抽象代数

作者: 实空
组织: 无
时间:December 22, 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 基础概念 **1**
1.1 二元运算 . . . 1
1.2 幺半群和群 . . . 2
1.3 子群与商群 . . . 8
1.4 环与域 . . . 20
1.5 模 . . . 29
1.6 同态与同构 . . . 33
1.7 同态基本定理 . . . 40
1.8 循环群 . . . 49

第 2 章 群 **58**
2.1 群的生成组 . . . 58
2.2 群集合上的作用 . . . 68
2.3 Sylow 子群 . . . 78
2.4 有限单群 . . . 84
2.5 群的直积 . . . 86
2.6 可解群和幂零群 . . . 95
2.7 Jordan-Hölder 定理 . . . 106
2.8 自由幺半群与自由群 . . . 111
2.9 点群 . . . 117

第 3 章 环 **126**
3.1 分式域 . . . 126
3.2 多项式环 . . . 129
3.3 对称多项式 . . . 137
3.4 唯一析因环 (唯一分解整环) . . . 143
3.5 主理想整环与 Euclid 环 . . . 154
3.6 域上一元多项式 . . . 158
3.7 唯一析因环的多项式环 . . . 165
3.8 素理想与极大理想 . . . 169

第 4 章 域 **173**
4.1 域的单扩张 . . . 173

参考文献 **179**

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 $(ab)c = a(bc)(\forall a, b, c \in G)$, 也即 G 是半群;

(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.

例题 1.2 令 Ω 是任意一个集合,G 是一个群,G^Ω 是 Ω 到 G 的所有映射的集合. 对任意两个映射 $f, g \in G^\Omega$, 定义乘积 fg 是这样的映射: 对任意 $a \in \Omega$, $(fg)(a) = f(a)g(a)$. 则 G^Ω 是群, 并且这个群 G 为 Abel 群当且仅当 G 是 Abel 群.

证明 易知上述乘法有结合律,$1 \in G^\Omega$ 是其单位元, 其中 $1(a) = 1_G$, $\forall\, a \in \Omega(1_G$ 表示群 G 的单位元); 任一元 $f \in G^\Omega$ 有逆元 f^{-1}, 其中 $f^{-1}(a) := (f(a))^{-1}$, $\forall\, a \in \Omega$. 故 G^Ω 成为群.

显然群 G 为 Abel 群当且仅当 G 是 Abel 群.

□

例题 1.3 b 是含幺半群 G 中的元 a 的逆元当且仅当成立 $aba = a, ab^2a = 1$.

证明 设 b 是 a 的逆元, 显然有 $aba = a$ 和 $ab^2a = 1$. 反之, 若 $aba = a, ab^2a = 1$, 则

$$ab = ab(ab^2a) = ab^2a = 1, \quad ba = (ab^2a)ba = ab^2a = 1.$$

即 b 是 a 的逆元.

□

例题 1.4

(1) 令 G 是所有秩不大于 r 的 $n \times n$ 复方阵的集合, 则 G 在矩阵乘法下构成一个半群, 并且当 $r < n$ 时, 它不是一个含幺半群; 当 $r = n$ 时, 它是一个含幺半群, 但不是群.

(2) 整数集 $\mathbb{Z}$ 对于乘法成为一个含幺半群, 但不是群.

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

$$(a_1 a_2 \cdots a_r)^{-1} = a_r^{-1} a_{r-1}^{-1} \cdots a_1^{-1}.$$

(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

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

♡

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

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

其余各式显然.

(3) 只需注意到 $(a_1 a_2 \cdots a_r)(a_r^{-1} a_{r-1}^{-1} \cdots a_1^{-1}) = 1$ 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.

□

定理 1.3

设 $(G,\cdot)$ 是半群, 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, 即对 $\forall a,b\in G$, 群中方程 $ax=b$ 与 $xa=b$ 的解都存在且唯一.

♡

证明 **必要性**: 事实上, $x=a^{-1}b$ 和 $x=ba^{-1}$ 分别为两个方程的解, 由定理 1.2(5)知解唯一.

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.

□

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 1.4

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

♠

证明 证明是显然的.

□

定理 1.5

(1) 设 G 是一个有限半群, 则 G 是群的充要条件是在 G 内左右消去律均成立, 即由 $ax = ay$ 或 $xa = ya$ 可推出 $x = y$.

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

(3) 一个具有乘法运算 (对乘法封闭) 的非空集合 G, 则 G 是一个群的充要条件是 G 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 $aa' = e$).

♡

证明

(1) 必要性由定理 1.2(5)立得, 下证充分性. 设 $G = \{a_1, \cdots, a_n\}$, 由消去律知

$$\{a_1a_i, \cdots, a_na_i\} = G = \{a_ia_1, \cdots, a_ia_n\},$$

$\forall a_i \in G$. 故存在 $e \in G$, 使得 $a_i = ea_i$.

于是对于任一 $a_j \in G$, 有 $a_k \in G$ 使得 $a_j = a_ia_k$. 从而

$$ea_j = ea_ia_k = a_ia_k = a_j.$$

这表明 e 是左单位元, 又因为 $e \in G = Ga_j$, 故 a_j 有左逆元. 由此即知 G 是群.

(2) 必要性由定理 1.2立得, 下证充分性. 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.

(3) 必要性由定理 1.2立得, 下证充分性. 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.

□

命题 1.5

设 G 是群.

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

(2) G 是 Abel 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 1.5 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.

□

例题 1.6 在偶数阶群 G 中, 方程 $x^2 = 1$ 总有偶数个解.

证明 注意到若 $g^2 \neq 1$, 则 $(g^{-1})^2 \neq 1$ 且 $g \neq g^{-1}$. 因此 G 中满足 $x^2 \neq 1$ 的元 x 是成对出现的. 从而 G 中满足 $x^2 \neq 1$ 的元 x 有偶数个. 因此在偶数阶群 G 中, 方程 $x^2 = 1$ 总有偶数个解.

□

例题 1.7 令 G 是 n 阶有限群, $a_1, a_2, \cdots, a_n$ 是群 G 的任意 n 个元, 不一定两两不同. 试证存在整数 p 和 q, $1 \leqslant p \leqslant q \leqslant n$, 使得 $a_pa_{p+1}\cdots a_q = 1$.

证明 令 $S = \{a_1, a_1a_2, \cdots, a_1a_2\cdots a_n\}$. 若 $1 \in S$, 则结论已得证. 若 $1 \notin S$, 因 $|G| = n$, 故 S 中至少有两个元是相等的. 设 $a_1\cdots a_i = a_1\cdots a_ia_{i+1}\cdots a_j$, 则

$$a_{i+1}\cdots a_j = 1.$$

□

例题 1.8 设 a, b 是群 G 的两个元, 满足 $aba = ba^2b$, $a^3 = 1$, $b^{2n-1} = 1$. 试证 $b = 1$.

笔记 注意到 $b = 1$ 等价于 a, b 可交换, 故只需证明 a, b 可交换. 再利用条件和数学归纳法证明即可.

证明 由题设条件得

$$ab^2a = aba^3ba = (aba)a^2ba = (ba^2b)a^2ba = ba^2(ba^2b)a = ba^2(aba)a = b^2a^2.$$

故 $ab^2 = b^2a$. 设 $ab^{2^r} = b^{2^r}a$, 则 $ab^{2^{r+1}} = ab^{2^r}b^2 = b^{2^r}ab^2 = b^{2^r}b^2a = b^{2^{r+1}}a$. 因此对任一正整数 k 有 $ab^{2^k} = b^{2^k}a$. 特别地, 取 $k = n$ 得到 $ab^{2^n} = b^{2^n}a$. 因为 $b^{2n-1} = 1$, 所以 $b^{2n} = b$, 从而 $ab = ba$. 于是 $ba^2 = aba = ba^2b$. 故 $b = 1$.

□

例题 1.9 设群 G 的元 a_1, a_2, b_1, b_2 满足

$$a_1b_1 = a_2b_2 = b_1a_1 = b_2a_2, \quad a_1^m = a_2^m = b_1^n = b_2^n = 1,$$

其中 m 和 n 是互素的正整数. 则 $a_1 = a_2$, $b_1 = b_2$.

证明 设 k, l 是整数使得 $km + ln = 1$. 由 $a_1b_1 = a_2b_2$ 知

$$(a_1b_1)^{km} = (a_2b_2)^{km}.$$

因 $a_1b_1 = b_1a_1$, $a_2b_2 = b_2a_2$, $a_1^m = 1 = a_2^m$, 故

$$(a_1b_1)^{km} = a_1^{km}b_1^{km} = b_1^{km}, \quad (a_2b_2)^{km} = a_2^{km}b_2^{km} = b_2^{km}.$$

从而有 $b_1^{km} = b_2^{km}$. 而 $b_1^{ln} = b_2^{ln} = 1$, 故 $b_1 = b_1^{km+ln} = b_2^{km+ln} = b_2$. 同理可证 $a_1 = a_2$.

□

1.3 子群与商群

定义 1.9

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 1.6

设 H 是有限集,$\{a\}$ 为单点集, 则

$$|H| = |aH| = |Ha| = |aHa| = |HaH|.$$

♠

证明 令

$$\varphi : H \longrightarrow aH,$$
$$h \longmapsto ah, \quad \forall h \in H.$$

容易验证 φ 是 H 到 aH 的双射. 故 $|H| = |aH|$. 其他同理可证.

□

定义 1.10

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 $H < G$ 或 $H \leqslant G$.

♣

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**.

定义 1.11

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 1.6

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) 对 $\forall a, b \in H$, 有 $ab \in H, a^{-1} \in H$.

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

(5) 对 $a, b \in H$, 有 $a^{-1}b \in H$.

♡

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 $ab^{-1}, a^{-1}b \in H$.

(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.

(5) $\Rightarrow$ (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 $a^{-1} \in H$ 得 $ab = (a^{-1})^{-1}b \in H$. 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.

□

定理 1.7

设 A, B, C, H 是群 G 的非空子集,$g, a, b \in G$, 则

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

(2) $gA = gB$或$Ag = Bg \iff A = B$.

(3) H 是 G 的子群 $\iff HH = H, H^{-1} = H \iff H^{-1}H = H$.

(4) $ab \in H \iff a \in Hb^{-1} \iff b \in a^{-1}H$.

(5) $x \in gH \iff x^{-1} \in H^{-1}g^{-1}, x \in Hg \iff x^{-1} \in g^{-1}H^{-1}, x \in HgK \iff x^{-1} \in K^{-1}g^{-1}H^{-1}$.

♡

证明

(1)

(2)

(3)

(4) 只需注意到 $ab \in H \iff ab = h(h \in H) \iff a = hb^{-1} \in Hb^{-1} \iff b \in a^{-1}H$.

(5)

□

命题 1.7

(1) 设 H 是群 G 的非空有限子集, 则 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.

(5) 设 A 和 B 是有限群 G 的两个非空子集. 若 $|A| + |B| > |G|$, 则 $G = AB$.

♠

注 在这个命题 1.7(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 $1 \in H_i (\forall i \in I)$, 所以 $1 \in \bigcap_{i \in I} H_i$, 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 $\bigcap_{i \in I} H_i$ 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.

(5) $\forall ab \in AB$, 则 $a, b \in G$, 由 G 是群知 $ab \in G$. 故 $AB \subseteq G$. $\forall g \in G$, $|A^{-1}g| = |A|$. 因 $|A| + |B| > |G|$, 故 $A^{-1}g \cap B \neq \varnothing$, 于是有 $a \in A, b \in B$ 使得 $b = a^{-1}g$, 即 $g = ab$. 这表明 $G \subseteq AB$. 故 $G = AB$.

