间或子空间.

证明

□

例题 1.18 设 M 是一个 Abel 群, 其运算为加法. 映射

$$(m, x) \to mx, \quad m \in \mathbb{Z}, x \in M,$$

使 M 变成一个 $\boldsymbol{Z}$ **模**. 并且 M 的子集 N 为子模当且仅当 N 为 M 的子群.

证明

□

命题 1.20

设 R 是一个幺环, R 可看成左 R 模、右 R 模或 R 模. 又设 N 是 R 的子集, 则 N 是左 R 模 (或右 R 模、R 模) R 的子模当且仅当 N 是 R 的左理想 (或右理想、理想).

♠

证明

□

例题 1.19 设 V 是数域 P 上的线性空间, $\mathcal{A}$ 是 V 上的一个线性变换. 在定理 1.15中, 从 $\mathcal{A}$ 出发定义了 $P[\lambda]$ 模 V、V 的子集 V_1 是 $P[\lambda]$ 子模当且仅当 V_1 是 $\mathcal{A}$ 的不变子空间.

证明

□

定理 1.26

设 M 是一个 R 模, 则

(1) M 中任意多个子模之交仍为子模.

(2) M 中有限多个子模 $N_1, N_2, \cdots, N_r$ 之和

$$N_1 + N_2 + \cdots + N_r = \{x_1 + x_2 + \cdots + x_r | x_i \in N_i\}$$

仍为 M 的子模.

(3) 设 S 为 M 的子集, 则 M 中包含 S 的最小子模是所有包含 S 的子模之交, 称为**由 S 生成的子模**. 若

$S=\{y_1,y_2,\cdots,y_k\}$ 为有限集, 则 S 生成的子模为

$$Ry_1+Ry_2+\cdots+Ry_k=\left\{\sum_{i=1}^{k}a_iy_i\middle|a_i\in R\right\}.$$

特别地, 由一个元素 x 生成的子模 Rx 称为**循环子模**. 若 M 是由一个元素 x 生成, 即 $M=Rx$, 则称 M 为**循环模**.

♡

注 循环群就是循环 $\mathbb{Z}$ 模. 幺环 R 就是循环 R 模.

证明

(1)

(2)

(3)

□

定理 1.27

设 N 为 R 模 M 的子模.$\overline{M}=M/N$ 为 M 对 N 的商群, 定义 $R\times\overline{M}$ 到 $\overline{M}$ 的映射

$$(a,x+N)\longrightarrow ax+N,\quad \forall x\in M,a\in R,$$

则 $\overline{M}$ 为 R 模, 称为 M 对 N 的**商模**.

♡

证明 因为 N 为 M 的子模, 所以 N 为 Abel 群 M 的子群, 从而 $N\lhd M$. 因此商群 $\overline{M}$ 是良定义的.

先上述映射是单值的, 即 R 中元素 $\overline{M}$ 中元素所作乘法运算的合理性.

设 $x_1,x_2\in M$ 且 $x_1+N=x_2+N$, 于是 $x_1-x_2\in N$, 因而, 由 N 为子模有 $a(x_1-x_2)=ax_1-ax_2\in N$, 故 $ax_1+N=ax_2+N$, 即上面映射是单值的, 即是良定义的映射.

以下只要验证 R 模的 4 个定义条件. 这些验证不难.

□

定义 1.32

设 M,M' 为两个 R 模. 如果 M 到 M' 的映射 η 满足 $\forall a\in R,x,y\in M$ 有

(1) $\eta(x+y)=\eta(x)+\eta(y)$, 即 η 是群同态;

(2) $\eta(ax)=a\eta(x)$,

则称 η 为 M 到 M' 的一个**模同态**或 ***R* 同态**.

若 η 还是满映射, 则称 η 为**满同态**, 此时称 M 与 M' 同态.

η 若还是一一对应, 则称 η 为**模同构**或 ***R* 同构**, 此时称 M 与 M' 同构, 记为 $M\cong M'$.

♣

注 模同态的定义知**模同态必为群同态.**

命题 1.21

设 M,M' 是两个 Abel 群, η 是 M 到 M' 的群同态, 则 η 也是 $\mathbb{Z}$ 模 M 到 $\mathbb{Z}$ 模 M' 的模同态;

若 η 为群同构, 则 η 也是模同构.

♠

证明

□

定理 1.28

设 N 是 R 模 M 的子模, π 是 M 到商模 $\overline{M}=M/N$ 的自然映射, 即 $\pi(x)=x+N(\forall x\in M)$.

若已知 π 是群同态, 又对 $\forall a\in R,x\in M$ 有 $\pi(ax)=ax+N=a(x+N)=a\pi(x)$, 故 π 也是模同态, 称 π 是 M 到 M/N 上的**自然 (模) 同态**.

♡

证明

□

命题 1.22

设 N 是 R 模 M 的子模, 记 M 到商模 M/N 的自然映射为 π, 则

(1) 若 M_1 是模 M 的子模且 $M_1 \supseteq N$, 则 $\pi(M_1) = M_1/N$.

♠

证明

(1)

□

例题 1.20 假设 V 是域 F 上的线性空间. V 到自身的模同态 $\mathcal{A}$, 称为 V 的线性变换. 显然, 当 F 为数域时, $\mathcal{A}$ 就是线性代数中讲的线性空间的线性变换.

证明

□

定理 1.29

设 M 是一个 R 模,

(1) 设 η 是 M 到 M' 的 R 同态, 则 $\eta(M)$ 是 M' 的子模且 η 是 M 到 $\eta(M)$ 上的同态. 进而若 M_1 是 M 的子模, 则 $\eta(M_1)$ 也是 M' 的子模.

(2) 设 η 是 R 模 M 到 R 模 M' 的同态, η' 是 R 模 M' 到 R 模 M'' 的同态, 则 $\eta'\eta$ 是 M 到 M'' 的模同态 (图 1.2).

(3) R 模之间的同构关系是等价关系.

♡

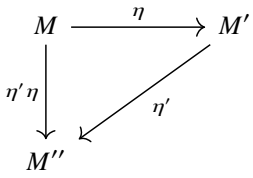

图 1.2

证明

(1) 后者注意到 $\eta|_{M_1}$ 是 $M_1 \to M'$ 上的模同态, 故由前面的结论知 $\eta(M_1)$ 也是 M' 的子模.

(2)

(3)

□

定义 1.33 (单模)

无非平凡子模的 R 模 M 称为**单模**.

♣

定理 1.30

R 模 M 为单模当且仅当对 $\forall x \in M, x \neq 0$ 有 $M = Rx$.

♡

证明 设 $x \in M, a, b \in R$, 于是 $ax - bx = (a-b)x \in Rx$, 故 Rx 是 M 的子群. 又 $aRx \subseteq Rx$. 因此 Rx 为 M 的子模, 显然 $x \neq 0$, 则 $Rx \neq 0$.

若 M 为单模, $x \in M$, $x \neq 0$. 于是 Rx 是 M 的非零子模, 因此 $M = Rx$.

反之, 设 $\forall x \in M, x \neq 0$ 有 $M = Rx$. 若 M_1 是 M 的非零子模. 于是有 $x \in M_1, x \neq 0$. 于是 $M = Rx \subseteq M_1 \subseteq M$, 故 $M_1 = M$, 即 M 为单模.

□

定义 1.34

一个 R 模 M 到自身的同态称为 M 的 R 自同态, 简称**自同态**. R 模 M 的 R 自同态的集合记为 $\mathrm{End}_R M$. 以 $\mathrm{End}M$ 表示 Abel 群 M 的所有群自同态的集合.

♣

注 由模同态的定义知模同态必为群同态, 故有 $\mathrm{End}_R M \subseteq \mathrm{End}M$. 另一方面, 可以验证在 $\mathrm{End}M$ 中可定义加法与乘法使 $\mathrm{End}M$ 是一个环.

