



抽象代数

作者: 实空

组织: 无

时间: November 9, 2025

版本: ElegantBook-4.5

自定义: 信息



宠辱不惊, 闲看庭前花开花落;
去留无意, 漫随天外云卷云舒.

目录

第1章 群	1
1.1 二元运算与同余关系	1
1.2 幺半群 群	4
1.3 子群与商群	7
1.4 环与域	13
1.5 同态与同构	17
1.6 模	22
1.7 同态基本定理	26

第1章 群

1.1 二元运算与同余关系

定义 1.1

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 1.2

设集合 A 有二元运算 $(a, b) \rightarrow ab$ 且满足结合律, 则对 $\forall n \in \mathbf{N}$ (\mathbf{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**

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

命题 1.1

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

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

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 1.3

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. $na + ma = (n + m)a$, $n(ma) = (nm)a$, $\forall a \in A, m, n \in \mathbf{N}$.

2. 若 $a + b = b + a$, 则

$$n(a + b) = na + nb, \quad \forall n \in \mathbf{N},$$

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. □

定义 1.4 ((二元) 关系)

所谓在集合 A 中定义了二元素间的一个 **(二元) 关系** R , 也就是给出了集合 $A \times A$ 中元素的一个性质 R , 若 $a, b \in A$, (a, b) 有性质 R , 则称 a 与 b 有关系 R , 记为 aRb .

 **笔记** 事实上, 集合 A 中关系 R 可由 $A \times A$ 中子集

$$S \triangleq \{(a, b) \mid a, b \in A, aRb\}$$

来刻画. 即若 aRb , 则 $(a, b) \in S$.

反之, 由 $A \times A$ 的一个子集 S , 也可确定 A 一个关系 R . 即若 $(a, b) \in S$, 则 aRb .

定义 1.5 (等价关系)

1. 集合 A 中关系若满足以下条件:

(1) **自反性** $aRa, \forall a \in A$;

(2) **对称性** 若 aRb , 则 bRa ;

(3) **传递性** 若 aRb, bRc , 则 aRc ,

则称 R 为 A 的一个 **等价关系**.

2. 若仍以 R 表示 A 中关系所确定的 $A \times A$ 的子集, 则 R 为等价关系当且仅当下列三个条件同时成立:

(1) $(a, a) \in R, \forall a \in A$;

(2) 若 $(a, b) \in R$, 则 $(b, a) \in R$;

(3) 若 $(a, b) \in R, (b, c) \in R$, 则 $(a, c) \in R$.

注 在等价关系定义中的三个条件是互相独立的, 缺一不可.

定义 1.6 (等价类和代表元素)

若 R 是集合 A 的一个等价关系且 $a \in A$, 则 A 中所有与 a 有关系 R 的元素集合

$$K_a = \{b \in A \mid bRa\}$$

称为 a 所在的 **等价类**, a 称为这个等价类的 **代表元素**.

定义 1.7 (分划/分类)

集合 A 的一个子集族 $\{A_\alpha\}$ 称为 A 的一个 **分划** 或 **分类**, 如果满足

$$A = \bigcup_{\alpha} A_{\alpha}, \quad A_{\alpha} \cap A_{\beta} = \emptyset, \quad \text{若 } \alpha \neq \beta.$$

也称 A 是 $\{A_\alpha\}$ 中所有不相交的集合的并或无交并.

定理 1.1

设 R 是集合 A 的等价关系, 则由所有不同的等价类构成的子集族 $\{K_a\}$ 是 A 的分划.

反之, 若 $\{A_\alpha\}$ 是 A 的分划, 则可在 A 中定义等价关系 R ,

$$aRb, \quad \text{若 } \exists A_\alpha, \text{ 使 } a, b \in A_\alpha.$$

并且使得每个 A_α 是一等价类.



证明 设 R 是 A 的等价关系. 由 $\forall a \in A, aRa$ 知 $a \in K_a$, 于是 $A = \bigcup_a K_a$. 设 $K_a \cap K_b \neq \emptyset$, 即 $\exists c \in K_a \cap K_b$, 对 $\forall x \in K_a$ 有 cRa, xRa , 因而 xRc . 又 cRb , 故 xRb , 即 $x \in K_b$, 从而得 $K_a \subseteq K_b$. 同样可得 $K_b \subseteq K_a$, 故 $K_a = K_b$, 亦即若 $K_a \neq K_b$, 则 $K_a \cap K_b = \emptyset$. 这样就证明了 $\{K_a\}$ 是 A 的分划.

反之, 设 $\{A_\alpha\}$ 是 A 的一个分划. 在 A 中定义关系 R ,

$$aRb, \quad \text{若 } \exists A_\alpha, \text{ 使 } a, b \in A_\alpha.$$

因 $A = \bigcup_\alpha A_\alpha$, 故对 $\forall a \in A, \exists A_\alpha$, 使 $a \in A_\alpha$, 因此 $a, a \in A_\alpha$, 即 aRa . 其次, 若 aRb , 即 $\exists A_\alpha$, 使 $a, b \in A_\alpha$. 自然 $b, a \in A_\alpha$, 故 bRa . 再次, 若 aRb, bRc , 即有 A_α, A_β , 使 $a, b \in A_\alpha$ 且 $b, c \in A_\beta$, 故 $b \in A_\alpha \cap A_\beta$. 由 $\{A_\alpha\}$ 为 A 的分划知 $A_\alpha = A_\beta$, 因而 aRc . 这样就证明了 R 是等价关系. 由 R 的定义知若 $a \in A_\alpha$, 则 a 所在的等价类 $K_a = A_\alpha$.