□

例题 1.10 设 A, B 是群 G 的两个子群且 $G = AB$. 如果子群 C 包含 A, 则 $C = A(B \cap C)$.

证明 设 $c \in C$, 由 $C \subseteq G = AB$ 知存在 $a \in A, b \in B$, 使得 $c = ab$. 从而由 $C < G$ 知 $b = a^{-1}c \in C$, 故 $b \in B \cap C$. 因此 $c = ab \in A(B \cap C)$. 于是 $C \subseteq A(B \cap C)$. 又设 $a_1 b_1 \in A(B \cap C)$, 则 $a_1 \in A \subseteq C, b_1 \in C$. 由 $C < G$ 知 $a_1 b_1 \in C$. 故 $C \supseteq A(B \cap C)$. 综上 $C = A(B \cap C)$.

□

定理 1.8

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 1.12

设 H, K 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**. 集合 HaK 称为以 a 为代表元的 H, K 的**双陪集**.

♣

定理 1.9

设 H, K 是群 G 的非空子集. 则

(1) 由

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

所确定的 G 中的关系 R 是一个等价关系的充要条件是 H 是 G 的子群. 并且当 H 是 G 的子群时, g

所在的等价类为 gH, 故 H 的左陪集族 $\{gH : g \in G\}$(集合无相同元素) 是 G 的一个分划. 即

$$G = \bigsqcup_{g\in G} gH,$$

其中 a 取遍不同 H 的左陪集的代表元.

(2) 由

$$aRb \iff ab^{-1} \in H$$

所确定的 G 中的关系 R 是一个等价关系的充要条件是 H 是 G 的子群. 并且当 H 是 G 的子群时, g 所在的等价类为 Hg, 故 H 的右陪集族 $\{Hg : g \in G\}$(集合无相同元素) 是 G 的一个分划. 即

$$G = \bigsqcup_{g\in G} Hg,$$

其中 g 取遍不同 H 的右陪集的代表元.

(3) 由

$$xRy \iff x \in HyK$$

所确定的 G 中的关系 R 是一个等价关系的充要条件是 H, K 是 G 的子群. 并且当 H, K 是 G 的子群时, g 所在的等价类为 HgK, 故 H 的右陪集族 $\{HgK : g \in G\}$(集合无相同元素) 是 G 的一个分划. 即

$$G = \bigsqcup_{g\in G} HgK,$$

其中 g 取遍不同 H, K 的双陪集的代表元.

♡

证明

(1) **充分性**: 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

$$gRx \iff g^{-1}x \in H \iff x = g(g^{-1}x) \in gH$$

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

必要性: 由等价关系的定义和定理 1.6是显然的.

(2) **充分性**: 由 $aa^{-1} \in H$ 知 $aRa(\forall a \in G)$. 又设 aRb, 即 $ab^{-1} \in H$, 故 $(ab^{-1})^{-1} = ba^{-1} \in H$, 即 bRa. 再设 aRb, cRb, 即 $ab^{-1}, cb^{-1} \in H$, 故 $ac^{-1} = (ab^{-1})(bc^{-1}) \in H$, 即 aRc. 这样知 R 是等价关系. 又由

$$xRg \iff xg^{-1} \in H \iff x = (xg^{-1})g \in Hg$$

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

必要性: 由等价关系的定义和定理 1.6是显然的.

(3) **充分性**: 对 $\forall x \in G$, 由 $x = 1 \cdot x \cdot 1 \in HxK$ 知 xRx. 设 $x, y \in G$ 且 xRy, 则 $x \in HyK$, 于是存在 $h \in H, k \in K$, 使得 $x = hyk$. 从而

$$y = h^{-1}xk^{-1} \in HxK \Longrightarrow yRx.$$

又设 $x, y, z \in G$ 且 xRy, yRz, 则 $x \in HyK, y \in HzK$, 于是存在 $h_1, h_2 \in H, k_1, k_2 \in K$, 使得

$$x = h_1yk_1 = h_1h_2zk_1k_2 \in HzK \Longrightarrow xRz.$$

综上可知 R 是等价关系. 又由

$$gRx \Longleftrightarrow g \in HxK \Longleftrightarrow g = hxk\,(h \in H, k \in K) \Longleftrightarrow x = h^{-1}gk^{-1} \in HgK.$$

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

必要性: 由等价关系的定义和定理 1.6是显然的.

□

定理 1.10

设 A, B, H 是群 G 的非空子群,$a, b \in G$, 则

(1) $a \in aH$.

(2) $aH = H$ 的充分必要条件是 $a \in H$.

(3) aH 为子群的充分必要条件是 $a \in H$.

(4) $aH = bH \iff a^{-1}b \in H \iff b^{-1}a \in H \iff aH \cap bH \neq \varnothing$;

$Ha = Hb \iff ab^{-1} \in H \iff ba^{-1} \in H \iff Ha \cap Hb \neq \varnothing$.

(5) AB 也是群 G 的子群的充分必要条件是 $AB = BA$.

♡

证明

(1) 只需注意到 $a = ae \in aH$.

(2) 如果 $aH = H$, 因 $a \in aH$, 所以 $a \in H$.

反之, 如果 $a \in H$, 则 $a^{-1} \in H$. 从而

$$aH \subseteq H \cdot H = H, \quad H = (aa^{-1})H = a(a^{-1}H) \subseteq aH,$$

所以 $aH = H$.

(3) 设 aH 为子群. 因为 $a \in aH$, 所以 $a^{-1} \in aH$, 于是 $e = aa^{-1} \in aH$. 从而存在 $h \in H$, 使 $e = ah$. 所以 $a = eh^{-1} = h^{-1} \in H$.

另一方面, 如果 $a \in H$, 则 $aH = H$ 为子群.

(4) 如果 $aH = bH$, 则

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

从而由定理 1.10(2)知,$a^{-1}b \in H$.

反之, 如果 $a^{-1}b \in H$, 则又由定理 1.10(2)得 $a^{-1}bH = H$, 于是

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

故 $aH = bH \iff a^{-1}b \in H$. 交换 a, b 位置即得 $bH = aH \iff b^{-1}a \in H$.

若 $aH = bH$, 则显然有 $aH \cap bH \neq \varnothing$. 假设 $aH \cap bH \neq \varnothing$. 任取 $g \in aH \cap bH$, 则存在 $h_1, h_2 \in H$, 使

$$ah_1 = g = bh_2.$$

从而

$$aH = a(h_1H) = (ah_1)H = (bh_2)H = b(h_2H) = bH.$$

故 $aH = bH \iff aH \cap bH \neq \varnothing$.

$Ha = Hb$ 的等价条件同理可证.

(5) **必要性**: 设 AB 为 G 的子群. 对任意的 $ab \in AB$, 其中 $a \in A, b \in B$, 有 $(ab)^{-1} \in AB$. 因而存在 $a_1 \in A, b_1 \in B$, 使 $a_1b_1 = (ab)^{-1}$. 从而

$$ab = (a_1b_1)^{-1} = b_1^{-1}a_1^{-1} \in BA,$$

所以

$$AB \subseteq BA.$$

反之, 对任意的 $ba \in BA$, 其中 $b \in B, a \in A$, 有 $(ba)^{-1} = a^{-1}b^{-1} \in AB$. 于是

$$ba = (a^{-1}b^{-1})^{-1} \in AB,$$

所以

$$BA \subseteq AB.$$

这就证明了 $AB = BA$.

充分性: 对任意的 $a_1b_1, a_2b_2 \in AB$, 其中 $a_i \in A, b_i \in B$ $(i = 1, 2)$, 由于 $AB = BA$, 因此由定理 1.7(1)和定理 1.7(3)有

$$a_1b_1(a_2b_2)^{-1} = a_1b_1b_2^{-1}a_2^{-1} = a_1(b_1b_2^{-1})a_2^{-1} \in ABA = A(BA) = A(AB) = (AA)B = AB,$$

由此知 AB 是 G 的子群.

□

定义 1.13

设 H, K 是群 G 的子群.

(1) 由定理 1.9(1)定义 G 中的等价关系 R 为

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

将 G 对等价关系 R 的商集合, 即以左陪集 gH, $g \in G$ 为元素的集合记为 $G/H = \{gH : g \in G\}$, 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 $[G : H]$.

这个等价关系 R 的完全代表系就称为关于 H 的**左陪集代表元系**或**左陪集代表系**. 显然左陪集代表系的阶就是 $[G : H]$.

(2) 由定理 1.9(2)定义 G 中的等价关系 R 为

$$aRb \iff ab^{-1} \in H.$$

将 G 对等价关系 R 的商集合, 即以右陪集 Hg, $g \in G$ 为元素的集合记为 $G/H = \{Hg : g \in G\}$, 称为 G 对 H 的**右陪集空间**.

这个等价关系 R 的完全代表系就称为关于 H 的**右陪集代表元系**或**右陪集代表系**. 显然右陪集代表系的阶就是 $[G : H]$.

(3) 由定理 1.9(3)定义 G 中的等价关系 R 为

$$xRy \iff x \in HyK.$$

将 G 对等价关系 R 的商集合, 即以双陪集 HgK, $g \in G$ 为元素的集合记为 $G/R = \{HgK : g \in G\}$, 称为 G 对 H 的**双陪集空间**.

这个等价关系 R 的完全代表系就称为关于 (H, K)– **双陪集代表元系**或**双陪集代表系**. 显然双陪集代表系的阶就是 $|G/R|$.

♣

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 1.11 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 1.12 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

□

定理 1.11

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 $\dfrac{G}{H}$. 并且 H 为 G/H 的幺元,aH 的逆元为 $a^{-1}H$.

♡

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

$$aH \cdot bH = abH, \quad \forall a, b \in G. \tag{1.2}$$

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.

□

定义 1.14 (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

□

定理 1.13

设 H 是群 G 的子群, 则下列条件等价:

(1) $H \lhd G$;

(2) 对 $\forall a, b \in G$, 如果 $ab \in H$, 则 $ba \in H$;

(3) $ghg^{-1} \in H, \forall g \in G, h \in H \iff gHg^{-1} \subseteq H, \forall g \in G$;

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

(5) $gH = Hg, \forall g \in G \iff GH = HG$;

(6) $g_1 H g_2 H = g_1 g_2 H, \forall g_1, g_2 \in G$.

♡

注 由这个定理 1.13(4)可知**一个群的任意正规子群都是 Abel 群.**

证明 (1) $\Rightarrow$ (2). 设 H 是 G 的正规子群, 则对任意的 $a,b\in G$, 如果 $ab\in H$, 则

$$ba=b(ab)b^{-1}\in H.$$

(2) $\Rightarrow$ (3). 对 $\forall a,b\in G$, 如果由 $ab\in H$, 可推出 $ba\in H$, 则对任意的 $a\in G, h\in H$, 由于 $a^{-1}(ah)=h\in H$, 因此

$$aha^{-1}=(ah)a^{-1}\in H,$$

(3) $\Rightarrow$ (4). 对 $\forall g\in G$, 由 $gHg^{-1}\subseteq H$ 知, 对 $\forall h\in H$, 有 $g^{-1}hg=\left(g^{-1}\right)^{-1}hg^{-1}\in H$. 从而 $h=g\left(g^{-1}hg\right)g^{-1}\in gHg^{-1}$. 故由 h 的任意性知 $H\subseteq gHg^{-1}$. 因此 $gHg^{-1}=H,\forall g\in G$.

(4) $\Rightarrow$ (5). $\forall g\in G, h\in H$ 有 $gh=ghg^{-1}g\in Hg, hg=gg^{-1}hg\in gH$, 故 $gH=Hg$.