定理 1.31

设 M 是一个 R 模, 则 M 的 R 自同态的集合 $\mathrm{End}_R M$ 是 Abel 群 M 的自同态环 $\mathrm{End}M$ 的子环. $\mathrm{End}_R M$ 称为 R 模 M 的**模自同态环**.

♡

证明 显然, $\mathrm{id}_M \in \mathrm{End}_R M$, 故 $\mathrm{End}_R M \neq \varnothing$, 又若 $\eta_1, \eta_2 \in \mathrm{End}_R M$, $x, y \in M$, $a \in R$, 则有

$$(\eta_1 - \eta_2)(x+y) = \eta_1(x+y) - \eta_2(x+y) = (\eta_1 - \eta_2)(x) + (\eta_1 - \eta_2)(y),$$

可知 $\eta_1 - \eta_2 \in \mathrm{End}_R M$, 故 $\mathrm{End}_R M$ 对加法成群. 又由同态性质知 $\eta_1\eta_2 \in \mathrm{End}_R M$, 由此可知 $\mathrm{End}_R M$ 是 $\mathrm{End}M$ 的子环.

□

例题 1.21 设 M 为 Abel 群, 于是 M 为 $\mathbb{Z}$ 模. 则由命题 1.21知 $\mathrm{End}_{\mathbb{Z}} M = \mathrm{End}M$.

证明

□

例题 1.22 设 R 是一个幺环, 则 R 作为左 R 模有 $\mathrm{End}_R R = R_r$.

注 设 M 是一个左 R 模, 一般把 M 的模自同态环记为 ${}_R\mathrm{End}M$. 若 M 是右 R 模, 则将 M 的模自同态环记为 $\mathrm{End}_R M$. 交换幺环上的模, 可自然地看成双模, 故这时没必要区分这两种记号, 统一地以 $\mathrm{End}_R M$ 表示.

证明 $\forall a \in R$, 可定义 a 的右乘变换 a_r 为 $a_r(x) = xa (\forall x \in R)$. 显然, 对 $\forall x, y, a, b \in R$ 有 $a_r(x+y) = a_r(x) + a_r(y)$, $a_r(bx) = bxa = ba_r(x)$, 故 $a_r \in \mathrm{End}_R R$. 令 $R_r = \{a_r | a \in R\}$, 即有 $R_r \subseteq \mathrm{End}_R R$. 现设 $\eta \in \mathrm{End}_R R$, $\eta(1) = a$, 于是 $\eta(x) = \eta(x \cdot 1) = x\eta(1) = xa = a_r(x)$, 即 $\eta = a_r$. 故 $\eta \in R_r$, 这样就证明了幺环 R 作为左 R 模有 $\mathrm{End}_R R = R_r$.

□

1.7 同态基本定理

定义 1.35 (同态核)

1. 设 f 是群 G_1 到群 G_2 的同态,G_2 的幺元 e_2 的原像集合

$$\ker f = f^{-1}(e_2) = \{x \in G_1 | f(x) = e_2\}$$

称为 f 的**核**或**同态核**.

G_1 中所有元素的像集合

$$\mathrm{im}(f) = f(G_1) = \{y \in G_2 : \exists x \in G_1, y = f(x)\} = \{f(x) : x \in G_1\} \subseteq G_2.$$

称为 f 的**像**.

2. 设 f 是环 R_1 到环 R_2 的同态,R_2 的零元素 0 的原像集合

$$\ker f = f^{-1}(0) = \{x \in R_1 | f(x) = 0\}$$

称为 f 的**核**或**同态核**.

G_1 中所有元素的像集合

$$\mathrm{im}(f) = f(G_1) = \{y \in R_2 : \exists x \in R_1, y = f(x)\} = \{f(x) : x \in R_1\} \subseteq R_2.$$

称为 f 的**像**.

3. 设 R 是一个环,M_1, M_2 都是 R 模,f 是 M_1 到 M_2 的模同态. M_2 的零元素 0 的原像集合

$$\ker f = f^{-1}(0) = \{x \in M_1 | f(x) = 0\}$$

称为 f 的**核**或**同态核**.

G_1 中所有元素的像集合

$$\mathrm{im}(f) = f(G_1) = \{y \in M_2 : \exists x \in M_1, y = f(x)\} = \{f(x) : x \in M_1\} \subseteq M_2.$$

称为 f 的**像**.

命题 1.23

(1) 设 f 是群 G 到群 G' 的同态, 则 $\ker f$ 是 G 的子群,$f(G)$ 是 G' 的子群.

(2) 设 f 是环 R 到环 R' 的同态, 则 $f(R)$ 是 R' 的子环.

(3) 设 R 是一个环,M_1, M_2 都是 R 模,f 是 M_1 到 M_2 的模同态, 则 $f(M_1)$ 是 M_2 的子模.

注 $\ker f$ 在大多情况下都不是环 R 的子环.

证明

(1) 设 e, e' 分别是 G, G' 的幺元, 由群同态与同构的基本性质知 $f(e) = e'$, 故 $e \in \ker(f)$. 设 $x, y \in \ker(f)$, 利用同态的性质,$f(xy^{-1}) = f(x)f(y)^{-1} = e'e'^{-1} = e'$, 这就证明了 $xy^{-1} \in \ker(f)$. 故 $\ker f$ 是 G 的子群.
同样由群同态与同构的基本性质知 $f(e) = e'$, 我们有 $e' \in \mathrm{im}(f)$. 设 $y = f(x), y' = f(x') \in \mathrm{im}(f)$, 同样利用同态的性质,$yy'^{-1} = f(x)f(x')^{-1} = f(xx'^{-1}) \in \mathrm{im}(f)$. 故 $f(G)$ 是 G' 的子群.

(2) 由结论 (1) 知 $f(R)$ 构成 R' 的加法子群. 由 R 对加法构成 Abel 群知 $f(R)$ 对加法也构成 Abel 群. 由同态的性质易知 f 对乘法构成半群, 故 $f(R)$ 是 R' 的子环.

(3)

□

命题 1.24

(1) 设 H 是群 G 的正规子群. π 是 G 到商群 G/H 的自然同态 (见定理 1.19), 则有 $\ker \pi = H$.

(2) 设 I 是环 R 的理想,π 是 R 到商环 R/I 的自然同态 (见定理 1.23), 则有 $\ker \pi = I$.

(3) 设 N 是 R 模 M 的子模,π 是 M 到商模 M/N 的自然同态 (见定理 1.28), 则有 $\ker \pi = N$.

证明

(1)

(2)

(3)

□

命题 1.25

1. 设 f 是群 G_1 到群 G_2 的同态,G_1 的幺元是 e_1, 则 f 是单同态的充要条件是 $\ker f = \{e_1\}$.
2. 设 f 是环 R_1 到环 R_2 的同态, 则 f 是单同态的充要条件是 $\ker f = \{0\}$.
3. 设 R 是一个环,M_1, M_2 都是 R 模,f 是 M_1 到 M_2 的模同态, 则 f 是单同态的充要条件是 $\ker f = \{0\}$.

证明

□

定理 1.32 (群的同态基本定理)

设 f 是群 G 到群 H 上的同态, 则有下列结论:

(1) 若 G 的子群 G' 满足 $G' \supseteq \ker f$, 则 $\ker f \lhd G'$;

(2) 设 π 为 G 到商群 $G/\ker f$ 上的自然同态, 则有 $G/\ker f$ 到 $f(G)$ 上的群同构映射 $\overline{f}$, 使得

$$f = \overline{f} \cdot \pi, \tag{1.8}$$

进而

$$G\backslash\ker f \cong f(G).$$

如图 1.3所示.