□

定义 1.8 (商集和自然映射)

设 R 是集合 A 的等价关系. 以关于 R 的等价类为元素的集合 $\{K_a\}$ 称为 A 对 R 的**商集合**或**商集**. 记为 A/R . 由

$$\pi(a) = K_a, \quad \forall a \in A$$

定义的 A 到 A/R 上的映射 π 称为 A 到 A/R 上的**自然映射**.



注 显然自然映射都是满射.

定理 1.2

设 $f: A \rightarrow B$ 是满映射. 在 A 中定义关系 R ,

$$aRb, \quad \text{若 } f(a) = f(b),$$

则 R 是 A 的等价关系. 又设 $\pi: A \rightarrow A/R$ 为自然映射, 则有 A/R 到 B 上的一一对应 g 满足

$$g\pi = f. \quad (1.1)$$

即图 1.1 是交换图.

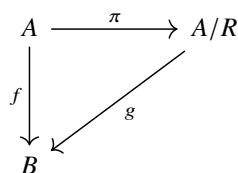


图 1.1

证明 考虑 $y \in B$ 的原像 $f^{-1}(y)$ 构成的子集族. 显然, $A = \bigcup_{y \in B} f^{-1}(y)$. 又若 $y, z \in B, f^{-1}(y) \cap f^{-1}(z) \neq \emptyset$, 即 $\exists a \in A$, 使 $f(a) = y, f(a) = z$, 即 $y = z$. 故 $f^{-1}(y) = f^{-1}(z)$, 从而 $\{f^{-1}(y)\}$ 是 A 的一个分划. 于是由定理 1.1 知, 在 A 中可定

义等价关系 $R: aRb$, 若 $\exists f^{-1}(y)$, 使 $a, b \in f^{-1}(y)$, 即 $f(a) = f(b)$. 由此知定理的第一部分成立.

定义 A/R 到 B 的映射 g ,

$$g(K_a) = f(a), \quad \forall a \in A.$$

注意到 A 中元素 a 所在等价类 $K_a = f^{-1}(f(a))$, 由于 $K_a = K_b$ 当且仅当 $f(a) = f(b)$, 故 g 是单射. 又 $f(A) = B$, 故 g 是满射. 因此 g 是一一对应. 由 π 的定义知式 (1.1) 成立.

□

定义 1.9 (同余关系和同余类)

设集合中 A 的二元运算, 记作乘法. 若 A 的一个等价关系 \sim 满足

$$\text{若 } a \sim b, c \sim d, \text{ 则 } ac \sim bd, \forall a, b, c, d \in A.$$

则称 \sim 为 A 的一个**同余关系**. $a \in A$ 的等价类 K_a 此时也称为 a 的**同余类**.

✿

例题 1.1

1. 设 $m \in \mathbf{Z}$ (所有整数的集合), $m \neq 0$. 在 \mathbf{Z} 中定义关系

$$a \sim b, \quad \text{若 } a \equiv b \pmod{m}.$$

易证 \sim 是等价关系且由 $a \equiv b \pmod{m}, c \equiv d \pmod{m}$ 可得 $a + c \equiv b + d \pmod{m}, ac \equiv bd \pmod{m}$. 因而 \sim 对于 \mathbf{Z} 中的加法与乘法都是同余关系.

2. 设 $\mathbf{P}[x]$ 是数域 \mathbf{P} 上一元多项式的集合. 设 $f(x) \in \mathbf{P}[x], f(x) \neq 0$. 在 $\mathbf{P}[x]$ 中定义关系 $\sim: g(x) \sim h(x)$, 若 $f(x) \mid (g(x) - h(x))$. 与第一问类似可证 \sim 对 $\mathbf{P}[x]$ 中的加法与乘法都是同余关系.
3. 以 $\mathbf{P}^{n \times n}$ 表示数域 \mathbf{P} 上所有 n 阶方阵的集合. 方阵的加法与乘法都是 $\mathbf{P}^{n \times n}$ 中的二元运算. 对 $A \in \mathbf{P}^{n \times n}$, 用 $\text{ent}_{ij} A, \text{row}_i A, \text{col}_j A$ 和 $\det A$ 分别表示 A 的第 i 行第 j 列元素、 A 的第 i 行、 A 的第 j 列和 A 的行列式. $\mathbf{P}^{n \times n}$ 中由 $\det A = \det B$ 确定的关系, 对乘法是同余关系, 但对加法除 $n = 1$ 的情形外不是同余关系.

定理 1.3

设集合 A 有二元运算乘法, \sim 是 A 的一个同余关系. 又 $\pi: A \rightarrow A/\sim$ 是自然映射, 则在商集合 A/\sim 中可定义二元运算

$$\pi(a)\pi(b) = \pi(ab), \quad \forall a, b \in A.$$

♡

证明 要证明这个二元运算的良好性, 只需证由 $\pi(a) = \pi(a_1), \pi(b) = \pi(b_1)$ 可得 $\pi(ab) = \pi(a_1 b_1)$, 其中 $a, b, a_1, b_1 \in A$. 事实上, 由 π 的定义知 $\pi(a) = \pi(a_1)$, 即 $a \sim a_1, \pi(b) = \pi(b_1)$, 即 $b \sim b_1$. 因 \sim 是同余关系, 故 $ab \sim a_1 b_1$, 所以 $\pi(ab) = \pi(a_1 b_1)$.