(5) $\Rightarrow$ (6). 设 $g_1,g_2\in G, h_1,h_2,h\in H$. 由 $gH=Hg$ 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 $g_1H\cdot g_2H=g_1g_2H$.

(6) $\Rightarrow$ (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 1.8

(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) 设 H 和 N 分别是群 G 的子群和正规子群. 证明:HN 是 G 的子群.

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

(5) 设 G 是一个群, 且 $N_1,N_2,\cdots,N_k\lhd G$, 则 $N_1N_2\cdots N_k\lhd G$.

(6) 设 G 是一个群,$N_1,N_2,\cdots N_k\lhd G$, 且 $N_i\cap\prod\limits_{j=1}^{i-1}N_j=\{1\}(i\neq j)$, 则对 $\forall i,j\in\{1,2,\cdots,k\}$, 有

$$n_in_j=n_jn_i,\ \forall n_i\in N_i,n_j\in N_j.$$

并且

$$N_j\subseteq C_G(N_i)\triangleq\{g\in G\mid gn_i=n_ig,\forall n_i\in N_i\},\ \forall i,j\in\{1,2,\cdots,k\}.$$

♠

证明

(1) 因为

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

所以 H 是 G 的正规子群.

对 $\forall g_1H,g_2H\in G/H$, 由定理 1.13(6)有

$$g_1Hg_2H=g_1g_2H=g_2g_1H=g_2Hg_1H.$$

故 G/H 也是 Abel 群.

(2) 由命题 1.7(3)知 N 是 H 的子群. 又由 $N\lhd G$ 知

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

故 $N\lhd H$.

(3) 由于 N 是 G 的正规子群, 因此对任意的 $h\in H$, 有 $hN=Nh$. 由此推出,$HN=NH$, 从而由定理 1.10(5)知,HN 为 G 的子群.

(4) 设 I 为任意指标集,$H_i\lhd G,\forall i\in I$. 则对 $\forall g\in G$, 有

$$gH_ig^{-1}\subseteq H_i,\quad\forall i\in I.$$

对 $\forall h \in \bigcap\limits_{i\in I} H_i$, 有 $h \in H_i, \forall i \in I$. 从而由上式可得

$$ghg^{-1} \in H_i, \quad \forall i \in I \Longrightarrow ghg^{-1} \in \bigcap_{i\in I} H_i.$$

进而 $g\bigcap\limits_{i\in I} H_i g^{-1} \subseteq \bigcap\limits_{i\in I} H_i$. 故由定理 1.13(2)知 $\bigcap\limits_{i\in I} H_i \lhd G$.

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

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

于是对 $\forall n_1 n_2 \cdots n_k \in N_1 N_2 \cdots N_k, g \in G$, 有

$$g(n_1 n_2 \cdots n_k) g^{-1} = \left(gn_1 g^{-1}\right)\left(gn_2 g^{-1}\right) \cdots \left(gn_k g^{-1}\right) \in N_1 N_2 \cdots N_k.$$

故 $N_1 N_2 \cdots N_k \lhd G$.

(6) 设 $n_i \in N_i, n_j \in N_j$, 不妨设 $i < j$, 则

$$n_i n_j n_i^{-1} n_j^{-1} = n_i(n_j n_i^{-1} n_j^{-1}) \in N_i \subseteq N_1 N_2 \cdots N_{j-1};$$

$$n_i n_j n_i^{-1} n_j^{-1} = (n_i n_j n_i^{-1}) n_j^{-1} \in N_j,$$

所以

$$n_i n_j n_i^{-1} n_j^{-1} \in (N_1 N_2 \cdots N_{j-1}) \cap N_j = \{1\},$$

从而 $n_i n_j n_i^{-1} n_j^{-1} = 1$, 由此得 $n_i n_j = n_j n_i$. 进而

$$n_j \in C_G(N_i),$$

再由 n_j 的任意性知

$$N_j \subseteq C_G(N_i).$$

再由 i, j 的任意性知结论成立.

□

例题 1.13 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

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

(4) 对任意的 $a \in G$, 由已知条件知, 存在 $b \in G$, 使 $aH = Hb$, 则 $a \in aH = Hb$, 从而 $a \in Ha \cap Hb$, 即 $Ha \cap Hb$ 非空, 因此 $Ha = Hb$, 于是 $aH = Ha$. 所以由定理 1.13知 H 是 G 的正规子群.

证明

□

例题 1.14 令 G 是 n 阶有限群, S 是 G 的一个子集, $|S| > \dfrac{n}{2}$. 试证对任意 $g \in G$, 存在 $a, b \in S$ 使得 $g = ab$.

证明 由命题 1.6知, 对任一 $g \in G$, gS^{-1} 含有 $|S|$ 个元, 这里 S^{-1} 是 S 中元的所有逆元组成的集合. 因为 $|S| > \dfrac{|G|}{2}$, 故 $gS^{-1} \cap S \neq \varnothing$. 从而存在 $a, b \in S$, 使得 $gb^{-1} = a$, 即 $g = ab$.

□

定理 1.14 (Lagrange 定理)

设 H 是有限群 G 的子群, 记 1 为 G, H 的幺元, 则有

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

即

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

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 $|aH|=|H|=[H:1]$. 又由定理 1.9知 $G=\bigcup\limits_{a\in G}aH$ 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.

□

推论 1.1

(1) 设 H 是有限群 G 的子群,K 是 H 的子群, 则 $[G:K]=[G:H][H:K]$, 进而 $[G:H]=\dfrac{[G:K]}{[H:K]}$.

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

(3) 设 G 为无限群, $H\lhd G$, 则商群 G/H 的阶 $[G/H:H]=[G:H]$.

(4) 设 A,B 是群 G 的有限子群, 则 $|A|\cdot|B|=|AB|\cdot|A\cap B|$.

♡

证明

(1) 这是Lagrange 定理的直接推论.

(2) 这是Lagrange 定理的直接推论.

(3) 这是Lagrange 定理的直接推论.

(4) 易知 $AB=\bigcup\limits_{a\in A}aB$. 记 $\Sigma=\{aB\mid a\in A\}$, 则 $|AB|=|\Sigma|\cdot|B|$. 令

$$\phi: A/A\cap B\longrightarrow \Sigma$$

$$x(A\cap B)\longmapsto xB,\quad \forall x\in A.$$

(i) 如果 $x(A\cap B)=y(A\cap B)(x,y\in A)$, 则 $y^{-1}x\in A\cap B\subseteq B$, 从而 $xB=yB$, 所以 ϕ 为 $A/A\cap B$ 到 Σ 的良定义的映射.

(ii) 设 $x(A\cap B),y(A\cap B)\in A/A\cap B$, 有 $\phi(x(A\cap B))=\phi(y(A\cap B))$, 即 $xB=yB$, 则 $y^{-1}x\in B$. 又因为 $x,y\in A$, 而 A 为群, 所以 $y^{-1}x\in A$, 于是 $y^{-1}x\in A\cap B$. 从而 $x(A\cap B)=y(A\cap B)$. 所以 ϕ 为单映射.

(iii) 对任意的 $x\in A$, 有 $x(A\cap B)\in A/A\cap B$, 且 $\phi(x(A\cap B))=xB$, 所以 ϕ 为满映射.

由此得 $|A/A\cap B|=|\Sigma|$, 所以再利用Lagrange 定理可得

$$|AB|\cdot|A\cap B|=|B|\cdot|\Sigma|\cdot|A\cap B|=|B|\cdot|A/A\cap B|\cdot|A\cap B|=|A|\cdot|B|.$$

□

命题 1.9

(1) 设 A 和 B 均为群 G 的子群, 则

(i) $g(A\cap B)=gA\cap gB,\forall g\in G$.

(ii) 若 A 和 B 均有有限的指数, 即 $[G:A],[G:B]$ 有限, 则 $A\cap B$ 也有有限的指数, 即 $[G:A\cap B]$ 有限.

(2) 如果 R 是群 G 对于子群 A 的右陪集代表元系, 则 R^{-1} 是群 G 对于 A 的左陪集代表元系.

(3) 设 $A<G,B<G$. 如果存在 $a,b\in G$, 使得 $Aa=Bb$, 则 $A=B$.

(4) 设 H 和 K 分别是有限群 G 的两个子群, $g\in G$, 则存在 $k_1,k_2,\cdots,k_t\in K$ 和 $h_1,h_2,\cdots,h_s\in H$, 其中

$t=[K:K\cap g^{-1}Hg], s=[H:H\cap gKg^{-1}]$, 使得

$$HgK=\bigsqcup_{1\leqslant i\leqslant t}Hgk_i,\quad HgK=\bigsqcup_{1\leqslant i\leqslant s}h_igK.$$

并且

$$|HgK|=|H|[K:K\cap g^{-1}Hg]=|K|[H:H\cap gKg^{-1}],$$
$$[K:K\cap g^{-1}Hg]=[H:H\cap gKg^{-1}].$$

(5) 设 A 是群 G 的具有有限指数的子群, 则存在 G 的一组元 $g_1,g_2,\cdots,g_m$, 它们既可以作为 A 在 G 中的右陪集代表元系, 又可以作为 A 在 G 中的左陪集代表元系.

♠

证明

(1) (i) $g(A\cap B)\subseteq gA, g(A\cap B)\subseteq gB$, 故 $g(A\cap B)\subseteq gA\cap gB$. 反之, $\forall x=gh\in gA\cap gB$, 则 $h\in A\cap B$, 从而 $x=gh\in g(A\cap B)$. 于是 $g(A\cap B)=gA\cap gB, \forall g\in G$.

(ii) 证法一:命题 1.9(1)(i)表明 $A\cap B$ 的任一左陪集是 A 的一个左陪集和 B 的一个左陪集之交. 若 A 和 B 均有有限个左陪集, 则 $A\cap B$ 也只有有限个左陪集. 由此即得证.

证法二:用 $\langle AB\rangle$ 表示 G 的由 AB 生成的子群. 则 $|\langle AB\rangle|\geqslant|AB|=\dfrac{|A||B|}{|A\cap B|}$. 两边同乘 $\dfrac{|G|}{|A||B|}$, 再利用Lagrange 定理得到

$$[G:A\cap B]=\frac{|G|}{|A\cap B|}\leqslant\frac{|G|}{|A|}\cdot\frac{|\langle AB\rangle|}{|B|}\leqslant\frac{|G|}{|A|}\cdot\frac{|G|}{|B|}<+\infty.$$

(2) 由题设知 $G=\bigcup_{g\in R}Ag$, 并且满足 $Ag\cap Ah=\varnothing, \forall g\neq h, g,h\in R$. 需要验证 $G=\bigcup_{x\in R^{-1}}xA$, 并且满足 $xA\cap yA=\varnothing, \forall x\neq y, x,y\in R^{-1}$.

显然 $G\supseteq\bigcup_{x\in R^{-1}}xA$.$\forall z\in G$, 由题设 $z^{-1}\in Ag$, 对某一 $g\in R$, 于是 $z\in g^{-1}A^{-1}=g^{-1}A$. 故 $G\subseteq\bigcup_{x\in R^{-1}}xA$. 因此 $G=\bigcup_{x\in R^{-1}}xA$. 若 $z\in xA\cap yA$, 其中 $x,y\in R^{-1}$ 且 $x\neq y$, 即 $z=xa=yb, a,b\in A$, 从而

$$Ax^{-1}\cap Ay^{-1}=A(az^{-1})\cap A(bz^{-1})=Az^{-1}\neq\varnothing$$

其中 $x^{-1},y^{-1}\in R$. 从而由题设 $x^{-1}=y^{-1}$, 进而 $x=y$ 矛盾!