♡

笔记

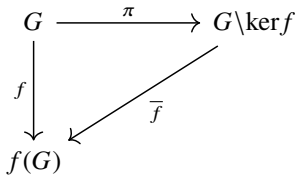

图 1.3

证明

(1) 设 e, e' 分别为 G', H 的幺元, 于是 $f(e) = e'$, 又设 $x, y \in \ker f, z \in G'$, 则

$$f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} = e',$$

因此 $xy^{-1} \in \ker f$, 故知 $\ker f$ 是 G' 的子群, 而且有

$$f(zxz^{-1}) = f(z)f(x)f(z)^{-1} = e',$$

即 $zxz^{-1} \in \ker f$, 由此知 $\ker f \lhd G'$.

(2) 由命题 1.23知 $f(G)$ 是 G 的子群. 注意到 f 是 G 到 $f(G)$ 上的满映射, 故由定理 1.19知 f 在 G 中诱导一个等价关系

$$R : xRy, \quad x, y \in G,$$

当且仅当 $f(x) = f(y)$, 即

$$f(x) = f(y) \iff f(x)^{-1}f(y) = f(x^{-1}y) = e' \iff x^{-1}y \in \ker f.$$

因而 f 诱导的等价关系恰好是 G 的正规子群 $\ker f$ 诱导的同余关系, 即有商群 $G/R = G/\ker f$ 且

$$\pi(x) = \pi(y) \text{ 当且仅当 } f(x) = f(y).$$

又由定理 1.19知有 $G/\ker f$ 到 $f(G)$ 的一一对应 $\overline{f}$, 使得 $\overline{f} \cdot \pi = f$, 又 $\forall x, y \in G$ 有

$$\overline{f}(\pi(x)\pi(y)) = \overline{f}(\pi(xy)) = f(xy) = f(x)f(y) = \overline{f}(\pi(x)) \cdot \overline{f}(\pi(y)).$$

由此知 $\overline{f}$ 是 $G/\ker f$ 到 $f(G)$ 上的群同构.

□

定理 1.33

设 f 是群 G 到群 H 上的满同态,f 的核为 K, 即 $K = \ker f$,G 中包含 K 的子群的集合为 Σ,H 的子群的集合为 Γ, 则有下列结论:

(1) f 是 $\Sigma \to \Gamma$ 的一一对应;

(2) 若 $G_1 \lhd G$,$G_1 \supseteq K$, 则

$$f(G_1) \lhd H.$$

若 $H_1 \lhd H$, 则

$$f^{-1}(H_1) \lhd G.$$

(3) 若 $G_1 \lhd G, G_1 \supseteq K$, 则

$$K \lhd G_1 \lhd G, \quad G/G_1 \cong H/f(G_1). \tag{1.9}$$

♡

证明

(1) 对 $\forall G_1 \in \Sigma$, 由 $f(G_1)$ 是 G_1 在 $f|_{G_1}$ 下的像, 又 f 是群同态, 故 $f(G_1)$ 为 H 的子群, 即 $f(G_1) \in \Gamma$. 由此知 f 是 Σ 到 Γ 的良定义的映射. 设 $H_1 \in \Gamma, H_1$ 在 f 下原像的集合

$$G_1 = f^{-1}(H_1) = \{x \in G | f(x) \in H_1\} \supseteq \{x \in G | f(x) = e', \ e' \text{ 为} H \text{ 的幺元}\} = K,$$

而且对 $\forall x, y \in G_1, f(xy^{-1}) = f(x)f(y)^{-1} \in H_1$, 故 $xy^{-1} \in G_1$, 因而 G_1 为 G 的子群, 故 $G_1 \in \Sigma$, 因此 f^{-1} 可视为 Γ 到 Σ 的良定义的映射.

由 f 是 $G \to H$ 上的满同态知 $f(G_1) = f(f^{-1}(H_1)) = H_1$, 由 H_1 的任意性知 $ff^{-1} = \mathrm{id}_\Gamma$. 反之, 设 $G_1 \in \Sigma$, 显然有 $G_1 \subseteq f^{-1}(f(G_1))$. 若 $u \in f^{-1}(f(G_1))$, 即有 $v \in G_1$, 使得 $f(u) = f(v)$, 从而

$$f(uv^{-1}) = f(u)f(v)^{-1} = e'.$$

因而 $uv^{-1} \in K \subseteq G_1$, 故 $u \in G_1$, 即有 $f^{-1}(f(G_1)) = G_1$, 由 G_1 的任意性知 $f^{-1}f = \mathrm{id}_\Sigma$.

综上所述知 f 是 $\Sigma \to \Gamma$ 的一一对应, f^{-1} 是其逆映射. 故结论 (1) 成立.

(2) 设 $G_1 \supset K$ 且 $G_1 \lhd G$, 即 $G_1 \in \Sigma$ 且 $G_1 \lhd G$, 则由 (1) 可知 $f(G_1)$ 是 H 的子群. 对 $\forall g \in f(G_1), y \in H$, 因为 f 是满同态, 所以存在 $a \in G_1, x \in G$, 使得 $f(a) = g, f(x) = y$. 从而

$$ygy^{-1} = f(x)f(a)f(x)^{-1} = f(xax^{-1}) \in f(G_1).$$

故知 $f(G_1) \lhd H$.

反之, 若 $H_1 \lhd H$ 且对 $\forall b \in f^{-1}(H_1), y \in G$, 由

$$f(yby^{-1}) = f(y)f(b)f(y)^{-1} \in H_1$$

知 $yby^{-1} \in f^{-1}(H_1)$, 故知 $f^{-1}(H_1) \lhd G$, 即结论 (2) 成立.

(3) 由群的同态基本定理 (1)知 $\ker f \lhd G_1$, 再由命题 1.10(2)知 $K \lhd G_1$, 再结合条件可得

$$K \lhd G_1 \lhd G.$$

由结论 (2) 的证明知 $f(G_1) \lhd H$. 令 π' 是 H 到商群 $H/f(G_1)$ 的自然同态, 由此可知有 G 到 $H/f(G_1)$ 上的同态映射 $\pi' \cdot f$, 注意到 $H/f(G_1)$ 的幺元为 $f(G_1)$, 则知

$$\begin{aligned} \ker(\pi' f) &= \{x \in G | \pi' f(x) = f(G_1)\} \\ &= \{x \in G | f(x) \in f(G_1)\} \\ &= f^{-1}(f(G_1)) = G_1. \end{aligned}$$

最后一个等号是因为由 (1) 知 f 是 $\Sigma \to \Gamma$ 的一一对应. 设 π 为 G 到 G/G_1 的自然同态, 又因为自然同态 π' 是满同态且 f 也是满同态, 所以由群的同态基本定理知有 G/G_1 到 $H/f(G_1)$ 的群同构 $\overline{f}$, 使得 $\pi' f = \overline{f} \cdot \pi$, 亦使图 1.4为交换图, 即式(1.9)成立.

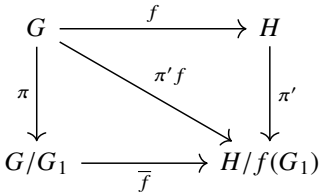

图 1.4

□

推论 1.6

设 N 为群 G 的正规子群,π 为 G 到商群 G/N 上的自然同态,G 中包含 N 的子群的集合为 Σ,G/N 的子群的集合为 Γ, 则

(1) π 是 $\Sigma \to \Gamma$ 的一一对应;

(2) 若 $H \lhd G, H \supseteq N$, 则

$$\pi(H) = H/N \lhd G/N.$$

若 $H' \lhd G/N$, 则

$$\pi^{-1}(H') \lhd G.$$

(3) 若 $H \lhd G, H \supseteq N$, 则

$$N \lhd H \lhd G, \quad G/H \cong (G/N)/(H/N).$$

♡

证明 事实上, 由于自然同态必是满同态, 故只要在定理 1.33中将 H 换成 G/N,f 换成 π, 即得本推论. 对于 (3), 由命题 1.16(1)知 $\pi(H) = H/N$, 故由定理 1.33可得

$$N \lhd H \lhd G,$$

以及如下交换图.