□

1.2 么半群 群

定义 1.10 ((么) 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

$$1a = a1 = a, \quad \forall a \in M, \quad (1.2)$$

则称 M 为**么半群**, 1 称为**么元素**或**么元**.

如果一个么半群 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**交换么半群** (或**交换半群**), 也简单地称 M (或 S) 为**可换的**.

对于交换么半群, 有时把二元运算记为加法, 此时么元素记为 0, 改称**零元素**或**零**.



例题 1.2

- (1) \mathbf{N} 对乘法是么半群, 对加法是半群而不是么半群. 非负整数集对加法与乘法均为么半群.
- (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, $M(X)$ 是一个么半群, id_X 是一个么元素. 当 $|X| \geq 2$ 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 \emptyset 也是 X 的一个子集, 则 $P(X)$ 对集合的并的运算是一个么半群, \emptyset 为么元素. 同样, $P(X)$ 对集合的交的运算是一个么半群, X 为么元素, 这两种么半群都是可换的.

命题 1.3

么半群中的么元素是唯一的.



证明 如果 1 与 $1'$ 都是么半群 M 的么元素, 则由条件 (1.2) 可知 $1 = 1'$.



定义 1.11 (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**左么元**, 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. 这时左么元改称**零元**, 以 0 表示; a 的左逆元改称 a 的**负元**, 记为 $-a$.



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

定理 1.4 (群的基本性质)

设 (G, \cdot) 是一个群, $a \in G$, 1 是 G 的左么元, 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. 1 也是 G 的**右么元**, 即 $a \cdot 1 = a (\forall a \in G)$, 故 1 为 G 的**么元**. 故 G 为么半群, 么元唯一.
4. 群运算满足**消去律**, 即

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

5. 若 $a, b \in G$, 则群中方程 $ax = b$ (或 $xa = b$) 的解存在且唯一.



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. 设 b 为 a 的逆元, 则有

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

4. 两边同乘 x^{-1} 即得.

5. 事实上, $x = a^{-1}b$ (或 $x = ba^{-1}$) 为解, 由性质 4 知解唯一.

□

定义 1.12

设 a 是群 G 的元素, 可定义 a 的**非正整数次乘幂**如下:

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

♣

定理 1.5

设 G 是一个群, 则对 $\forall m, n \in \mathbf{Z}, a, b \in G$ 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 $(ab)^m = a^m b^m$.

♡

证明

□

定义 1.13

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 $G = \{1, a_1, a_2, \dots, a_{n-1}\}$ 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	$a_1 a_2$		$a_1 a_{n-1}$
a_2	a_2	$a_2 a_1$	a_2^2		$a_2 a_{n-1}$
\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, 可定义半群与么半群的阶, 对于有限半群与么半群, 其运算也可列表给出.

♣

定义 1.14

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

♣

定理 1.6 (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 $\forall m, n \in \mathbf{Z}$ 且 $m \neq n$ 时, $a^m \neq a^n$.

2. 设 a 的阶为 d , 则

$$a^m = a^n \iff m \equiv n \pmod{d}. \quad (1.3)$$

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 $m-n \in \mathbf{N}$. 矛盾.

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

2. 设 a 的阶为 $d, m, n \in \mathbf{N}$, 由带余除法知, 一定能找到整数 t_1, t_2, r_1, r_2 , 使 $m = dt_1 + r_1 (0 \leq r_1 < d), n = dt_2 + r_2 (0 \leq r_2 < d)$. 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 (1.3) 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 1.15

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么半群可同样使用.

♣

定义 1.16

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 1.7

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 $H \neq \emptyset$ 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

□

命题 1.4

- (1) 若 H_1, H_2 是群 G 的子群, 则 $H_1 \cap H_2$ 也是 G 的子群.
 (2) 若 G 是一个群, 则 G 的任意子群的交 $\bigcap_{H < G} H$ 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.

◆

证明

- (1)
 (2)
 (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.

□

例题 1.3

1. 设 V 是数域 \mathbf{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 \mathbf{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

□

例题 1.4 设 $m \in \mathbf{Z}$, 则 $m\mathbf{Z} = \{mx | x \in \mathbf{Z}\}$ 是整数加法群 \mathbf{Z} 的子群. 并且 \mathbf{Z} 的任何子群都是这样的子群.

证明

□

定义 1.17 (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 $\{1, 2, \dots, n\}$ 的对称群.

例题 1.5 假定集合 $X = \{1, 2, \dots, n\}$, 记 S_n 为 X 的对称群, 设 $\sigma \in S_n$, 则 $\sigma(1), \sigma(2), \dots, \sigma(n)$ 是 $1, 2, \dots, n$ 的一个排列. 常用下面记法:

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

更一般地, 若 i_1, i_2, \dots, i_n 是 $1, 2, \dots, n$ 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

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

例题 1.6 设 n 个不定元 x_1, x_2, \dots, x_n 的多项式

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

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

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

则 $A_\sigma = \pm A$. 若 $A_\sigma = A$, 则称 σ 为偶置换, 并记 $\text{sgn}\sigma = 1$; 若 $A_\sigma = -A$, 则称 σ 为奇置换, 并记 $\text{sgn}\sigma = -1$, $\text{sgn}\sigma$ 称为 σ 的符号. 故有

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

令 A_n 为 S_n 中偶置换集合, 即

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

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

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

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

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

于是

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

又注意到 $\text{sgn}\tau^{-1} = \text{sgn}\tau, \forall \tau \in S_n$, 故

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

由此知 A_n 为 S_n 的子群. □

定义 1.18

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. ♣

定理 1.8

设 H 是群 G 的子群, 则由

$$aRb, \text{ 若 } a^{-1}b \in H$$

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 1.1 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) $aH \cap bH \neq \emptyset$;
- (2) $aH = bH$;
- (3) $a^{-1}b \in H$,

而且 $G = \bigcup_{a \in G} aH$ 为不相交的并.