(3) 因 $A=Bba^{-1}$, 故 $ba^{-1}=1\cdot ba^{-1}\in Bba^{-1}=A$, 但 A 是子群, 故 $(ba^{-1})^{-1}=ab^{-1}\in A$. 于是 $A=Aab^{-1}=Bbb^{-1}=B$.

(4) 定义 K 上的一个关系 $\sim$:

$$k\sim k'\Longleftrightarrow Hgk=Hgk'.$$

显然这个关系是等价关系. 设这个等价关系的完全代表系为 $\{k_1,k_2,\cdots,k_t\}$, 则由定理 1.18知

$$K=\bigsqcup_{1\leqslant i\leqslant t}[k_i],\ \text{其中}\ [k_i]=\{k'\in K\mid Hgk_i=Hgk'\}. \tag{1.4}$$

从而 $[k_i]\cap[k_j]=\varnothing, i\neq j$. 于是 $Hgk_i\neq Hgk_j, i\neq j$, 故由定理 1.10(4)知 $Hgk_i\cap Hgk_j=\varnothing, i\neq j$.

对 $\forall hgk\in HgK$, 有 $h\in H,k\in K$, 则由(1.4)式知, 存在 $i\in[1,t]\cap\mathbb{N}$, 使得 $k\in[k_i]$, 即 $Hgk=Hgk_i$. 从而 $hgk\in Hgk=Hgk_i$. 故 $HgK\subseteq\bigcup_{1\leqslant i\leqslant t}Hgk_i$. 又显然 $HgK\supseteq\bigcup_{1\leqslant i\leqslant t}Hgk_i$. 因此

$$HgK=\bigsqcup_{1\leqslant i\leqslant t}Hgk_i.$$

因此由命题 1.6知

$$|HgK|=\sum_{i=1}^{t}|Hgk_i|=|H|\cdot t.$$

注意到对 $\forall k, k' \in K$, 有

$$k \sim k' \Longleftrightarrow Hgk = Hgk' \Longleftrightarrow gkk'^{-1}g^{-1} \in H \Longleftrightarrow kk'^{-1} \in K \cap g^{-1}Hg.$$

故由定理 1.9(2)知

$$[k] = \{k' \in K \mid Hgk = Hgk'\} = (K \cap g^{-1}Hg)k, \quad \forall k \in K.$$

因此由(1.4)式可得

$$K = \bigsqcup_{1 \leqslant i \leqslant t} [k_i] = \bigsqcup_{1 \leqslant i \leqslant t} (K \cap g^{-1}Hg)k_i.$$

于是 $t = [K : K \cap g^{-1}Hg]$. 从而由推论 1.1(1)可得

$$|HgK| = |H| \cdot [K : K \cap g^{-1}Hg].$$

同理可得

$$HgK = \bigsqcup_{1 \leqslant i \leqslant s} h_i gK, \text{ 其中} s = [H : H \cap gKg^{-1}].$$

故由命题 1.6知

$$|HgK| = \sum_{i=1}^{s} |h_i gK| = |K| \cdot [H : H \cap gKg^{-1}].$$

另外, 考虑映射

$$\begin{aligned} \varphi : & K \cap g^{-1}Hg \longrightarrow H \cap gKg^{-1}, \\ & x \longmapsto gxg^{-1}, \forall x \in K \cap g^{-1}Hg. \end{aligned}$$

设 $x \in K \cap g^{-1}Hg$, 则存在 $k \in K, h \in H$, 使得 $x = g^{-1}hg = k$. 从而

$$\varphi(x) = gxg^{-1} = h = gkg^{-1} \in H \cap gKg^{-1},$$

即 $\varphi(K \cap g^{-1}Hg) \subseteq H \cap gKg^{-1}$. 又显然当 $x_1, x_2 \in K \cap g^{-1}Hg$ 且 $x_1 = x_2$ 时, 有 $\varphi(x_1) = \varphi(x_2)$. 故 φ 是良定义的映射. 设 $h_1 = gk_1g^{-1} \in H \cap gKg^{-1}$, 则令 $x_1 = g^{-1}h_1g = k_1 \in K \cap g^{-1}Hg$, 则 $\varphi(x_1) = h_1 = gk_1g^{-1}$. 故 φ 是满射. 若 $\varphi(x_1) = \varphi(x_2)$, 则 $gx_1g^{-1} = gx_2g^{-1}$, 从而 $x_1 = x_2$. 故 φ 是单射. 因此 φ 是 $K \cap g^{-1}Hg$ 到 $H \cap gKg^{-1}$ 的双射, 故

$$|K \cap g^{-1}Hg| = |H \cap gKg^{-1}|.$$

(5) 由定理 1.9(3), 可将 G 写成双陪集的无交并: $G = \bigsqcup_{g \in R} AgA$, 其中 R 是 (A, A)-的双陪集代表系. 对 $\forall g \in G$, 由命题 1.9(4)知每个双陪集 AgA 既是 $[A : A \cap gAg^{-1}]$ 个互不相交右陪集之并, 也是 $[A : A \cap gAg^{-1}]$ 个互不相交左陪集之并. 记 $t = [A : A \cap gAg^{-1}]$, 则有无交并

$$AgA = \bigsqcup_{1 \leqslant i \leqslant t} Aga_i = \bigsqcup_{1 \leqslant i \leqslant t} b_i gA,$$

其中 $a_i, b_i \in A$. 于是 $A = Ab_i = a_iA$, 故有无交并

$$AgA = \bigsqcup_{1 \leqslant i \leqslant t} Ab_iga_i, \quad AgA = \bigsqcup_{1 \leqslant i \leqslant t} b_iga_iA.$$

因为 a_i, b_i, t 与 g 有关, 所以记 $b_i = b_i(g), a_i = a_i(g), t = t(g)$, 于是

$$G = \bigsqcup_{g \in R} AgA = \bigsqcup_{g \in R} \bigsqcup_{1 \leqslant i \leqslant t(g)} Ab_i(g)ga_i(g) = \bigsqcup_{g \in R} \bigsqcup_{1 \leqslant i \leqslant t(g)} b_i(g)ga_i(g)A.$$

因此

$$\bigcup_{g \in R} \{b_i(g)ga_i(g) \mid 1 \leqslant i \leqslant t(g)\}$$

既是 G 关于 A 的右陪集的一个代表元系, 也是 G 关于 A 的左陪集的一个代表元系.

□

1.4 环与域

定义 1.15 (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 $(R,+,\cdot)$.

♣

例题 1.15

(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 ***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) $\mathrm{ent}_{ij}(\alpha\beta)=\sum\limits_{k=1}^{n}\mathrm{ent}_{ik}(\alpha)\mathrm{ent}_{kj}(\beta)$

定义的 $R^{n\times n}$ 加法与乘法使其成为一个环, 称为 R 上的 ***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 1.15 (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 $(ab)^m=a^mb^m,\forall m\in\mathbb{N}$.

(2) 由分配律成立有

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

(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 1.16

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:** 交换的体, 即非零元素集合对乘法为 Abel 群的环.

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

注 有些书上这样定义除环、体和域:

除环: 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.

体: 不可交换的除环.

域: 交换的除环.

实际上, 这样定义的除环就是我们上面定义的体, 而体的定义中多了一个不可交换, 域的定义则没有变化.

定义 1.17

1. 设 R 是一个环, 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**.
2. 设 R 是一个体, 若非空子集 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**.
3. 设 R 是一个域, 若非空子集 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 1.16

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.

□

定理 1.17

设 R 为环, 则

$$C(R)=\{r\in R\mid rs=sr,\forall s\in R\}$$

为 R 的一个子环. 这个子环称为 R 的**中心** (center).

♡

证明 对任意 $x\in R$, 有 $0\cdot x=x\cdot 0=0$, 所以 $0\in C(R)$. 从而 $C(R)$ 是 R 的一个非空子集.

对任意 $a,b\in C(R),x\in R$, 有

$$(a-b)x=ax-bx=xa-xb=x(a-b),$$

$$(ab)x=a(bx)=a(xb)=(ax)b=(xa)b=x(ab),$$

所以 $a-b,ab\in C(R)$. 从而由定理 1.16(2)知 $C(R)$ 为 R 的子环.

□

命题 1.10

(1) 一切数域 P 都是环, 也都是域, 因而也是体.

(2) 体一定是整环, 进而域也一定是整环.

(3) 若 R 是一个环, 则 R 的任意子环的交也是 R 的子环.

(4) 若 R 是一个体, 则 R 的任意子体的交也是 R 的子体.

(5) 若 R 是一个域, 则 R 的任意子体的交也是 R 的子域.

♠

证明

(1)

(2) 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.

(3) 设 $\{R_i\mid i\in I\}$ 为环 R 的一簇子环, 对任意的 $x,y\in\bigcap\limits_{i\in I}R_i$, 有 $x,y\in R_i(i\in I)$, 于是

$$x-y,\ xy\in R_i,\ \forall i\in I.$$

因此

$$x-y,\ xy\in\bigcap_{i\in I}R_i.$$

所以 $\bigcap\limits_{i\in I}R_i$ 是 R 的子环.

(4)

(5)

□

命题 1.11

(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.

当 R 是整环时, 有 $R^*=R\setminus\{0\}$ 对乘法构成幺半群且消去律成立, 即

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

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

♠

证明

(1)

(2) 因为 R 是整环且 $R^* \subseteq R$, 所以 R 对乘法构成幺半群. 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 1.12

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 $a \equiv b \pmod p$ 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

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

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 1.18

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

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

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 1.13

设 $\mathbf{H}$ 为四元数体, 令

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

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

则

$$\mathbf{i}\cdot\mathbf{j}=\mathbf{k},\quad \mathbf{i}\cdot\mathbf{k}=-\mathbf{j},$$
$$\mathbf{j}\cdot\mathbf{i}=-\mathbf{k},\quad \mathbf{j}\cdot\mathbf{k}=\mathbf{i},$$
$$\mathbf{k}\cdot\mathbf{i}=\mathbf{j},\quad \mathbf{k}\cdot\mathbf{j}=-\mathbf{i},$$
$$\mathbf{1}^2=\mathbf{1},\quad \mathbf{i}^2=\mathbf{j}^2=\mathbf{k}^2=-\mathbf{1},$$
$$\mathbf{1}\cdot\mathbf{i}=\mathbf{i}\cdot\mathbf{1}=\mathbf{i},\quad \mathbf{1}\cdot\mathbf{j}=\mathbf{j}\cdot\mathbf{1}=\mathbf{j},\quad \mathbf{1}\cdot\mathbf{k}=\mathbf{k}\cdot\mathbf{1}=\mathbf{k}.$$

并且有下面结论:

(1) $\forall\alpha\in\mathbf{H}$, 存在唯一的一组 $(a,b,c,d)\in\mathbb{R}^{1\times4}$, 使得 $\alpha=a\mathbf{1}+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}$. 进而

$$\mathbf{H}=\{a\mathbf{1}+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}\mid a,b,c,d\in\mathbb{R}\}.$$

(2) $\mathbf{H}$ 的变换 σ:

$$\sigma(a\mathbf{1}+b\mathbf{i}+c\mathbf{j}+d\mathbf{k})=a\mathbf{1}-b\mathbf{i}-c\mathbf{j}-d\mathbf{k}$$

是 $\mathbf{H}$ 的一个对合.

♠

注 我们一般省略不写 $\mathbf{1}$, 即将 $a\mathbf{1}$ 简写成 a.