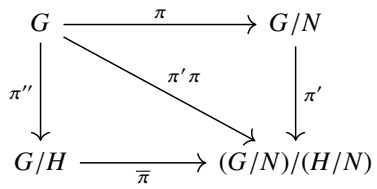

图 1.5

□

定理 1.34

设 N 是群 G 的正规子群,π 是 G 到商群 G/N 上的自然同态,H 是 G 的一个子群, 则有下列结论:

(1) HN 是 G 中包含 N 的子群且

$$N \lhd HN = \pi^{-1}(\pi(H)). \tag{1.10}$$

(2) $H \cap N \lhd H$ 且 $H \cap N = \ker(\pi|_H)$,$\pi|_H$ 表示 π 在 H 上的限制;

(3)

$$HN/N \cong H/(H \cap N).$$

♡

证明

(1) 显然,$HN \supseteq N$. 设 $h_i n_i \in HN (i = 1, 2)$, 则由 $N \lhd G$ 有

$$h_1 n_1 (h_2 n_2)^{-1} = h_1 h_2^{-1} (h_2 (n_1 n_2^{-1}) h_2^{-1}) \in HN.$$

故 HN 是 G 中含 N 的子群且 $\pi(h_1 n_1) = \pi(h_1)\pi(n_1) = \pi(h_1) \in \pi(H)$, 故 $HN \subseteq \pi^{-1}(\pi(H))$.
又设 $x \in \pi^{-1}(\pi(H))$, 则 $\pi(x) \in \pi(H)$, 从而存在 $h \in H$, 使得

$$\pi(x) = \pi(h) \iff xN = hN \iff x^{-1}h \in N.$$

于是存在 $n \in N$, 使得 $x^{-1}h = n$. 故 $x = hn^{-1} \in HN$. 因此 $\pi^{-1}(\pi(H)) \subseteq HN$. 综上可知 $HN = \pi^{-1}(\pi(H))$. 因为 H 是 G 的包含 N 的子群且 $N \lhd G$, 所以由命题 1.10(2)知 $N \lhd HN$.

(2) 由于 $N \lhd G$, 对 $\forall h \in H, a \in N \cap H$ 有 $hah^{-1} \in N \cap H$, 故 $N \cap H \lhd H$. 又 $\pi|_H(h) = \pi(h)$ 且 $\ker \pi = N$, 于是 $\ker(\pi|_H) = H \cap N$.

(3) 由 (1) 的结论知 $HN = \pi^{-1}(\pi(H))$, 再由自然同态是满同态知

$$\pi(HN) = \pi(\pi^{-1}(\pi(H))) = \pi(H).$$

由群的同态基本定理知

$$HN/\ker\pi|_{HN} \cong \pi(HN) = \pi(H) \cong H/\ker\pi|_H.$$

又注意到 $\ker(\pi|_{HN}) = HN \cap N = N, \ker \pi|_H = H \cap N$, 故

$$HN/N \cong H/(H \cap N).$$

□

定理 1.35 (环的同态基本定理)

设 f 是环 R 到环 R' 上的同态, 则有下列结论:

(1) $\ker f$ 是 R 的理想;

(2) 设 π 是 R 到商环 $R/\ker f$ 上的自然同态, 则有 $R/\ker f$ 到 $f(R)$ 上的环同构映射 $\overline{f}$, 使得

$$f = \overline{f} \cdot \pi. \tag{1.11}$$

即

$$R/\ker f \cong f(R).$$

♡

证明

(1) 设 $x, y \in \ker f$, 则有 $f(x-y) = 0$, 故 $x-y \in \ker f$. 又显然有 $\ker f$ 对乘法满足结合律且加法与乘法间满足左右分配律, 因此 $\ker f$ 是 R 的子环. 又设 $a \in R$, 则 $f(ax) = f(a)f(x) = 0, f(xa) = f(x)f(a) = 0$, 即 $ax, xa \in \ker f$, 故 $\ker f$ 为 R 的理想.

(2) 由命题 1.23知 $f(R)$ 是 R' 的子环. 又 f 为环同态, 故也是加法群 R 到加法群 $f(R)$ 上的同态, π 也是加法群 R 到商群 $R/\ker f$ 上的自然同态, 于是由群的同态基本定理知有加法群 $R/\ker f$ 到加法群 $f(R)$ 上的同构 $\overline{f}$, 使 $f = \overline{f} \cdot \pi$.

另外, $\forall a, b \in R$ 有

$$\begin{aligned}\overline{f}(\pi(a)\pi(b)) &= \overline{f}(\pi(ab)) = f(ab) = f(a)f(b)\\ &= \overline{f}(\pi(a))\overline{f}(\pi(b)),\end{aligned}$$

因而 $\overline{f}$ 也是环 $R/\ker f$ 到环 $f(R)$ 上的环同构.

□

定理 1.36

设 f 是环 R 到环 R' 上的满同态, 又 $K = \ker f$, R 中包含 K 的子环集合为 Σ, R' 的子环集合为 Γ, 则有下列结论:

(1) f 是 $\Sigma \to \Gamma$ 的一一对应;

(2) 若 H 为 R 的理想且 $H \supseteq K$, 则 $f(H)$ 为 R' 的理想;
若 H' 为 R' 的理想, 则 $f^{-1}(H')$ 为 R 的理想;

(3) 若 I 是 R 的理想且 $I \supseteq K$, 则

$$R/I \cong R'/f(I). \tag{1.12}$$

♡

证明

(1) 设 H 为 R 的子环且 $H \supseteq K$, 由环同态的基本性质 (1)知 $f(H)$ 为 R' 的子环. 故 f 是 $\Sigma \to \Gamma$ 上的良定义的映射. 反之, 若 H' 为 R' 的子环, 则 H' 也是 R' 的加法子群, 由定理 1.33(1)知 f 建立了加法群 R 中包含 K 的子

群与加法群 R' 的子群间的一一对应, 故 $f^{-1}(H')$ 是 R 中唯一包含 K 的加法子群. 又若 $a,b\in f^{-1}(H')$, 则有 $f(ab)=f(a)f(b)\in H'$, 即 $ab\in f^{-1}(H')$, 故 $f^{-1}(H')$ 对乘法构成半群. 再设 $c\in f^{-1}(H')$, 则

$$f((a+b)c)=f(a+b)f(c)=f(a)f(c)+f(b)f(c)\in H',$$
$$f(c(a+b))=f(c)f(a+b)=f(c)f(a)+f(c)f(b)\in H'.$$

因而 $f^{-1}(H')$ 是 R 中包含 K 的子环, 故 f^{-1} 可视为 $\Gamma\to\Sigma$ 上的良定义的映射.

对 $\forall H\in\Sigma, H'\in\Gamma$, 注意到 H 也是 R 中包含 K 的加法子群,H' 也是 R' 的加法子群, 由定理 1.33(1)知 $f^{-1}f(H)=H, ff^{-1}(H')=H'$. 由 H 的任意性知 $f^{-1}f=\mathrm{id}_\Sigma, ff^{-1}=\mathrm{id}_\Gamma$. 故 f 是 $\Sigma\to\Gamma$ 的一一对应,f^{-1} 是其逆映射. 即结论 (1) 成立.

(2) 对 $\forall a',b'\in R', h\in H$, 由环同态都是满同态知存在 $a,b\in R$, 使得 $f(a)=a', f(b)=b'$. 于是再由 H 是 R 的理想知

$$a'f(a)b'=f(a)f(h)f(b)=f(ahb)\in f(H).$$

故 $f(H)$ 为 R' 的理想.