证明



定义 1.19

设 H 是群 G 的子群, 由定理 1.8 定义 G 中的等价关系 R 为

$$aRb, \text{ 若 } a^{-1}b \in H.$$

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 1.7 设 V 是数域 \mathbf{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. $\forall \lambda \in \mathbf{P}, \lambda \neq 0$, 令 $D(\lambda) = \text{diag}(\lambda, 1, \dots, 1)$, 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 1.8 设 V 是 n 维 Euclid 空间. 由 $A \in O(V)$ 有 $\det A = \pm 1$, 令 $D(\lambda) = \text{diag}(\lambda, 1, \dots, 1)$, 于是

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

证明



例题 1.9 设 $m > 0, m\mathbf{Z}$ 为 \mathbf{Z} 的子群, 则有

$$\mathbf{Z} = \bigcup_{k=0}^{m-1} (k + m\mathbf{Z}), \quad [\mathbf{Z} : m\mathbf{Z}] = m.$$

证明

□

例 1.10 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, 则有

$$[G : 1] = [G : H][H : 1] \quad (1.4)$$

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 $h \rightarrow ah$ 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 (1.4) 成立.

□

推论 1.3

有限群 G 的任一元素 a 的阶是 G 的阶的因子, 即 $\text{ord } a \mid [G : 1]$.

♡

证明 令 $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$, 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 ($0 \leq r_n < d$), 使 $n = t_n d + r_n$, 于是 $a^n = a^{r_n}$. 因此 $\langle a \rangle$ 中至多只有 d 个元素 $1, a, \dots, a^{d-1}$.

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

□

定义 1.20 (循环群)

设 G 是一个群且 $a \in G$, 我们称

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

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.

♣

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 $H \triangleleft G$. 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 $1 \cdot H = H$.

♡

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 $(ac)^{-1}(bd) = c^{-1}a^{-1}ah_1d = h_2(d^{-1}h_1d) \in H$, 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 1.3 知 G/H 中的乘法为

$$aH \cdot bH = abH, \quad \forall a, b \in G. \quad (1.5)$$

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 1.4

若 G 为有限群, $H \triangleleft G$, 商群 G/H 的阶 $[G/H : H] = [G : H] = \frac{[G : 1]}{[H : 1]}$.

♥

证明 这是 Lagrange 定理的直接推论. 当 G 为无限群时, $[G/H : H] = [G : H]$ 仍然成立.

□

定理 1.11

设 H 是群 G 的子群, 则下列条件等价:

- (1) $H \triangleleft G$;
- (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 $H \triangleleft G$ 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 $g_1h_1g_2h_2 = g_1g_2h'_1h_2 \in g_1g_2H, g_1g_2h = g_1h'g_2 \cdot 1 \in g_1H \cdot g_2H$, 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 $H \triangleleft G$.

□

命题 1.5

- (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 $H \supseteq N, N \triangleleft G$, 则 $N \triangleleft H$.

♠

证明

(1)

(2) 由命题 1.4(3) 知 N 是 H 的子群. 又由 $N \triangleleft G$ 知

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

故 $N \triangleleft H$.

□

例题 1.11 为方便计, 将商群 G/H 中元素记为 $\bar{g} = gH$, 则

- (1) $SL(V) \triangleleft GL(V), GL(V)/SL(V) = \{\overline{D(\lambda)} | \lambda \neq 0\}$ 且 $\overline{D(\lambda)D(\mu)} = \overline{D(\lambda\mu)}$;
- (2) $SO(V) \triangleleft O(V), O(V)/SO(V) = \{\overline{D(1)}, \overline{D(-1)}\}$;
- (3) $m\mathbf{Z} \triangleleft \mathbf{Z}, \mathbf{Z}/m\mathbf{Z} = \mathbf{Z}_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$;
- (4) $A_n \triangleleft S_n, S_n/A_n = \{\bar{1}, \bar{\sigma} | \sigma \text{ 奇置换}\}$ 且

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

定义 1.21

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**.

若么半群 M 的子集 Q 对 M 的运算也是么半群且 M 的么元 $1 \in Q$, 则称 Q 为 M 的**子么半群**.

如果关系 \sim 是么半群 (或半群) 中的同余关系, 那么商集合对导出的运算也是么半群 (或半群), 称之为**商么半群** (或**商半群**).



1.4 环与域

定义 1.22 (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**.

**命题 1.6**

一切数域都是环.



证明

□

例题 1.12

- (1) \mathbf{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 $P[x_1, x_2, \dots, x_n]$ 对多项式的加法和乘法是环, 称为 P 上的 **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 $a_{ij} = \text{ent}_{ij}(\alpha)$. 由下面的两个关系:

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

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

定义的 $R^{n \times n}$ 加法与乘法使其成为一个环, 称为 R 上的 **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 1.12 (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) $\forall m, n \in \mathbf{Z}, a, b \in R,$

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

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

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

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

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

(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 1.23

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.
7. **体**: 非零元素集合对乘法构成群的环.
8. **域**: 交换的体, 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.