证明

(1) 根据定理 1.18,$\alpha\in\mathbf{H}$ 有 $a,b,c,d\in\mathbb{R}$, 使得

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

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 $\beta=a_1\mathbf{1}+b_1\mathbf{i}+c_1\mathbf{j}+d_1\mathbf{k}$,$a_1,b_1,c_1,d_1\in\mathbb{R}$, 则

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

$$\begin{aligned}\sigma(\alpha\beta)&=\sigma\left((a\mathbf{1}+b\mathbf{i}+c\mathbf{j}+d\mathbf{k})(a_1\mathbf{1}+b_1\mathbf{i}+c_1\mathbf{j}+d_1\mathbf{k})\right)\\&=\sigma\left((aa_1-bb_1-cc_1-dd_1)\mathbf{1}+(ab_1+ba_1+cd_1-dc_1)\mathbf{i}+(ac_1+ca_1+db_1-bd_1)\mathbf{j}+(ad_1+da_1+bc_1-cb_1)\mathbf{k}\right)\\&=(aa_1-bb_1-cc_1-dd_1)\mathbf{1}-(ab_1+ba_1+cd_1-dc_1)\mathbf{i}-(ac_1+ca_1+db_1-bd_1)\mathbf{j}-(ad_1+da_1+bc_1-cb_1)\mathbf{k}\\&=(a_1\mathbf{1}-b_1\mathbf{i}-c_1\mathbf{j}-d_1\mathbf{k})(a\mathbf{1}-b\mathbf{i}-c\mathbf{j}-d\mathbf{k})=\sigma(\beta)\sigma(\alpha).\end{aligned}$$

因此 σ 是 $\mathbf{H}$ 的反自同构. 又因

$$\sigma^2(\alpha)=\sigma(a\mathbf{1}-b\mathbf{i}-c\mathbf{j}-d\mathbf{k})=a\mathbf{1}+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}=\alpha,$$

故 σ 是对合.

□

定义 1.18

若 R_1 为环 R 的子环, 并且 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**.

若 P 是环 R 的理想且 $P\neq R$, 则称 P 是 R 的**真理想**.

$\{0\}$ 与 R 都是 R 的理想, 称为**平凡理想**.

♣

注 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 1.19

设 R 是一个环,I 是 R 的一个非空子集, 则 I 是 R 的理想的充分必要条件是 I 同时满足下列两个条件

(1) 对 $\forall r_1, r_2 \in I$, 有 $r_1 - r_2 \in I$.

(2) 对 $\forall r \in I, s \in R$, 则 $rs, sr \in I$.

♡

证明 由定理 1.16和理想的定义立得.

□

定义 1.19

设 R 为环,I, J 都是 R 的理想, 集合

$$I + J = \{a + b \mid a \in I, b \in J\} \quad 与 \quad I \cap J$$

分别称为理想 I 与 J 的**和**与**交**.

♣

定理 1.20

(1) 一个环中有限多个理想的和还是理想.

(2) 一个环中任意多个理想之交还是理想.

(3) 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.

(4) 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) 设 $I_1, I_2, \cdots, I_m$ 为环 R 的理想, 令

$$I = I_1 + I_2 + \cdots + I_m = \{a_1 + a_2 + \cdots + a_m \mid a_i \in I_i, i = 1, 2, \cdots, m\}.$$

对任意的 $x = x_1 + x_2 + \cdots + x_m, y = y_1 + y_2 + \cdots + y_m \in I (x_i, y_i \in I_i), r \in R$, 有 $x_i - y_i \in I_i, rx_i, x_i r \in I_i (i = 1, 2, \cdots, m)$, 从而

$$x - y = (x_1 - y_1) + (x_2 - y_2) + \cdots + (x_m - y_m) \in I,$$

$$rx = rx_1 + rx_2 + \cdots + rx_m \in I,$$

$$xr = x_1 r + x_2 r + \cdots + x_m r \in I,$$

所以 I 为 R 的理想.

(2) 设 $\{I_i \mid i \in J\}$ 为环 R 的一簇理想 (其中 J 为指标集), 令

$$I = \bigcap_{i \in J} I_i.$$

对任意的 $x, y \in I, r \in R$, 有 $x, y \in I_i$, 于是 $x - y \in I_i, rx, xr \in I_i (i \in J)$, 从而

$$x - y \in I,\ rx, xr \in I,$$

所以 I 为 R 的理想.

(3)

(4)

□

定理 1.21

设 $R_1, R_2, \cdots, R_n$ 为 n 个环. 令

$$R = R_1 \oplus R_2 \oplus \cdots \oplus R_n = \{(a_1, a_2, \cdots, a_n) \mid a_i \in R_i, i = 1, 2, \cdots, n\}.$$

对任意的 $(a_1, a_2, \cdots, a_n), (b_1, b_2, \cdots, b_n) \in R$, 规定

$$(a_1, a_2, \cdots, a_n) + (b_1, b_2, \cdots, b_n) = (a_1 + b_1, a_2 + b_2, \cdots, a_n + b_n),$$

$$(a_1, a_2, \cdots, a_n) \cdot (b_1, b_2, \cdots, b_n) = (a_1 b_1, a_2 b_2, \cdots, a_n b_n),$$

则 R 关于上面所定义的加法与乘法构成一个环. 这个环称为环 $R_1, R_2, \cdots, R_n$ 的**直和** (direct sum). 并且

(1) R 有单位元的充分必要条件是每个 R_i 都有单位元.

(2) R 是交换环的充分必要条件是每个 R_i 都是交换环.

♡

证明

□

定义 1.20

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 1.22

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

$$\langle a \rangle = \left\{ \sum_{i=1}^{n} x_i a y_i + xa + ay + ka \mid x_i, y_i, x, y \in R, n \in \mathbb{N}, k \in \mathbb{Z} \right\},$$

$$\langle a_1, \cdots, a_n \rangle = \left\{ \sum_{i=1}^{n} \sum_{j=1}^{m_i} x_{ij} a_i y_{ij} + \sum_{i=1}^{n} x_i a_i + \sum_{i=1}^{n} a_i y_i + \sum_{i=1}^{n} k_i a_i \mid x_{ij}, y_{ij}, x_i, y_i \in R, n \in \mathbb{N}, k_i \in \mathbb{Z} \right\}.$$

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 $\langle a_1, a_2, \cdots, a_n \rangle \subseteq I$.

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

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

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

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 $\langle a_1, a_2, \cdots, a_n \rangle \subseteq I$.

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

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

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

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 $\langle a_1, a_2, \cdots, a_n \rangle \subseteq I$.

♡

证明

(1) 只须证明第二个等式. 利用定理 1.19容易验证.

(2) 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

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

对 $\forall r\in R$, 都有

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

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

因此由定理 1.19知 $Ra_1R+\cdots+Ra_nR$ 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 $\langle a_1,\cdots,a_n\rangle=Ra_1R+\cdots+Ra_nR$.

(3) 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

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

对 $\forall r\in R$, 由 R 是交换幺环可得

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

因此由定理 1.19知 $Ra_1+\cdots+Ra_n$ 是 R 的理想, 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 1.23

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 1.11 知 “$\sim$” 对 R 的加法为同余关系, 再由命题 1.8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 1.2

若 R 为交换环, I 为 R 的理想, 则 R/I 也是交换环.

证明

□

推论 1.3

若 R 为幺环,I 为 R 的理想, 则 R/I 也是幺环且 $1+I$ 为幺元.

证明

□

例题 1.16 从定理 1.23知 $m\mathbb{Z}$ 为 $\mathbb{Z}$ 的理想, 故 $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ 对剩余类 (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 1.17 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 模

定义 1.21 (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.

定理 1.24

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 1.18 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 1.19 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 1.20 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 1.22

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 1.21 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 1.22 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 1.14

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 1.23 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 1.19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 1.23

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 1.15

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 1.16

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 1.24 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 1.1).

(3) R 模之间的同构关系是等价关系.

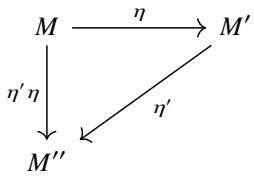

图 1.1

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 1.24 (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 1.25

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 1.25 设 M 为 Abel 群, 于是 M 为 $\mathbb{Z}$ 模. 则由命题 1.15知 $\mathrm{End}_{\mathbb{Z}} M = \mathrm{End}M$.

证明

□

例题 1.26 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 $\mathrm{End}_R R = R_r$.

□

1.6 同态与同构

定义 1.26

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 $G_1 \cong G_2$.

♣

例题 1.27 证明:

(1) 有理数加法群 $\mathbb{Q}$ 和非零有理数乘法群 $\mathbb{Q}^*$ 不同构.

(2) 有理数加法群 $\mathbb{Q}$ 和正有理数乘法群 $\mathbb{Q}^+$ 不同构.

(3) 实数加法群 $\mathbb{R}$ 同构于正实数乘法群 $\mathbb{R}^+$.

证明

(1) 若 $(\mathbb{Q},+)\cong(\mathbb{Q}^*,\cdot)$, 则有群同构 f 和 $a\in\mathbb{Q}$ 使得 $f(a)=2$, 从而

$$2=f(a)=f\left(\frac{a}{2}+\frac{a}{2}\right)=f\left(\frac{a}{2}\right)^2,$$

即 $\sqrt{2}$ 是有理数, 矛盾!

(2) 若 $(\mathbb{Q},+)\cong(\mathbb{Q}^+,\cdot)$, 则有群同构 f 和 $a\in\mathbb{Q}$ 使得 $f(a)=2$, 从而

$$2=f(a)=f\left(\frac{a}{2}+\frac{a}{2}\right)=f\left(\frac{a}{2}\right)^2,$$

即 $\sqrt{2}$ 是有理数, 矛盾!

(3) 将每一实数 x 变到 e^x 就给出了实数加法群 $\mathbb{R}$ 到正实数乘法群 $\mathbb{R}^+$ 的同构映射.

□

定理 1.32

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). "~" 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 1.17

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 1.7(3)知 N 也是 H 的子群, 故 $H/N=\{hN:h\in H\}=\pi(H)$.

□

例题 1.28

(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 1.33 (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 $G_1 \cong G_3$.

♡

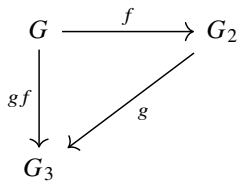

图 1.2

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, 由定理 1.33(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 $G_1\cong G_3$ (参见定理 1.33(1)).

□

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 $\mathrm{Aut}G$.

♣

定义 1.28

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 1.18

G 上由 a 决定的左平移, 右平移 L_a,R_a 都是 G 到 G 上的一一对应, 即为 $\mathrm{Aut}G$ 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 $\mathrm{Aut}G$ 的子群.

♠

证明

□

定理 1.34 (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

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

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 $G\cong L_G\cong R_G$.

□

定理 1.35

设 G 是一个群, 则有

(1) Aut$G$ 对变换的乘法也是一个群, 称为 G 的**自同构群**.

(2) 对 $\forall a \in G$, $f : a \mapsto a^{-1}$ 是群 G 的自同构当且仅当 G 是 Abel 群.

(3) $\forall g \in G$, 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**.

(4) G 的内自同构的集合 Int$G$ (也记成 ad$G$ 或 Inn(G)) 是 Aut$G$ 的正规子群, 称为 G 的**内自同构群**.

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

(6) 若 $C(G) = \{1\}$, 则 $\mathrm{ad} : g \to \mathrm{ad}g$ 是群 G 到 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 Aut$G$ 是群.