反之, 设 H' 为 R' 的理想. 对 $\forall b\in R, x\in f^{-1}(H')$, 由 H' 是 R' 的理想知

$$f(bx)=f(b)f(x)\in H', f(xb)=f(x)f(b)\in H'.$$

即 $bx,xb\in f^{-1}(H')$, 故 $f^{-1}(H')$ 为 R 的理想. 由此知结论 (2) 成立.

(3) 设 π 是 R 到 R/I 的自然同态,π' 是 R' 到 $R'/f(I)$ 的自然同态. 由命题 1.18(2)知 $\pi' f$ 是 R 到 $R'/f(I)$ 上的环同态. 注意到

$$\begin{aligned}\ker(\pi' f)&=\{x\in R:\pi' f(x)=f(I)\}\\&=\{x\in R:f(x)\in f(I)\}\\&=f^{-1}(f(I))=I.\end{aligned}$$

最后一个等号是因为由 (1) 知 f 是 $\Sigma\to\Gamma$ 的一一对应. 于是由环的同态基本定理得式(1.12)成立.

□

推论 1.7

设 A,B 均为环 R 的理想且 $A\subseteq B$, 则有 B/A 是 R/A 的理想且

$$R/B\cong(R/A)/(B/A).$$

♡

证明 事实上, 只要在定理 1.36中取 $R'=R/A, f$ 为 R 到 R/A 的自然同态, 并且由定理 1.19(1)知 $f(B)=B/A$, 再由定理 1.36(2)知 $f(B)=B/A$ 是 $R'=R/A$ 的理想. 因此即得本推论.

□

定理 1.37

设 H 为环 R 的子环,K 为 R 的理想,π 是环 R 到商环 R/K 上的自然同态, 则有

(1) $H+K$ 为 R 中包含 K 的子环,K 是 $H+K$ 的理想, 并且

$$H+K=\pi^{-1}(\pi(H)).$$

(2) $H\cap K$ 为 H 的理想且 $H\cap K=\ker\pi|_H$.

(3)

$$(H+K)/K\cong H/(H\cap K).\tag{1.13}$$

♡

证明

(1) 显然 $H+K\supseteq K$. 设 $h_i+k_i\in H+K(i=1,2), r\in R$, 则 $(h_1+k_1)-(h_2+k_2)=h_1-h_2+k_1-k_2\in H+K$. 于是 $H+K$ 是 R 的加法子群. 由 $H+K\subseteq R$ 知 $H+K$ 对乘法满足结合律且加法与乘法间满足左右分配律. 故

$H+K$ 是 R 中含 K 的子环. 又注意到 $\pi(h_1+k_1)=h_1+k_1+K=h_1+K\in\pi(H)$. 故 $h_1+k_1\in\pi^{-1}(\pi(H))$, 因此 $H+K\subseteq\pi^{-1}(\pi(H))$.

反之, 设 $x\in\pi^{-1}(\pi(H))$, 则 $\pi(x)\in\pi(H)$. 从而存在 $h'\in H$, 使得 $\pi(x)=\pi(h')\Longleftrightarrow x+K=h'+K\Longleftrightarrow -x+h'\in K$. 于是存在 $k'\in K$, 使得 $-x+h'=k'$, 从而 $x=h'-k'\in H+K$. 故 $\pi^{-1}(\pi(H))\subseteq H+K$. 综上可知 $H+K=\pi^{-1}(\pi(H))$.

因为 H 为环 R 的子环,K 为 R 的理想且 $H+K\supseteq K$, 所以由定理 1.16(2)知 K 是 $H+K$ 的理想.

(2) 由 H,K 都是 R 的子环知 $H\cap K$ 是 R 的子环. 又因为 $H\supseteq H\cap K$, 所以 $H\cap K$ 也是 H 的子环. 对 $\forall x\in H\cap K, h\in H$, 由 K 是 R 的理想知 $hx,xh\in H\cap K$. 故 $H\cap K$ 是 H 的理想. 又 $\pi|_H(h)=\pi(h)$ 且 $\ker\pi=K$, 故 $\ker\pi|_H=H\cap K$.

(3) 由结论 (1) 知 $H+K=\pi^{-1}(\pi(H))$, 再由自然同态都是满同态知

$$\pi(H+K)=\pi(\pi^{-1}(\pi(H)))=\pi(H).$$

于是由环的同态基本定理知

$$(H+K)/\ker\pi|_{H+K}\cong\pi(H+K)=\pi(H)\cong H/\ker\pi|_H.$$

注意到 $\ker\pi|_{H+K}=(H+K)\cap K=K$,$\ker\pi|_H=H\cap K$, 故

$$(H+K)/K\cong H/(H\cap K).$$

□

定理 1.38 (模同态的基本定理)

设 M,M' 都是幺环 R 上的模,f 是模 M 到模 M' 上的同态,M 中包含 N 的子模集合为 Σ,M' 中子模集合为 Γ, 则有下面结论:

(1) $\ker f=N$ 是 M 的子模.

(2) 设 π 是 M 到 M/N 上的自然模同态, 则有 M/N 到 $f(M)$ 的模同构 $\overline{f}$, 使得

$$\overline{f}\cdot\pi=f \tag{1.14}$$

即

$$M/N\cong f(M).$$

♡

证明

(1) 对 $\forall x,y\in\ker f$, 由 f 是模同态知 $f(x-y)=f(x)-f(y)=0$. 从而 $x-y\in\ker f$, 于是 $\ker f=N$ 是加法群 M 的子群, 设 $a\in R,x\in N$, 则 $f(ax)=af(x)=0$, 因而 $ax\in N$, 故 N 是 M 的子模.

(2) 由命题 1.23知 $f(M)$ 是 M' 的子模. 由群的同态基本定理知有加法群 M/N 到加法群 $f(M)$ 上的同构 $\overline{f}$, 使 $\overline{f}\cdot\pi=f$. 现只需证 $\overline{f}$ 是模同构. 又设 $a\in R,x\in M$, 于是有

$$\overline{f}(a\pi(x))=\overline{f}(\pi(ax))=f(ax)=af(x)=a\overline{f}(\pi(x)),$$

即 $\overline{f}$ 为模同构.

□

定理 1.39

设 M,M' 都是幺环 R 上的模,f 是模 M 到模 M' 上的满同态,M 中包含 N 的子模集合为 Σ,M' 中子模集合为 Γ, 则有下面结论:

(1) f 是 $\Sigma\to\Gamma$ 的一一对应.

(2) 若 M_1 是 M 的子模且 $M_1\supseteq N$, 则

$$M/M_1\cong M'/f(M_1) \tag{1.15}$$

♡

证明

(1) 若 M_1 为 M 的子模, 则由定理 1.29(1)知 $f(M_1)$ 为 M' 的子模. 故 f 是 $\Sigma \to \Gamma$ 上的良定义的映射.
反之, 若 M_1' 为 M' 的子模, 则 M_1' 也是 M' 的加法子群. 从而由定理 1.33(1)知 $f^{-1}(M_1')$ 是 M 中唯一包含 N 的加法子群. 又设 $a \in R, x \in f^{-1}(M_1')$. 由 $f(ax) = af(x) \in M_1'$ 知 $ax \in f^{-1}(M_1')$, 即 $f^{-1}(M')$ 是 M 的子模. 故 f^{-1} 可视为 $\Gamma \to \Sigma$ 上的良定义的映射.
对 $\forall H \in \Sigma, H' \in \Gamma$, 注意到 H 也是 R 中包含 K 的加法子群,H' 也是 R' 的加法子群, 由定理 1.33(1)知 $f^{-1}f(H) = H, ff^{-1}(H') = H'$. 由 H 的任意性知 $f^{-1}f = \mathrm{id}_\Sigma, ff^{-1} = \mathrm{id}_\Gamma$. 故 f 是 $\Sigma \to \Gamma$ 的一一对应,f^{-1} 是其逆映射, 即结论 (1) 成立.