命题 1.7

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.

**证明**

□

例题 1.13 设 p 是一个素数. 于是 \mathbf{Z} 中关系 $a \equiv b \pmod{p}$ 对加法及乘法都是同余关系, 因而在 $\mathbf{Z}_p = \mathbf{Z}/p\mathbf{Z}$ 中有加法运算, 使 \mathbf{Z}_p 为 Abel 群, 而且在 \mathbf{Z}_p 中有乘法运算, 使 \mathbf{Z}_p 为交换幺半群. $\mathbf{Z}_p = \{0, 1, \dots, \overline{p-1}\}$. 又 $\forall \bar{a}, \bar{b}, \bar{c} \in \mathbf{Z}_p$ 有

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

即分配律成立. 故 \mathbf{Z}_p 是交换幺环. 又对 $a \in \mathbf{N}, a < p$, 由 p 为素数知有 $m, n \in \mathbf{Z}$, 使 $ma + np = 1$, 因而 $\bar{m} \cdot \bar{a} = \bar{1}$, 即

\mathbf{Z}_p 中每个非零元素可逆, 因而 \mathbf{Z}_p 是只含 p 个元素的域且非数域.

证明

□

例题 1.14 设 \mathbf{C} 为复数域. 考虑 $\mathbf{C}^{2 \times 2}$ 中子集

$$H = \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \mid \alpha, \beta \in \mathbf{C} \right\}.$$

证明 H 是体, 称 H 为 \mathbf{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 $\forall \alpha, \beta, \gamma, \delta \in \mathbf{C}$ 有

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

故 H 对矩阵乘法为么半群. 显然加法与乘法间有分配律, 故 H 为么环. 又若

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

则

$$\left| \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \right| = \alpha\bar{\alpha} + \beta\bar{\beta} > 0.$$

此时有

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

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

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

由 $AB \neq BA$, 故 H 不是域.

□

定义 1.24

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 1.13

- (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 $A \subseteq B$, 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)

□

定理 1.14

设 I 为环 R 的子环. 在 R 中定义关系 “ \sim ”,

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

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

$$(a + I) + (b + I) = (a + b) + I, \quad \forall a, b \in R, \quad (1.6)$$

$$(a + I) \cdot (b + I) = ab + I, \quad \forall a, b \in R. \quad (1.7)$$

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 1.5 知在 R/I 中有加法运算 (1.6) 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 (1.7) 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 1.5**

若 R 为交换环, 则 R/I 也是交换环.



证明

**推论 1.6**

若 R 为幺环, 则 R/I 也是幺环且 $1 + I$ 为幺元.



证明



例题 1.15 从定理 1.14 知 $m\mathbb{Z}$ 为 \mathbb{Z} 的理想, 故 $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ 对剩余类 $(\text{mod } m)$ 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 $m = m_1 m_2 (m_i \in \mathbb{Z}, |m_i| > 1, i = 1, 2)$, 则 \mathbb{Z}_m 有零因子 $\overline{m_1}, \overline{m_2}$.

例题 1.16 设 R 是一个环. 考虑 $R^{n \times n}$ 中子集

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

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

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

1.5 同态与同构

定义 1.25

设 G_1, G_2 是两个群 (或半群、么半群), 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 1.15

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 (或么半群). “ \sim ” 是 G 中一个同余关系, 则 G 到商半群 (或商么半群) 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 1.8

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 1.4(3) 知 N 也是 H 的子群, 故

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

例题 1.17

- (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 $f : f(\sigma) = \text{sgn} \sigma (\forall \sigma \in S_n)$, 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 \mathbf{R} 到正实数乘法群 $\mathbf{R}^+ = \{x \in \mathbf{R} | x > 0\}$ 的映射,

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

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

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

其中, A' 为 A 的转置, I_n 为 n 阶单位矩阵. 还有

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

证明

- 1.
- 2.
- 3.
- 4.
- 5.

6. 事实上, 在 V 中取定一组基 $\alpha_1, \alpha_2, \dots, \alpha_n$, 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 $A \rightarrow M(A)$ 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 1.16 (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 1.2);
- (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 $G_1 \cong G_3$.

♡

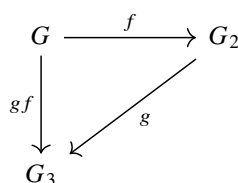


图 1.2

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 $f = \text{id}_G$); 若 $G_1 \cong G_2$, 则 $G_2 \cong G_1$ (若 $f: G_1 \rightarrow G_2$ 为同构映射, 则 $f^{-1}: G_2 \rightarrow G_1$ 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 1.26

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 1.9

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

$$L_a L_b = L_{ab}, \quad R_a R_b = R_{ba}, \quad L_1 = R_1 = \text{id}_G,$$

$$L_{a^{-1}} = L_a^{-1}, \quad R_{a^{-1}} = R_a^{-1}, \quad L_a R_b = R_b L_a, \quad \forall a, b \in G,$$

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 1.17 (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么半群也是适用的. 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, 但对么半群 G 仍有 $G \cong L_G$, 这时 L_G 是 $M(G)$ 的子么半群 ($M(G)$ 的定义见例题 1.2).