(2) 显然 f 是双射, 故 f 将每一元变成其逆元是自同构 $\iff (ab)^{-1} = a^{-1}b^{-1}, \forall a, b \in G \iff ab = (a^{-1}b^{-1})^{-1} = ba, \forall a, b \in G \iff G$ 是 Abel 群.

(3) 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.

(4) 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 Int$G$ 是 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 Int$G$ 是 Aut$G$ 的正规子群.

(5) 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 Int$G$ 上的同态映射.

(6) 由定理 1.35(5)可知 ad 是 G 到 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

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

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 Int$G$ 的同构.

□

例题 1.29 求有理数加法群 $\mathbb{Q}$ 的自同构群 $\mathrm{Aut}(\mathbb{Q})$. 再证明 $\mathrm{Aut}(\mathbb{Q},+)\cong(\mathbb{Q}^*,\cdot)$.

解 一方面, 由命题 1.18知对任一非零有理数 a, L_a 是将 x 变成 ax 是有理加法群 $\mathbb{Q}$ 的一个自同构. 另一方面, 设 f 是有理数加群 $\mathbb{Q}$ 的任一自同构. 令 $f(1)=a$, 则 a 是非零有理数. 因为对任一正整数 n 和 m 有

$$f(n)=f(1+\cdots+1)=f(1)+\cdots+f(1)=nf(1)=na,$$
$$f(n)=f\left(\frac{n}{m}+\cdots+\frac{n}{m}\right)=f\left(\frac{n}{m}\right)+\cdots+f\left(\frac{n}{m}\right)=mf\left(\frac{n}{m}\right).$$

故得到

$$f\left(\frac{n}{m}\right)=\frac{1}{m}f(n)=\frac{n}{m}a.$$

由此推知 $f(x)=ax,\forall x\in\mathbb{Q}$, 即 $f=L_a$. 于是

$$\mathrm{Aut}(\mathbb{Q},+)=\{f_a\mid a\in\mathbb{Q},a\neq 0\}.$$

对 $\forall a\in(\mathbb{Q}^*,\cdot)$, 其中 $(\mathbb{Q}^*,\cdot)$ 是非零有理数的乘法群. 令 $\varphi:a\to L_a$ 是 $\mathbb{Q}^*$ 到 $\mathrm{Aut}(\mathbb{Q},+)$ 的映射, 则 φ 显然是双射且满足

$$L_aL_b=L_{ab}.$$

故 φ 是群同构 $\mathrm{Aut}(\mathbb{Q},+)\cong(\mathbb{Q}^*,\cdot)$.

□

定义 1.29

群 G 的自同构 α 称为**没有不动点的自同构**, 是指对 G 的任意元 $g\neq 1$ 有 $\alpha(g)\neq g$. ♣

例题 1.30 如果有限群 G 具有一个没有不动点的自同构 α 且 $\alpha^2=1$, 试证: G 一定是奇数阶 Abel 群.

证明 令 $H=\{g^{-1}\alpha(g)\mid g\in G\}$, 显然 $H\subseteq G$, 则 $|H|\leqslant|G|$. 不难发现 $f:g^{-1}\alpha(g)\to g$ 是 H 到 G 的满射, 故由命题 1.9(2)知 $|H|\geqslant|G|$. 因此 $H=G$. 于是, 对任一 $a\in G, a=g^{-1}\alpha(g)$. 因 $\alpha^2=1$, 故

$$a^{-1}=\alpha(g^{-1})g=\alpha(g^{-1})\alpha(\alpha(g))=\alpha(g^{-1}\alpha(g))=\alpha(a).$$

从而 $\alpha(ab)=(ab)^{-1}=b^{-1}a^{-1}=\alpha(b)\alpha(a)=\alpha(ba)$. 故 $ba=ab,\forall a,b\in G$. 即 G 是 Abel 群. 因 $\forall a\in G\setminus\{1\}$, 有 $a^{-1}\neq a$, 且 $1\in G$, 故 G 的阶为奇数.

□

例题 1.31 设 G 是奇数阶有限群, $\alpha\in\mathrm{Aut}(G)$ 且 $\alpha^2=1$. 令

$$G_1=\{g\in G\mid\alpha(g)=g\},\ G_{-1}=\{g\in G\mid\alpha(g)=g^{-1}\}.$$

试证: $G=G_1G_{-1}$ 且 $G_1\cap G_{-1}=1$.

笔记 证明思路: 猜测对 $\forall g\in G$, 有 $g=(gx)x^{-1}\in G_1G_{-1}$. 进而只需找到 $x\in G$, 满足 $\alpha(gx)=gx$, $\alpha(x^{-1})=x$. 而这等价于 $x^2=g^{-1}\alpha(g)$.

证明 由题设知 $(2,|G|)=1$, 设 $2k+l|G|=1$, 则由定理 1.47知

$$g=g^{2k+l|G|}=(g^k)^2,\ \forall g\in G.$$

因此 G 中任一元均可写成某一元的平方的形式. 对任一 $g\in G$, 设 $g^{-1}\alpha(g)=x^2$. 因

$$\alpha(x)^2=\alpha(g^{-1}\alpha(g))=\alpha(g)^{-1}g=(g^{-1}\alpha(g))^{-1}=x^{-2},$$

而 x 和 $\alpha(x)$ 的阶相同且为奇数, 记为 $2n+1$, 由此可得

$$1=\alpha(x)^{2n+1}=x^{-2n}\cdot\alpha(x)\Longrightarrow\alpha(x)=x^{2n}=x^{-1}\Longrightarrow x\in G_{-1}$$

又由 $g^{-1}\alpha(g)=x^2$ 知 $x=x^{-1}g^{-1}\alpha(g)$, 进而 $x^{-1}=\alpha(g)gx$. 于是

$$\alpha(gx)=\alpha(g)\alpha(x)=\alpha(g)x^{-1}=gx,$$

即 $gx \in G_1$, 故

$$g = (gx)x^{-1} \in G_1G_{-1},$$

即 $G = G_1G_{-1}$.

若 $g \in G_1 \cap G_{-1}$, 则 $\alpha(g) = g = g^{-1}$, 进而 $g^2 = 1$, 于是 $\operatorname{ord} g \leqslant 2$. 但 $|G|$ 是奇数, 因此 $\operatorname{ord} g$ 也只能是奇数, 故 $\operatorname{ord} g = 1 \iff g = 1$, 即 $G_1 \cap G_{-1} = 1$.

□

定义 1.30

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 1.31

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 1.19

(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 1.36

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 1.20

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 1.32 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 1.32

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 1.37

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 1.33 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

□

1.7 同态基本定理

定义 1.33 (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 1.21

(1) 设 f 是群 G 到群 G' 的同态, 则

(i) $\ker f$ 是 G 的正规子群,$f(G)$ 是 G' 的子群.

(ii) f 是单同态的充要条件是 $\ker f = \{1\}$.

(2) 设 f 是环 R 到环 R' 的同态, 则

(i) $\ker f$ 是 R 的理想,$f(R)$ 是 R' 的子环.

(ii) f 是单同态的充要条件是 $\ker f = \{0\}$.

(3) 设 R 是一个环,M, M' 都是 R 模,f 是 M 到 M' 的模同态, 则

(i) $\ker f$ 是 M 的子模,$f(M)$ 是 M' 的子模.

(ii) f 是单同态的充要条件是 $\ker f = \{0\}$.

♠

证明

(1) (i) 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 $\ker f \lhd G'$.

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.

(ii) 设 G' 的幺元为 $1'$.

必要性: 设 f 为单同态, 则对任意的 $x \in \ker f$, 有 $f(x) = 1' = f(1)$. 因为 f 为单同态, 所以 $x = 1$, 于是 $\ker f = \{1\}$.

充分性: 设 $x, y \in G$, 如果 $f(x) = f(y)$, 则 $f(xy^{-1}) = f(x)(f(y))^{-1} = 1'$, 从而 $xy^{-1} \in \ker f$. 而 $\ker f = \{1\}$, 所以 $xy^{-1} = 1$, 因此 $x = y$, 从而 f 为单同态.

(2) (i) 设 $x, y \in \ker f$, 则有 $f(x - y) = 0$, 故 $x - y \in \ker f$. 又显然有 $\ker f$ 对乘法封闭, 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.

(ii)

由命题 1.21(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) (i) 对 $\forall x, y \in \ker f$, 由 f 是摸同态知 $f(x - y) = f(x) - f(y) = 0$. 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.

(ii)

□

命题 1.22

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

(ii) 设 H, H' 都是群 G 的正规子群, 且 $G/H \cong G/H'$, 则 $H \cong H'$.

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

(ii) 设 I, I' 都是环 R 的理想, 且 $R/I \cong R/I'$, 则 $I = I'$.

(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 $\ker\pi = N$.

♠

证明

(1) (i)

(ii)

(2) (i)

(ii) 设 f 为 R/I 到 R/I' 的同构,π 为 R 到 R/I 的自然同态,π' 为 R 到 R/I' 的自然同态, 则

$$f\cdot\pi = \pi'.$$

注意 I, I' 分别是 $R/I, R/I'$ 的零元. 于是对 $\forall x \in \ker(f\cdot\pi)$, 有 $f\cdot\pi(x) = f(\pi(x)) = I'$. 再结合命题 1.22(2)(i)可得

$$\pi(x) \in f^{-1}\left(I'\right) = I \Longrightarrow x \in \ker\pi = I.$$

因此 $\ker(f\cdot\pi) \subseteq I$. 又因为

$$f\cdot\pi(I) = f(\pi(I)) = f(I) = I',$$

所以 $I \subseteq \ker(f\cdot\pi)$. 故 $I = \ker(f\cdot\pi)$. 故再结合命题 1.22(2)(i)可得

$$I = \ker(f\cdot\pi) = \ker\pi' = I'.$$

(3)

□

定理 1.38 (群的同态基本定理)

设 f 是群 G 到群 H 上的同态,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

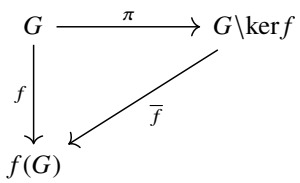

图 1.3

证明 由命题 1.21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 1.39

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) 由命题 1.21(1)知 $\ker f\lhd G_1$, 再由命题 1.8(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.

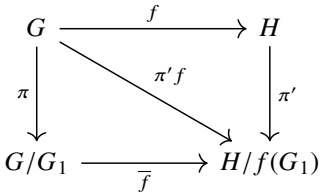

图 1.4

□

推论 1.4

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 1.39中将 H 换成 G/N,f 换成 π, 即得本推论. 对于 (3), 由命题 1.17(1)知 $\pi(H) = H/N$, 故由定理 1.39可得

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

以及如下交换图.

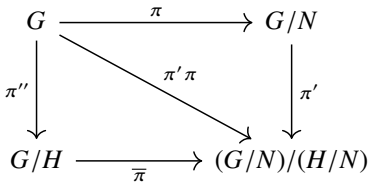

图 1.5

□

定理 1.40

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 1.8(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 1.41 (环的同态基本定理)

设 f 是环 R 到环 R' 上的同态,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 由命题 1.21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 1.42

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 1.39(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 1.39(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 1.19(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 1.5

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 1.42中取 $R'=R/A,f$ 为 R 到 R/A 的自然同态, 并且由定理 1.20(1)知 $f(B)=B/A$, 再由定理 1.42(2)知 $f(B)=B/A$ 是 $R'=R/A$ 的理想. 因此即得本推论.

□

定理 1.43

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 1.20(3)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 1.44 (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,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 由命题 1.21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 1.45

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 1.39(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 1.39(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 1.6

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 1.45(2)中取 $M' = M/N, f$ 为 M 到 $M' = M/N$ 的自然同态, 再由命题 1.16(1)知 $f(M_1) = M_1/N$, 即得本推论.