(2) 设 M_1 为 M 的子模且 $M_1 \supseteq N$. 又设 π_1 是 M 到 M/M_1 的自然同态,π' 是 M' 到 $M'/f(M_1)$ 的自然同态. 于是 $\pi' f$ 是 M 到 $M'/f(M_1)$ 上的同态, 而且

$$\begin{aligned}\ker(\pi' f) &= \{x \in R : \pi' f(x) = f(M_1)\} \\ &= \{x \in R : f(x) \in f(M_1)\} \\ &= f^{-1}(f(M_1)) = M_1.\end{aligned}$$

最后一个等号是因为由结论 (1) 知 f 是 $\Sigma \to \Gamma$ 的一一对应. 故由模同态的基本定理可知式(1.15)成立.

□

推论 1.8

设 M_1, N 都是 R 模 M 的子模, 而且 $M_1 \supseteq N$, 则有模同构

$$M/M_1 \cong (M/N)/(M_1/N).$$

♡

证明 事实上, 只要在定理 1.39(2)中取 $M' = M/N, f$ 为 M 到 $M' = M/N$ 的自然同态, 再由命题 1.22(1)知 $f(M_1) = M_1/N$, 即得本推论.

□

定理 1.40

设 H, N 为 R 模 M 的子模, 则有模同构

$$(H + N)/N \cong H/(H \cap N) \tag{1.16}$$

♡

证明 设 π 为模 M 到商模 M/N 的自然模同态, 由于 N 为商群 M/N 中的加法幺元, 即商模 M/N 中的零元, 于是有 $\pi(H + N) = \pi(H) + N = \pi(H)$, 因而由模同态的基本定理 (1)知

$$H + N/\ker(\pi|_{H+N}) \cong \pi(H + N) = \pi(H) \cong H/\ker(\pi|_H).$$

由 $\ker(\pi|_{H+N}) = (H + N) \cap N = N, \ker(\pi|_H) = H \cap N$, 即得式(1.16)成立.

□

1.8 循环群

定义 1.36 (循环群)

设 G 是一个群且 $a \in G$, 我们称

$$\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$$

是**由 a 生成的 G 的子群**, 如果在一个群 G 中存在一个元素 a, 使得 $G = \langle a \rangle$, 即 G 由 a 生成, 则称 G 是**循环群**, a 为 G 的一个**生成元**.

♣

注 对 $\forall n_1, n_2 \in \mathbb{Z}$, 有 $a^{n_1}a^{-n_2} = a^{n_1-n_2} \in G$. 因此 $\langle a \rangle$ 是 G 的子群. 故由 a 生成的 G 的子群是良定义的.

命题 1.26

循环群都是 Abel 群.

证明

□

推论 1.9

有限群 G 的任一元素 a 的阶是 G 的阶的因子, 即 $\operatorname{ord} a \mid [G:1]$. 进一步, 若 $G=\langle a\rangle$, 则 $\operatorname{ord} a=[G:1]$, 并且 $G=\langle a\rangle=\{1,a,\cdots,a^{\operatorname{ord} a-1}\}$.

证明 令 $\langle a\rangle=\{a^n|n\in\mathbb{Z}\}$, 容易验证这是 G 的一个子群. 又由于 G 有限, 故 $\langle a\rangle$ 有限, 因而 a 是有限阶的, 设为 d. 对 $n\in\mathbb{Z}$ 有 t_n 与 r_n $(0\leqslant r_n<d)$, 使 $n=t_nd+r_n$, 于是 $a^n=a^{r_n}$. 因此 $\langle a\rangle$ 中至多只有 d 个元素 $1,a,\cdots,a^{d-1}$.

又对 $\forall r_1,r_2\in\mathbb{N}$, 且 $r_1\neq r_2, 0\leqslant r_1,r_2<d$, 则 $|r_1-r_2|<d$, 从而 $a^{r_1-r_2}\neq 1$, 进而 $a^{r_1}\neq a^{r_2}$. 故 $1,a,\cdots,a^{d-1}$ 互不相同. 由此知 $\langle a\rangle=\{1,a,\cdots,a^{d-1}\}$, 即 $\langle a\rangle$ 是 d 阶群. 故由Lagrange 定理知 d 为 $[G:1]$ 的因子.

若 $G=\langle a\rangle, \operatorname{ord} a=d$, 则由上述证明知 $G=\langle a\rangle=\{1,a,\cdots,a^{d-1}\}$ 是 d 阶群, 故 $d=[G:1]$.

□

定理 1.41

循环群的任何子群也是循环群.

证明 设 G_1 是循环群 $G=\langle a\rangle$ 的一个非平凡子群. 令

$$k=\min\{m'\in\mathbb{N}|a^{m'}\in G_1\},$$

于是 G 中由 a^k 生成的子群 $\langle a^k\rangle\subseteq G_1$, 又若有 $a^{m'}\in G_1$, 则有整数 q,r 满足

$$m'=kq+r,\quad 0\leqslant r<k,$$

因而 $a^r=a^{m'}(a^k)^{-q}\in G_1$, 由 k 的取法知 $r=0$, 否则与 k 的最小值取法矛盾! 因而 $a^{m'}=(a^k)^q\in\langle a^k\rangle$, 故 $G_1\subseteq\langle a^k\rangle$, 所以 $G_1=\langle a^k\rangle$ 为循环群.

□

推论 1.10

设 $\operatorname{ord} a=n$, r 是任一整数. 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

$$d=nu+rv.$$

于是 $a^d=a^{nu+rv}=a^{rv}\in\langle a^r\rangle$. 另一方面, 同样由于 $(n,r)=d$, 所以 $d\mid r$, 从而又有 $a^r\in\langle a^d\rangle$, 于是 $\langle a^r\rangle\subseteq\langle a^d\rangle$. 由此得 $\langle a^r\rangle=\langle a^d\rangle$.

□

推论 1.11

设 $G=\langle a\rangle$ 为循环群,

(1) 如果 $|G|=\infty$, 则 G 的全部子群为 $\{\langle a^d\rangle\mid d=0,1,2,\cdots\}$, 并且 $\langle a^{d_1}\rangle\neq\langle a^{d_2}\rangle, \forall d_1,d_2\in\mathbb{N}_0$且$d_1\neq d_2$;

(2) 如果 $|G|=n$, 则 G 的全部子群为 $\{\langle a^d\rangle\mid d$ 为 n 的正因子 $\}$, 并且 $\langle a^{d_1}\rangle\neq\langle a^{d_2}\rangle, \forall d_1,d_2$ 为 n 的正因子.

证明 设 e 为 G 的幺元,G 的所有子群构成的集合为 S. 由定理 1.41知, 循环群的任一子群必形如 $\langle a^r\rangle(r\in\mathbb{Z})$. 显然, 有

$$\langle a^r\rangle=\langle a^{-r}\rangle.$$

因此, 循环群的任一子群必形如 $\langle a^r\rangle (r\in\mathbb{Z}, r\geqslant 0)$. 此即

$$S=\{\langle a^r\rangle \mid r\in\mathbb{Z}, r\geqslant 0\}=\{\langle a^r\rangle \mid r=0,1,2,\cdots\}. \tag{1.17}$$

(1) 如果 $|G|=\infty$, 由(1.17)式知

$$S=\{\langle a^r\rangle \mid r=0,1,2,\cdots\}.$$

只需证这个集合中的元素两两不同即可. 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 $a^r\notin\langle a^0\rangle=\langle e\rangle=\{e\}$, 所以有

$$\langle a^r\rangle\neq\langle e\rangle.$$

故 $\langle a^{d_1}\rangle\neq\langle a^{d_2}\rangle, \forall d_1,d_2\in\mathbb{N}_0$且$d_1\neq d_2$.