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 1.27

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 $\text{Aut}G$.

定理 1.18

设 G 是一个群, 则有

- (1) $\text{Aut}G$ 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 $\text{ad}g = L_g R_{g^{-1}}$ 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 $\text{Int}G$ (也记成 $\text{ad}G$) 是 $\text{Aut}G$ 的正规子群, 称为 G 的**内自同构群**;
- (4) $\text{ad} : g \rightarrow \text{ad}g$ 是群 G 到 $\text{Int}G$ 上的同态.

证明

- (1) 显然有 $\text{id}_G \in \text{Aut}G \subseteq S_G$, 任取 $\theta_1, \theta_2 \in \text{Aut}G$, 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 $\theta_1 \theta_2^{-1} \in \text{Aut}G$. 故 $\text{Aut}G$ 是群.

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

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

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

- (3) 对 $\forall g_1, g_2 \in G$, 有

$$\begin{aligned}(\text{ad}g_1)(\text{ad}g_2)^{-1} &= L_{g_1} R_{g_1^{-1}} (L_{g_2} R_{g_2^{-1}})^{-1} \\ &= L_{g_1} R_{g_1^{-1}} R_{g_2} L_{g_2^{-1}} = L_{g_1} L_{g_2^{-1}} R_{g_1^{-1}} R_{g_2} \\ &= L_{(g_1 g_2^{-1})} R_{(g_2 g_1^{-1})} = \text{ad}g_1 g_2^{-1}.\end{aligned}\tag{1.8}$$

故 $\text{Int}G$ 是 $\text{Aut}G$ 的子群.

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

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

因而

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

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

- (4) 在式 (1.8) 中, 取 $g_1 = 1$, 则有

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

一般由式 (1.8) 知

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

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

□

定义 1.28

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

□

定义 1.29

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 1.10

- (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 $R_1 \rightarrow R'$ 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 1.19

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 1.11

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

$$\mathcal{A} \rightarrow M(\mathcal{A}), \quad \forall \mathcal{A} \in \text{End}V$$

是 $\text{End}V$ 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 1.30

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 $\eta^2 = \text{id}_R$, 则称 η 为 R 的一个**对合**.

定理 1.20

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 $x \rightarrow x'$ 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 1.19 设 P 是一个数域, 在环 $P^{n \times n}$ 中定义映射 $\tau: A \rightarrow A'$, 则 τ 是 $P^{n \times n}$ 的对合.

证明

1.6 模

定义 1.31 (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: $(a, x) \rightarrow ax (a \in R, x \in M)$, 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 $(x, a) \rightarrow xa (a \in R, x \in M)$, 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 1.20 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 1.21 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

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

及 $R_+ \times R$ 到 R_+ 的映射

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

使 R_+ 变成一个 R 模, 因而 R 可看成它自身上的模.

证明

□

例题 1.22 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 $(f(\lambda), x) \rightarrow f(\mathcal{A})x, f(\lambda) \in R (x \in V)$, 使 V 成为一个左 R 模.

证明

□

例题 1.23 设 M 是一个 Abel 群, 运算为加法, 则 $\text{End}M$ 为 M 的自同态环, 并且 $\text{End}M \times M$ 到 M 的映射 $(\eta, x) \rightarrow \eta(x) (\eta \in \text{End}M, x \in M)$, 使 M 成为一个左 $\text{End}M$ 模.

证明

□

定理 1.21

设 M 是一个 R 模, 则

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

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

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

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

♥

证明

(1)

(2)

□

定义 1.32

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 $ax \in N,$

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 1.24 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 1.25 设 M 是一个 Abel 群, 其运算为加法. 映射

$$(m, x) \rightarrow mx, \quad m \in \mathbf{Z}, x \in M,$$

使 M 变成一个 \mathbf{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 1.12

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 1.26 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 1.22 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 1.22

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, \dots, N_r 之和

$$N_1 + N_2 + \dots + N_r = \{x_1 + x_2 + \dots + x_r \mid x_i \in N_i\}$$

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

$$Ry_1 + Ry_2 + \dots + Ry_k = \left\{ \sum_{i=1}^k a_i y_i \mid a_i \in R \right\}.$$

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.

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 1.23

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

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

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 $N \triangleleft M$. 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.

以下只要验证 R 模的 4 个定义条件. 这些验证不难.

□

定义 1.33

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 1.13

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 1.24

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

□

例题 1.27 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 1.25

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 1.3).
- (3) R 模之间的同构关系是等价关系.

♡

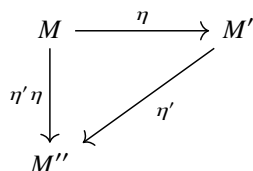


图 1.3

证明

- (1) 后者注意到 $\eta|_{M_1}$ 是 $M_1 \rightarrow M'$ 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 1.34

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 $\text{End}_R M$. 以 $\text{End} M$ 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 $\text{End}_R M \subseteq \text{End} M$. 另一方面, 可以验证在 $\text{End} M$ 中可定义加法与乘法使 $\text{End} M$ 是一个环.

定理 1.26

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

♡

证明 显然, $\text{id}_M \in \text{End}_R M$, 故 $\text{End}_R M \neq \emptyset$, 又若 $\eta_1, \eta_2 \in \text{End}_R M, x, y \in M, a \in R$, 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 $\eta_1 - \eta_2 \in \text{End}_R M$, 故 $\text{End}_R M$ 对加法成群. 又由同态性质知 $\eta_1 \eta_2 \in \text{End}_R M$, 由此可知 $\text{End}_R M$ 是 $\text{End} M$ 的子环.