□

定理 1.46

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 $\pi(H + N) = \pi(H) + N = \pi(H)$, 因而由命题 1.21(3)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 1.34 (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.

注 显然若 a 在群 G 中, 则 $\langle a \rangle \subseteq G$.

命题 1.23 (循环群都是 Abel 群)

循环群都是 Abel 群.

♠

证明 设 $G = \langle a \rangle$ 为循环群, 则对任意的 $x, y \in G$, 存在 k, l, 使 $x = a^k, y = a^l$, 于是

$$xy = a^k a^l = a^{k+l} = a^l a^k = yx.$$

所以 G 为 Abel 群.

□

命题 1.24 (素数阶群必为循环群)

设 G 是一个群, 且 $|G| = p$ 为一个素数, 则 G 必是循环群, 并且 $\forall a \in G$ 且 $a \neq e$ 有 $G = \langle a \rangle$.

♠

证明 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.

□

定义 1.35

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 1.47

有限群 G 的任一元素 a 的阶是 G 的阶的因子, 即 $\operatorname{ord} a \mid |G|$. 特别地, $G = \langle a \rangle \iff \operatorname{ord} a = |G|$.

♡

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 $n = t_n d + r_n$, 于是 $a^n = a^{r_n}$. 因此 $\langle a \rangle$ 中至多只有 d 个元素 $1, a, \cdots, a^{d-1}$.

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.

设 $\operatorname{ord} a = d$. 若 $G = \langle a \rangle$, 则由上述证明知 $G = \langle a \rangle = \{1, a, \cdots, a^{d-1}\}$ 是 d 阶群, 故 $d = |G|$. 又若 $d = |G|$, 则由上述证明知 $\langle a \rangle = d = |G|$. 又显然有 $\langle a \rangle \subseteq G$, 故 $\langle a \rangle = G$.

□

定理 1.48 (群元素的阶的基本性质)

设 $(G, \cdot)$ 是一个群, $a, b \in G$, 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

$$a^m = a^n \iff m \equiv n \pmod{d}. \tag{1.17}$$

特别地, 我们有

$$\operatorname{ord} a = 1 \iff a = 1, \quad a^{-1} = a \iff a = 1 \text{或 } \operatorname{ord} a = 2.$$

(3) $\operatorname{ord} a = \operatorname{ord} a^{-1} = \operatorname{ord}(gag^{-1}), \forall g \in G$. 进而 $\operatorname{ord}(ab) = \operatorname{ord}(ba)$.

(4) 若 a 为 m 阶元素, 则对 $\forall k \in \mathbb{N}$,a^k 的阶为 $\dfrac{m}{(m,k)}$, 其中 (m,k) 是 m 与 k 的最大公因数.

进而, a^k 为 m 阶元素的充要条件是 $(m,k) = 1$.

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

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

(7) 设群 G 中的元 g 的阶 $\operatorname{ord} g = mn$, $(m,n) = 1$. 则 $g = ab$, $\operatorname{ord} a = m$, $\operatorname{ord} b = n$, 且 a, b 均为 g 的幂.

(8) 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

(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 (1.17) 成立. 特别地, 由 (1.17) 式可得

$$a^{-1} = a \iff a^2 = 1 = a^0 \iff 2 \equiv 0 \pmod{d} \iff \operatorname{ord} a = 1 \text{或} 2 \iff a = 1 \text{或 } \operatorname{ord} a = 2.$$

(3) 如果 $\operatorname{ord} a$ 或 $\operatorname{ord} a^{-1}$ 有一个为有限的, 记为 n. 则由 $(a^n)^{-1} = (a^{-1})^n$ 知另一个也必是有限的, 这说明 $\operatorname{ord} a$ 与 $\operatorname{ord} a^{-1}$ 必同时有限或同时无限, 故仅需对 $\operatorname{ord} a$ 与 $\operatorname{ord} a^{-1}$ 同时有限的情形加以证明. 再由 $(a^n)^{-1} = (a^{-1})^n$ 知 $a^k = 1$ 当且仅当 $(a^{-1})^k = 1$, 故 a^{-1} 与 a 同阶.

如果 $\operatorname{ord} a$ 或 $\operatorname{ord}(gag^{-1})$ 有一个为有限的, 当 $\operatorname{ord} a = n < \infty$ 时, 则

$$(gag^{-1})^n = ga^ng^{-1} = 1,$$

故 $\operatorname{ord}(gag^{-1}) \leqslant n < \infty$. 当 $\operatorname{ord}(gag^{-1}) < \infty$ 时, 同理可证 $\operatorname{ord} a < \infty$. 这说明 $\operatorname{ord} a$ 与 $\operatorname{ord}(gag^{-1})$ 必同时有限或同时无限, 故仅需对 $\operatorname{ord} a$ 与 $\operatorname{ord}(gag^{-1})$ 同时有限的情形加以证明. 现设 $\operatorname{ord} a = r_1$,$\operatorname{ord}(gag^{-1}) = r_2$, 则

$$a^{r_2} = g^{-1}(gag^{-1})^{r_2}g = 1,$$

$$(gag^{-1})^{r_1} = ga^{r_1}g^{-1} = 1.$$

由此得 $r_2 \geqslant r_1$,$r_1 \geqslant r_2$, 从而 $r_1 = r_2$. 所以 gag^{-1} 与 a 有相同的阶.

注意到 $ba = b(ab)b^{-1}$, 故只需取 $g = b$, 则由上述证明知 ab 与 ba 有相同的阶.

(4) 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 $\dfrac{m}{(m,k)} | q$. 又 $(a^k)^{\frac{m}{(m,k)}} = (a^m)^{\frac{k}{(m,k)}} = 1$, 即得 $q | \dfrac{m}{(m,k)}$, 因而 $q = \dfrac{m}{(m,k)}$.

(5) 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 $m_1 = [m,n]$.

(6) 设 m_1 是 $\langle a\rangle \cap \langle b\rangle$ 的阶, 由定理 1.47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 1.48(5)知 ab 的阶为 $[m,n] = mn$.

(7) 因 $(m,n) = 1$, 故有整数 s, t 使得 $sm + tn = 1$, 而且 $(t,m) = (s,n) = 1$. 令 $a = g^{tn}$, $b = g^{sm}$, 则 $g = ab$, 并且由

可得

$$\operatorname{ord} a = \operatorname{ord} g^{tn} = \frac{\operatorname{ord} g}{(tn, \operatorname{ord} g)} = \frac{mn}{n(t,m)} = m,$$
$$\operatorname{ord} b = \operatorname{ord} g^{sm} = \frac{\operatorname{ord} g}{(sm, \operatorname{ord} g)} = \frac{mn}{m(s,n)} = n.$$

(8) 因为 $(n,r)=d$, 所以存在 $u,v\in\mathbb{Z}$, 使

$$d = nu + rv.$$

于是 $a^d = a^{nu+rv} = a^{rv} \in \langle a^r\rangle$, 故 $\langle a^d\rangle \subseteq \langle a^r\rangle$. 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 $\langle a^r\rangle = \langle a^d\rangle$.

□

例题 1.34 设群 G 中两个元 g,h 可换, $o(g)=m$, $o(h)=n$. 记 $(m,n),[m,n]$ 分别是 m,n 的最大公因子和最小公倍数. 则

(1) $\operatorname{ord}(g^n h^m) = \dfrac{[m,n]}{(m,n)}$;

(2) G 中存在阶为 (m,n) 的元;

(3) G 中存在阶为 $[m,n]$ 的元.

证明

(1) 由定理 1.48(4)知 $\operatorname{ord} g^n = \dfrac{m}{(m,n)}$, $\operatorname{ord} h^m = \dfrac{n}{(m,n)}$, $g^n h^m = h^m g^n$, $\left(\dfrac{m}{(m,n)}, \dfrac{n}{(m,n)}\right) = 1$, 故由定理 1.48(6)知

$$o(g^n h^m) = \frac{m}{(m,n)} \cdot \frac{n}{(m,n)} = \frac{[m,n]}{(m,n)}.$$

(2) 设 $m = p_1^{m_1}\cdots p_t^{m_t}$, $n = p_1^{n_1}\cdots p_t^{n_t}$, 其中 $p_1,\cdots,p_t$ 是互不相同的素数, m_i,n_i 均为非负整数. 不妨设 $m_i \geqslant n_i, 1\leqslant i\leqslant l$; $m_i < n_i, l+1\leqslant i\leqslant t$. 令

$$a = p_1^{m_1}\cdots p_l^{m_l}, \quad b = p_{l+1}^{n_{l+1}}\cdots p_t^{n_t}.$$

则由定理 1.48(4)知

$$\operatorname{ord} g^a = \frac{m}{(a,m)} = p_{l+1}^{m_{l+1}}\cdots p_t^{m_t}, \quad \operatorname{ord} h^b = p_1^{n_1}\cdots p_l^{n_l}.$$

这两个阶显然是互素的, 且 g^a 与 h^b 可换, 因此由定理 1.48(6)知

$$\operatorname{ord} g^a h^b = p_1^{n_1}\cdots p_l^{n_l} p_{l+1}^{m_{l+1}}\cdots p_t^{m_t} = (m,n).$$

(3) 设 $m = p_1^{m_1}\cdots p_t^{m_t}$, $n = p_1^{n_1}\cdots p_t^{n_t}$, 其中 $p_1,\cdots,p_t$ 是互不相同的素数, m_i,n_i 均为非负整数. 不妨设 $m_i \geqslant n_i, 1\leqslant i\leqslant l$; $m_i < n_i, l+1\leqslant i\leqslant t$. 令

$$a = p_{l+1}^{m_{l+1}}\cdots p_t^{m_t}, \quad b = p_1^{n_1}\cdots p_l^{n_l}.$$

则由定理 1.48(4)知

$$\operatorname{ord} g^a = \frac{m}{(a,m)} = p_1^{m_1}\cdots p_l^{m_l}, \quad \operatorname{ord} h^b = p_{l+1}^{n_{l+1}}\cdots p_t^{n_t}.$$

这两个阶显然是互素的, 且 g^a 与 h^b 可换, 因此由定理 1.48(6)知

$$\operatorname{ord} g^a h^b = p_1^{m_1}\cdots p_l^{m_l} p_{l+1}^{n_{l+1}}\cdots p_t^{n_t} = [m,n].$$

□

定理 1.49

循环群的任何子群也是循环群. 进而循环群 $\langle a\rangle$ 的所有子群构成的集合为

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

♡

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. 于是 $G_1 \subseteq \{\langle a^r\rangle \mid r = 0, 1, 2\cdots\}$. 因此记 $\langle a\rangle$ 的所有子群构成的集合为 S, 则 $S \subseteq \{\langle a^r\rangle \mid r = 0, 1, 2\cdots\}$. 又显然有 $S \supseteq \{\langle a^r\rangle \mid r = 0, 1, 2\cdots\}$, 故

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

□

推论 1.7

(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 $\mathbb{Z}$ 的任何子群必形如 $m\mathbb{Z}(m \in \mathbb{N}_0)$.

♡

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 1.49有 $m \geqslant 0$且$m \in \mathbb{Z}$, 使得 $G_1 = \langle m\rangle = m\mathbb{Z}$.

□

命题 1.25

设 $m > 0$, 则有

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

♠

证明 由推论 1.7(1)知 $m\mathbb{Z}$ 为 $\mathbb{Z}$ 的子群.

□

定理 1.50

设 $G = \langle a\rangle$ 为循环群, 则有以下结论.