(2) 如果 $|G|=n$, 对任意的正整数 r, 存在 n 的正因子 $d=(n,r)$, 由推论 1.10可知

$$\langle a^r\rangle=\langle a^d\rangle\in\{\langle a^d\rangle \mid d为n的正因子\}.$$

故再由(1.17)式知 $S\subseteq\{\langle a^d\rangle \mid d为n的正因子\}$. 又显然有 $S\supseteq\{\langle a^d\rangle \mid d为n的正因子\}$, 故

$$S=\{\langle a^d\rangle \mid d为n的正因子\}.$$

若 $d_1>d_2$ 为 n 的两个不同的正因子, 则 $d_1\nmid d_2$, 于是 $a^{d_2}\notin\langle a^{d_1}\rangle$, 从而

$$\langle a^{d_1}\rangle\neq\langle a^{d_2}\rangle.$$

故 $\langle a^{d_1}\rangle\neq\langle a^{d_2}\rangle, \forall d_1,d_2$ 为 n 的正因子.

□

推论 1.12

(1) 设 $m\in\mathbb{Z}$, 则 $m\mathbb{Z}\triangleq\{mx|x\in\mathbb{Z}\}$ 是整数加法群 $\mathbb{Z}$ 的子群.

(2) 整数加法群 $\mathbb{Z}$ 的任何子群必为 $m\mathbb{Z}(m\geqslant 0$且$m\in\mathbb{Z})$.

♡

证明

(1) 对 $\forall x_1,x_2\in\mathbb{Z}$, 有

$$mx_1-mx_2=m(x_1-x_2)\in m\mathbb{Z}.$$

故 $m\mathbb{Z}$ 是整数加法群 $\mathbb{Z}$ 的子群.

(2) 事实上, $\mathbb{Z}=\langle 1\rangle$. 设 G_1 为 $\mathbb{Z}$ 的子群. 于是由定理 1.41有 $m\geqslant 0$且$m\in\mathbb{Z}$, 使得 $G_1=\langle m\rangle=m\mathbb{Z}$.

□

命题 1.27 (素数阶群必为循环群)

设 G 是一个群, 且 $|G|=p$ 为一个素数, 则

(1) G 必是循环群, 并且 $\forall a\in G$ 且 $a\neq e$ 有 $G=\langle a\rangle$.

(2) G 只有平凡子群.

♠

证明

(1) 由 $p>1$ 知 G 中至少存在一个非幺元 $a\neq e$, 则对 $\forall a\in G$ 且 $a\neq e$, 有 $\langle a\rangle$ 是 G 的子群. 由 Lagrange 定理知 $\langle a\rangle$ 的阶是 $|G|=p$ 的因数, 而 p 为素数, 故 $\langle a\rangle$ 的阶为 1 或 p. 由 $a,e\in\langle a\rangle$ 知 $\langle a\rangle$ 的阶必大于 1, 因此 $\langle a\rangle$ 的阶为 p. 又因为 $\langle a\rangle\subseteq G$, 所以 $G=\langle a\rangle$. 故 G 为循环群.

(2) 由结论 (1) 知 G 是循环群. 又循环群的任何子群也是循环群, 故 G 的任意子群 H 也是循环群, 若 $H\neq\{e\}, G$, 则可设 $H=\langle a\rangle, a\in G\setminus\{e\}$, 再由结论 (1) 知 $G=\langle a\rangle=H$ 矛盾! 故 $H=\{e\}$或G.

□

命题 1.28

设 $m>0$, 则有

$$m\mathbb{Z}\lhd\mathbb{Z},\quad \mathbb{Z}=\bigcup_{k=0}^{m-1}(k+m\mathbb{Z}),\quad \mathbb{Z}_m\triangleq\mathbb{Z}/m\mathbb{Z}=\{\overline{0},\overline{1},\cdots,\overline{m-1}\},\quad [\mathbb{Z}:m\mathbb{Z}]=m.$$

♠

证明 由推论 1.12(1)知 $m\mathbb{Z}$ 为 $\mathbb{Z}$ 的子群.

□

定理 1.42

设 $G=\langle a\rangle$ 是一个循环群.

(1) 若 G 是无限阶的, 则 G 与整数加法群 $\mathbb{Z}$ 同构.

(2) 若 G 的阶 m 有限, 则 G 与加法群 $\mathbb{Z}_m$ 同构.

进而两个循环群同构当且仅当它们的阶相同.

♡

证明 作 $\mathbb{Z}$ 到 G 上的映射 $\varphi:\varphi(n)=a^n(n\in\mathbb{Z})$. 于是有

$$\varphi(n_1+n_2)=a^{n_1+n_2}=a^{n_1}\cdot a^{n_2}=\varphi(n_1)\varphi(n_2),$$

因而 φ 是 $\mathbb{Z}$ 到 G 上的同态映射, 故由群的同态基本定理知 $G\cong\mathbb{Z}/\ker\varphi$ 且 $\ker\varphi\lhd\mathbb{Z}$. 由推论 1.12(2)知存在 $m\geqslant 0$且$m\in\mathbb{Z}$, 使得 $\ker\varphi=m\mathbb{Z}$.

若 $m>0$, 则由命题 1.28知, 此时 $G\cong\mathbb{Z}/\ker\varphi=\mathbb{Z}/m\mathbb{Z}=\mathbb{Z}_m$ 且 $|G|=|\mathbb{Z}_m|=m$.

若 $m=0$, 则 $G\cong\mathbb{Z}$ 同构, 此时 G 的阶为无限.

□

推论 1.13

无限循环群的非平凡子群仍为无限循环群.

♡

证明 设 G 为无限循环群, 则由定理 1.42知 $G\cong\mathbb{Z}$. 又由推论 1.12(2)知 $\mathbb{Z}$ 的非平凡子群为 $m\mathbb{Z}(m\neq 0,1)$ 为无限循环群. 故 G 的非平凡子群也为无限循环群.

□

定理 1.43

设 G 是 m 阶循环群,m_1 是 m 的一个因数, 则存在唯一的 m_1 阶子群.

♡

证明 设 $G=\langle a\rangle$. 从推论 1.9知 G 的阶 m 也就是元素 a 的阶. 由 $m_1|m$ 知当 $0<k<m_1$ 时有 $0<km/m_1<m$, 因而 $(a^{m/m_1})^k\neq 1$, 但 $(a^{m/m_1})^{m_1}=1$, 故 $\langle a^{m/m_1}\rangle$ 是 G 的 m_1 阶子群.

下面证 m_1 阶子群的唯一性. 设 G_1 是 G 中的 m_1 阶子群, 由定理 1.41知 $G_1=\langle a^k\rangle$, 其中,$k\geqslant 0$, 并且当 $a^{m'}\in G_1$ 时,$k|m'$. 由 $a^m=1\in G_1$ 知 $k|m$, 若 $0<n<m/k$, 则 $0<kn<m$, 从而 $(a^k)^n=a^{kn}\neq 1$. 另外 $(a^k)^{m/k}=1$, 故 G_1 的阶为 $m/k=m_1$, 因而 $k=m/m_1$, 即 $G_1=\langle a^{m/m_1}\rangle$.

□

命题 1.29

设 G 是 n 阶群且其不同的子群有不同的阶. 试证:

(1) G 的任何子群都是正规子群;

(2) G 的子群与商群的不同子群也有不同的阶;

(3) G 是循环群.

♠

证明

(1) 设 H 为 G 的子群, $g \in G$. 对 $\forall h_1, h_2 \in H$, 有

$$(gh_1g^{-1})(gh_2g^{-1})^{-1} = (gh_1g^{-1})(gh_2^{-1}g^{-1}) = gh_1h_2^{-1}g^{-1} \in gHg^{-1}.$$

故 gHg^{-1} 是 G 的子群. 又由命题 1.9知 gHg^{-1} 与 H 有相同的阶. 因此由条件知 $gHg^{-1} = H$, 故 H 是正规子群.