□

例题 1.28 设 M 为 Abel 群, 于是 M 为 \mathbb{Z} 模. 则由例题??知 $\text{End}_{\mathbb{Z}} M = \text{End} M$.

证明

□

例题 1.29 设 R 是一个幺环, 则 R 作为左 R 模有 $\text{End}_R R = R_r$.

注 设 M 是一个左 R 模, 一般把 M 的模自同态环记为 ${}_R \text{End} M$. 若 M 是右 R 模, 则将 M 的模自同态环记为 $\text{End}_R M$. 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 $\text{End}_R M$ 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 $a_r \in \text{End}_R R$. 令 $R_r = \{a_r | a \in R\}$, 即有 $R_r \subseteq \text{End}_R R$. 现设 $\eta \in \text{End}_R R$, $\eta(1) = a$, 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 $\text{End}_R R = R_r$.

□

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

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

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

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

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

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

称为 f 的像.



例题 1.30

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 1.15), 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 1.19), 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, 则有 $\ker \pi = N$.

定理 1.27 (群的同态基本定理)

设 f 是群 G 到群 H 上的满同态, 则有下列结论:

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

$$f = \bar{f} \cdot \pi, \quad (1.9)$$

进而

$$G/\ker f \cong H = f(G).$$

如图 1.4 所示.



笔记

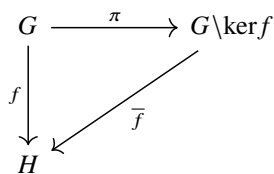


图 1.4

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 $\ker f \triangleleft G$.

- (2) 根据 f 是 G 到 H 上的满映射知 $H = f(G)$. 并且由定理 1.2 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 1.2 知有 $G/\ker f$ 到 H 的一一对应 \bar{f} , 使得 $\bar{f} \cdot \pi = f$, 又 $\forall x, y \in G$ 有

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

由此知 \bar{f} 是 $G/\ker f$ 到 H 上的群同构.

□

定理 1.28

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 $\Sigma \rightarrow \Gamma$ 的一一对应;
- (2) 若 $G_1 \triangleleft G, G_1 \supseteq K$, 则

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

若 $H_1 \triangleleft H$, 则

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

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

$$G/G_1 \cong H/f(G_1). \quad (1.10)$$

♡

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 $G \rightarrow H$ 上的满同态知 $f(G_1) = f(f^{-1}(H_1)) = H_1$, 由 H_1 的任意性知 $ff^{-1} = \text{id}_\Gamma$. 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 $f^{-1}f = \text{id}_\Sigma$.

综上所述知 f 是 $\Sigma \rightarrow \Gamma$ 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 $G_1 \triangleleft G$, 即 $G_1 \in \Sigma$ 且 $G_1 \triangleleft G$, 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 $f(G_1) \triangleleft H$.

反之, 若 $H_1 \triangleleft H$ 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 $f^{-1}(H_1) \triangleleft G$, 即结论 (2) 成立.

- (3) 设 $G_1 \in \Sigma$ 且 $G_1 \triangleleft G$. 由结论 (2) 的证明知 $f(G_1) \triangleleft H$. 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 $H/f(G_1)$ 的么元为 $f(G_1)$, 则知

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

最后一个等号是因为由 (1) 知 f 是 $\Sigma \rightarrow \Gamma$ 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 \bar{f} , 使得 $\pi' f = \bar{f} \cdot \pi$, 亦使图 1.5 为交换图, 即式 (1.10) 成立.

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ \pi \downarrow & \searrow \pi' f & \downarrow \pi' \\ G/G_1 & \xrightarrow{\bar{f}} & H/f(G_1) \end{array}$$

图 1.5

□

推论 1.7

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 $\Sigma \rightarrow \Gamma$ 的一一对应;
- (2) 若 $H \triangleleft G, H \supseteq N$, 则

$$\pi(H) \triangleleft G/N.$$

若 $H' \triangleleft G/N$, 则

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

- (3) 若 $H \triangleleft G, H \supseteq N$, 则

$$G/H \cong (G/N)/(H/N).$$

♡

证明 事实上, 由于自然同态必是满同态, 故只要在定理 1.28 中将 H 换成 G/N , f 换成 π , 即得本推论. 对于 (3), 由命题 1.8(1) 知 $\pi(H) = H/N$, 故我们有如下交换图.

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/N \\ \pi'' \downarrow & \searrow \pi' \pi & \downarrow \pi' \\ G/H & \xrightarrow{\bar{\pi}} & (G/N)/(H/N) \end{array}$$

图 1.6

□

定理 1.29

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

$$N \triangleleft HN = \pi^{-1}(\pi(H)). \quad (1.11)$$

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

(3)

$$HN/N \cong H/H \cap N. \quad (1.12)$$

♡

证明

(1) 显然, $HN \supseteq N$. 设 $h_i n_i \in HN (i = 1, 2)$, 则由 $N \triangleleft G$ 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 $N \triangleleft G$, 所以由命题 1.5(2) 知 $N \triangleleft HN$.