(2) 设 H_1, H_2 是 G 的子群 H 的子群, 自然也是 G 的子群, 于是由条件知 $H_1 = H_2$ 当且仅当 $|H_1| = |H_2|$.
设 $\overline{H_1}, \overline{H_2}$ 是商群 G/H 的子群. 记 π 为 G 到商群 G/H 上的自然同态,G 中包含 H 的子群的集合为 Σ,G/H 的子群的集合为 Γ, 由推论 1.6(1)知有 G 的子群 $H_1 \supseteq H, H_2 \supseteq H$ 使得

$$\overline{H_1} = \pi(H_1) = H_1/H, \quad \overline{H_2} = \pi(H_2) = H_2/H.$$

因为 π 是 $\Sigma \to \Gamma$ 的双射, 所以 $\overline{H_1} = \overline{H_2}$ 当且仅当 $H_1 = H_2$. 而 $H_1 = H_2$ 当且仅当 $|H_1| = |H_2|$. 注意

$$|H_i| = [H_i : H]|H| = |\overline{H_i}||H|, \quad i = 1, 2.$$

于是 $\overline{H_1} = \overline{H_2}$ 当且仅当 $|\overline{H_1}| = |\overline{H_2}|$.

(3) 设 $|G| = p_1p_2\cdots p_s$, 其中 $p_i (1 \leqslant i \leqslant s)$ 是素数.
对 s 作归纳证明 G 是循环群. 若 $s = 0$, 则 $|G| = 1$, 显然 G 是循环群. 若 $s = 1$, $|G| = p_1$ 是素数, 由命题 1.27知 G 是循环群. 假定 $s-1$ 时结论成立. 以 e 表示 G 的幺元, 取 $a_1 \in G, a_1 \neq e$. 若 a_1 的阶为 n, 则 G 是循环群. 不妨设 a_1 的阶为 $p_sp_{s-1}\cdots p_k \neq n$, 于是 $a = a_1^{p_{s-1}\cdots p_k}$ 的阶为 p_s. 由结论 (1), $\langle a\rangle$ 是 G 的正规子群. 由结论 (2), 商群 $G/\langle a\rangle$ 的不同子群有不同的阶, 由推论 1.3知 $G/\langle a\rangle$ 的阶为 $n_1 = p_1p_2\cdots p_{s-1}$. 由归纳假设, $G/\langle a\rangle$ 是循环群. 于是存在 $b \in G$ 使得 $G/\langle a\rangle$ 的元素为 $\langle a\rangle, b\langle a\rangle, \cdots, b^{n_1-1}\langle a\rangle$. 从而由 $(b\langle a\rangle)^{n_1} = \langle a\rangle$ 知对 $0 \leqslant k < p_s$, 有 $k_0 (0 \leqslant k_0 < p_s)$ 使得

$$(ba^k)^{n_1} = a^{k_0}.$$

下面证明 $b\langle a\rangle$ 中有元素 c 使得 $c^{n_1} \neq e$. 若 $b^{n_1} \neq e$, 则可取 $c = b$. 故设 $b^{n_1} = e$. 注意 $G/\langle a\rangle$ 的阶为 n_1, 于是当 $0 < r < n_1$ 时, $b^r \neq e, (ba)^r \neq e$. 如果 $(ba)^{n_1} = e$, 则 $\langle b\rangle$ 与 $\langle ba\rangle$ 均为 n_1 阶群, 因而由条件知 $\langle b\rangle = \langle ba\rangle$, 于是有 $ba = b^m, 0 < m < n_1$. 由于 $ba \in b\langle a\rangle, b^m \in b^m\langle a\rangle$, 而 $m \neq 1$ 时, 由推论 1.2知 $b\langle a\rangle \cap b^m\langle a\rangle = \varnothing$, 于是 $m = 1$, 即 $ba = b$, 从而 $a = e$, 这就得到矛盾. 由此可知 $(ba)^{n_1} \neq e$. 取 $c = ba$. 由 $c \in b\langle a\rangle$, 知 $b\langle a\rangle = c\langle a\rangle$, 于是 $G/\langle a\rangle = \langle c\langle a\rangle\rangle$. 因为 $G/\langle a\rangle$ 的阶为 n_1, 所以 $(c\langle a\rangle)^{n_1} = c^{n_1}\langle a\rangle = \langle a\rangle$. 因而 $c^{n_1} \in \langle a\rangle$. 注意 $c^{n_1} \neq e$, 于是

$$c^{n_1} = a^m \neq e, \quad 1 \leqslant m < p_s.$$

因为 p_s 是素数, 所以有 $(m, p_s) = 1$. 进而 $a \in \langle c\rangle, \langle a\rangle \subset \langle c\rangle$. 于是有

$$\langle c\rangle/\langle a\rangle = G/\langle a\rangle.$$

因此 $G = \langle c\rangle$ 为循环群.

□

定理 1.44

一个 m 阶群 G 对 m 的每个因数 m_1 存在唯一的 m_1 阶子群, 则群 G 必是循环群.

♡

证明 设 G_1, G_2 是 G 的两个不同子群, 则由Lagrange 定理知 $[G_1 : 1], [G_2 : 1]$ 都是 m 的因数. 若 $[G_1 : 1] = [G_2 : 1]$, 则由条件知 $G_1 = G_2$ 矛盾! 故 $[G_1 : 1] \neq [G_2 : 1]$. 因此 G 的不同的子群有不同的阶. 于是由命题 1.29(3)知 G 必是循环群.

□

定理 1.45

设 G 是一个群,$a, b \in G$. 它们的阶分别为 m, n, 则有下列结论:

(1) a^k 的阶为 $\dfrac{m}{(m,k)}$, 其中 (m, k) 是 m 与 k 的最大公因数;

(2) 若 $\langle a\rangle \cap \langle b\rangle = \{1\}$,$ab = ba$, 则 ab 的阶为 m, n 的最小公倍数 $[m, n]$.

♡

证明

(1) 设 a^k 的阶为 q, 即 $a^{kq}=1$, 因而有 $m|kq$, 故由数论相关结论知 $\frac{m}{(m,k)}|q$. 又 $(a^k)^{\frac{m}{(m,k)}}=(a^m)^{\frac{k}{(m,k)}}=1$, 即得 $q|\frac{m}{(m,k)}$, 因而

$$q=\frac{m}{(m,k)}.$$

(2) 设 ab 的阶为 m_1, 则有 $(ab)^{m_1}=1$. 由 $ab=ba$ 知 $a^{m_1}b^{m_1}=(ab)^{m_1}=1$, 即 $a^{m_1}=b^{-m_1}\in\langle a\rangle\cap\langle b\rangle=\{1\}$, 因而 $a^{m_1}=b^{m_1}=1$, 故 $m|m_1$,$n|m_1$, 因而 $[m,n]|m_1$. 另有 $(ab)^{[m,n]}=a^{[m,n]}b^{[m,n]}=1$, 故 $m_1|[m,n]$, 即 $m_1=[m,n]$.

□

推论 1.14

(1) 若 a 为 m 阶元素, 则 a^k 为 m 阶元素的充要条件是 $(m,k)=1$;

(2) 若 a,b 的阶分别为 m,n 且 $ab=ba$,$(m,n)=1$, 则 ab 的阶为 mn.

♡

证明

(1) 这是定理 1.45的自然推论.

(2) 设 m_1 是 $\langle a\rangle\cap\langle b\rangle$ 的阶, 由推论 1.9知 $\langle a\rangle,\langle b\rangle$ 的阶分别为 m,n. 由于 $\langle a\rangle\cap\langle b\rangle$ 是 $\langle a\rangle,\langle b\rangle$ 的子群, 故由Lagrange定理知 $m_1|m$,$m_1|n$. 但 $(m,n)=1$, 故 $m_1=1$, 因而 $\langle a\rangle\cap\langle b\rangle=\{1\}$, 于是由定理 1.45知 ab 的阶为 $[m,n]=mn$.

□