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

(3) 由 (1) 的结论及自然同态是满同态知 $\pi(HN) = \pi(\pi^{-1}(\pi(H))) = \pi(H)$. 又注意到 $\ker(\pi|_{HN}) = HN \cap N = N$, 故由群的同态基本定理知 $HN/N \cong \pi(H)$. 另有 $\pi(H) = \pi|_H(H)$, $\ker(\pi|_H) = N \cap H$, 故由群的同态基本定理知 $\pi(H) \cong H/H \cap N$, 即式 (1.12) 成立.

□

定理 1.30 (环的同态基本定理)

设 f 是环 R 到环 R' 上的满同态, 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 R' 上的环同构映射 \bar{f} , 使得

$$f = \bar{f} \cdot \pi. \quad (1.13)$$

♡

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) f 为环同态, 故也是加法群 R 到加法群 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 R' 上的同构 \bar{f} , 使 $f = \bar{f} \cdot \pi$.

另外, $\forall a, b \in R$ 有

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

因而 \bar{f} 也是环 $R/\ker f$ 到环 R' 上的环同构.

□

定理 1.31

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 $\Sigma \rightarrow \Gamma$ 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

$$R/I \cong R'/f(I). \quad (1.14)$$

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 $\Sigma \rightarrow \Gamma$ 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 1.28(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 $\Gamma \rightarrow \Sigma$ 上的良定义的映射.

对 $\forall H \in \Sigma, H' \in \Gamma$, 注意到 H 是 R 中包含 K 的加法子群, H' 是 R' 的加法子群, 由定理 1.28(1) 知 $f^{-1}f(H) = H, ff^{-1}(H') = H'$. 由 H 的任意性知 $f^{-1}f = \text{id}_\Sigma, ff^{-1} = \text{id}_\Gamma$. 故 f 是 $\Sigma \rightarrow \Gamma$ 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 1.10(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 $\Sigma \rightarrow \Gamma$ 的一一对应. 于是由环的同态基本定理得式 (1.14) 成立. □

推论 1.8

设 A, B 均为环 R 的理想且 $A \subseteq B$, 则有

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

证明 事实上, 只要在定理 1.31 中取 $R' = R/A, f$ 为 R 到 R/A 的自然同态, 并且由定理 1.11(1) 知 $\pi(B) = B/A$, 因此即得本推论. □

定理 1.32

设 H 为环 R 的子环, K 为 R 的理想, 则有 $H+K$ 为 R 的子环, $H \cap K$ 为 H 的理想且

$$(H+K)/K \cong H/(H \cap K). \quad (1.15)$$

证明 设 π 是环 R 到商环 R/K 上的自然同态. 因 H 是 R 的子环, 故 $\pi(H)$ 是 R/K 的子环. 与定理 1.29 一样有

$H + K = \pi^{-1}(\pi(H))$ 且 K 是 $H + K$ 的理想. 又根据定理 1.29 知 $H + K$ 是 R 的子环且 $\pi(H) \cong (H + K)/K$, 又 $\pi|_H$ 是 H 到 $\pi(H)$ 上的同态且 $\ker(\pi|_H) = H \cap K$, 因而 $\pi(H) \cong H/(H \cap K)$, 即得式(1.15). \square

定理 1.33 (模同态的基本定理)

设 M, M' 都是幺环 R 上的模, f 是 M 到 M' 上的模同态, M 中包含 N 的子模集合为 Σ , M' 中子模集合为 Γ , 则有以下结论:

(1) $\ker f = N$ 是 M 的子模. 若 π 是 M 到 M/N 上的自然模同态, 则有 M/N 到 M' 的模同构 \bar{f} , 使得

$$\bar{f} \cdot \pi = f \quad (1.16)$$

(2) f 是 $\Sigma \rightarrow \Gamma$ 的一一对应.

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

$$M/M_1 \cong M'/f(M_1) \quad (1.17)$$

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. 由群的同态基本定理知有加法群 M/N 到加法群 M' 上的同构 \bar{f} , 使 $\bar{f} \cdot \pi = f$. 现只需证 \bar{f} 是模同构. 又设 $a \in R, x \in M$, 于是有

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

即 \bar{f} 为模同构. 故定理结论 (1) 成立.

(2) 若 M_1 为 M 的子模, 则由定理 1.25(1) 知 $f(M_1)$ 为 M' 的子模. 故 f 是 $\Sigma \rightarrow \Gamma$ 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. 从而由群的同态基本定理知 $f^{-1}(M'_1)$ 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 $f^{-1}(M'_1)$ 是 M 的子模. 故 f^{-1} 可视为 $\Gamma \rightarrow \Sigma$ 上的良定义的映射. 结论 (2) 成立.

(3) 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

$$\ker(\pi'f) = M_1.$$

故由结论 (1) 可知式(1.17)成立. \square

推论 1.9

设 M_1, N 都是 R 模 M 的子模, 而且 $M_1 \supseteq N$, 则 M/M_1 与 $(M/N)/(M_1/N)$ 是模同构. \heartsuit

证明 事实上, 只要在模同态的基本定理中取 $M' = M/N, f$ 为 M 到 $M' = M/N$ 的自然同态, 即得本推论. \square

定理 1.34

设 H, N 为 R 模 M 的子模, 则

$$(H + N)/N \cong H/(H \cap N) \quad (1.18)$$

证明 设 π 为 M 到 M/N 的自然同态, 于是有 $\pi(H + N) = \pi(H)$, 因而

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

由 $\ker(\pi|_{H+N}) = N, \ker(\pi|_H) = H \cap N$, 即得式(1.18)成立. \square