(1) $\langle a^{-1}\rangle = \langle a\rangle$.

(2) 如果 $|G| = \infty$, 则

(i) $G = \{1, a, a^{-1}, a^2, a^{-2}, a^3, a^{-3}, \cdots\}$, 且对 $\forall k, l \in \mathbb{Z}$, 有 $a^k = a^l \iff k = l$.

(ii) a 与 a^{-1} 是 G 的两个仅有的生成元.

(iii) G 的全部子群为 $\{\langle a^d\rangle \mid d = 0, 1, 2, \cdots\}$, 并且对 $\forall d_1, d_2 \in \mathbb{N}_0$且$d_1 \neq d_2$, 有 $\langle a^{d_1}\rangle \neq \langle a^{d_2}\rangle$.

(iv) $G \cong (\mathbb{Z}, +)$.

(3) 如果 $|G| = n < \infty$, 则

(i) $G = \{1, a, a^2, a^3, \cdots, a^{n-1}\}$, 且对 $\forall k, l \in \mathbb{Z}$, 有 $a^k = a^l \iff n \mid k - l$.

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

(iii) G 的全部子群为 $\{\langle a^d\rangle \mid d$ 为 n 的正因子 $\}$, 并且对 $\forall d_1, d_2$ 为 n 的不同正因子, 有 $\langle a^{d_1}\rangle \neq \langle a^{d_2}\rangle$.

若还有正整数 n 的标准分解式为

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

其中 $p_1, p_2, \cdots, p_s$ 是 n 的不同素因子. 则 n 阶循环群 G 的子群的个数为

$$r = (r_1 + 1)(r_2 + 1)\cdots(r_s + 1).$$

(iv) $G \cong \mathbb{Z}_n$.

♡

证明

(1) 由循环群的定义易得.

(2) (i) 由循环群的定义知 $G=\{1,a,a^{-1},a^2,a^{-2},a^3,a^{-3},\cdots\}$. 因为这个集合中的元素互不相同, 所以

$$a^k=a^l \iff a^{k-l}=1 \iff k-l=0 \iff k=l.$$

(ii) 由定理 1.50(1)知 a 与 a^{-1} 都是 G 的生成元. 又如,a^k 是 G 的任一生成元, 则存在 $n\in\mathbb{Z}$, 使

$$(a^k)^n=a^{kn}=a.$$

由定理 1.50(2)(i)得 $kn=1$, 从而 $k=\pm1$.

(iii) 如果 $|G|=\infty$, 由定理 1.49知 G 的所有子群构成的集合为

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

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 $a^r\notin\langle a^0\rangle=\langle 1\rangle=\{1\}$, 所以有

$$\langle a^r\rangle\neq\langle 1\rangle.$$

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

(iv) 证法一:令

$$\begin{aligned}\phi:\mathbb{Z}&\to G,\\ k&\mapsto a^k,\quad \forall k\in\mathbb{Z}.\end{aligned}$$

显然 ϕ 是 $\mathbb{Z}$ 到 G 的良定义的映射;
设 $k,l\in\mathbb{Z}$, 如果 $a^k=a^l$, 则由定理 1.48(4)得,$k=l$, 所以 ϕ 为 $\mathbb{Z}$ 到 G 的单映射;
对任意的 $a^k\in G$, 有 $k\in\mathbb{Z}$, 使 $\phi(k)=a^k$, 所以 ϕ 是 $\mathbb{Z}$ 到 G 的满映射;
对任意的 $k,l\in\mathbb{Z}$,

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

所以 ϕ 是 $\mathbb{Z}$ 到 G 的同构映射. 因此,$G\cong(\mathbb{Z},+)$.
证法二: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 1.7(2)知存在 $m\in\mathbb{N}_0$, 使得 $\ker\varphi=m\mathbb{Z}$. 因此 $G\cong\mathbb{Z}/m\mathbb{Z}$.
若 $m\neq0$, 则由命题 1.25知

$$G\cong\mathbb{Z}/m\mathbb{Z}=\mathbb{Z}_m.$$

从而 $|G|=|\mathbb{Z}_m|=m<\infty$, 这与 $|G|=\infty$ 矛盾! 故此时 $m=0$, 因此 $G\cong\mathbb{Z}$.

(3) (i) 由定理 1.47知 $\operatorname{ord}a=n$, 故 $a^n=1$. 注意到对 $\forall m\in\mathbb{Z}$, 有

$$m\equiv 0 \text{ or } 1 \text{ or } \cdots \text{ or } n-1 \pmod n.$$

故由定理 1.48(2)知

$$a^m=1 \text{ or } a \text{ or } \cdots \text{ or } a^{n-1}.$$

因此 $\langle a\rangle\subseteq\{1,a,\cdots,a^{n-1}\}$. 又显然有 $\langle a\rangle\supseteq\{1,a,\cdots,a^{n-1}\}$, 故 $\langle a\rangle=\{1,a,\cdots,a^{n-1}\}$.
对 $\forall k,l\in\mathbb{Z}$, 由定理 1.48(2)知

$$a^k=a^l \iff k\equiv l \pmod n \iff n\mid k-l.$$

(ii) 由定理 1.48(4)可得 $\operatorname{ord} a^r = \dfrac{n}{(n,r)}$. 再由定理 1.47可得

$$a^r \text{为} G\text{的生成元} \iff \operatorname{ord} a^r = n \iff \frac{n}{(n,r)} = n \iff (n,r) = 1,$$

故由欧拉函数的定义知 G 的生成元的个数为 $\phi(n)$.

(iii) 如果 $|G| = n$, 对任意的正整数 r, 存在 n 的正因子 $d = (n,r)$, 由定理 1.48(8)可知

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

记 G 的所有子群构成的集合为 S, 则由定理 1.49知 $S \subseteq \{\langle a^d \rangle \mid d\text{为}n\text{的正因子}\}$. 又显然有 $S \supseteq \{\langle a^d \rangle \mid d\text{为}n\text{的正因子}\}$, 故

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

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 的不同正因子.

由上述证明知,n 阶循环群 G 的子群的个数恰为 n 的不同正因子的个数. 而 n 的不同正因子的个数等于

$$(r_1 + 1)(r_2 + 1) \cdots (r_s + 1),$$

即得所证.

(iv) 证法一: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 1.7(2)知存在 $m \in \mathbb{N}_0$, 使得 $\ker\varphi = m\mathbb{Z}$. 因此 $G \cong \mathbb{Z}/m\mathbb{Z}$.

若 $m \neq n$, 则当 $m = 0$ 时, 有 $G \cong \mathbb{Z}$, 从而 $|G| = \infty$ 矛盾! 当 $m \neq 0, n$ 时, 有

$$G \cong \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m.$$

从而 $|G| = |\mathbb{Z}_m| = m \neq n$ 矛盾! 故 $m = n$. 因此

$$G \cong \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n.$$

证法二:令

$$\phi : \mathbb{Z}_n \to G,$$
$$\bar{k} \mapsto a^k, \quad \forall \bar{k} \in \mathbb{Z}_n.$$

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

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

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

对任意的 $\bar{k}, \bar{l} \in \mathbb{Z}_n$, 有

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

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

□

推论 1.8

两个循环群同构当且仅当它们的阶相同.

♡

证明 设 G_1, G_2 为两个循环群, 则由定理 1.50(2)(iv)和定理 1.50(3)(iv)以及命题 1.25知

$$G_1 \cong G_2 \iff G_1 \cong G_2 \cong \mathbb{Z}\text{或}G_1 \cong G_2 \cong \mathbb{Z}_m (m \in \mathbb{N})$$
$$\iff |G_1| = |G_2| = \infty\text{或}|G_1| = |G_2| = |\mathbb{Z}_m| = m (m \in \mathbb{N}).$$

□

推论 1.9

(1) 群 G 仅有平凡子群的充分必要条件是 $G=\{1\}$ 或 G 是素数阶循环群.

(2) 无限循环群的非平凡子群仍为无限循环群.

♡

证明

(1) **必要性**: 设 G 仅有平凡子群. 如果 $G=\{1\}$, 则结论成立. 如果 $G\neq\{1\}$, 则存在 $a\in G$, 使 $a\neq 1$, 从而 $\langle a\rangle\neq\{1\}$, 于是由 G 仅有平凡子群知 $\langle a\rangle=G$. 由定理 1.50(2)(iii)可知,G 不可能是无限循环群. 否则, 由定理 1.50(2)(iii)知 G 有无穷多个非平凡子群矛盾! 设 $|G|=n$, 由于 G 仅有平凡子群, 所以再由定理 1.50(3)(iii)知 n 无真因子, 因此 n 为素数.

充分性: 如果 $G=\{1\}$, 则 G 显然只有平凡子群. 如果 G 是素数阶循环群, 则 $|G|$ 的仅有的正因子为 1 及 $|G|$, 由这两个因子得到的都是 G 的平凡子群, 所以再由定理 1.50(3)(iii)知 G 仅有平凡子群.

(2) 设 G 为无限循环群, 则由定理**??**知 $G\cong\mathbb{Z}$. 又由推论 1.7(2)知 $\mathbb{Z}$ 的非平凡子群为 $m\mathbb{Z}(m\in\mathbb{Z}且m\neq 0,1)$ 为无限循环群. 故 G 的非平凡子群也为无限循环群.

□

例题 1.35

(1) 任一偶数阶群必含有阶为 2 的元素.

(2) 设 $n>2$, 则有限群 G 中有偶数个阶为 n 的元.

证明

(1) 设 S 为 G 的所有阶大于 2 的元素的集合,T 为 G 的所有阶小于等于 2 的元素的集合. 如果 S 为空集, 则 $|S|=0$; 如果 S 非空, 则对任意的 $x\in S$, 有 $\operatorname{ord}x^{-1}=\operatorname{ord}x>2$, 所以 $x^{-1}\in S$ 且 $x^{-1}\neq x$, 由此得 $|S|$ 必为偶数. 因为已知 G 的阶为偶数, 所以 G 中阶小于等于 2 的元素的个数 $|T|$ 为偶数. 由于 G 中有且仅有一个阶为 1 的元素, 即 1, 所以 $|T|\neq 0$, 从而 $|T|\geqslant 2$ 且 T 中除 1 外其余元素的阶都是 2. 因此 G 必含有阶为 2 的元素.

(2) 若 G 无 n 阶元, 则结论成立. 若 G 有 n 阶元 g, 设 A 是 G 中所有 n 阶元构成的集合, 则对 $\forall x\in A$, 由定理 1.48(2)有 $\operatorname{ord}a^{-1}=\operatorname{ord}a=n$ 且 $a\neq a^{-1}$, 故 $a^{-1}\in A$. 又因为 $n>2$, 所以 $1\notin A$. 因此 A 中元素都成对出现, 故 $|A|$ 必是偶数.

□

命题 1.26

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

♠

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

(a) 如果 $r=pk$, 则由定理 1.48(4)知 $\operatorname{ord}a^k=\dfrac{r}{(r,k)}=p$, 结论成立.

(b) 如果 $p\nmid r$, 令 $H=\langle a\rangle$, 则由命题 1.8(1)知 H 为 G 的正规子群, 且商群 G/H 为交换群. 而 $|G/H|=\dfrac{n}{r}<n$, 且因 $p\nmid r$, 所以 $p\mid\left(\dfrac{n}{r}\right)$. 从而由归纳假设知, 存在 $bH\in G/H$, 使 $\operatorname{ord}bH=p$, 则 $b^p\in H$. 于是 $b^{pr}=e$. 由于 $p\nmid r$, 所以 $(bH)^r\neq H$, 即 $b^r\notin H$, 于是 $b^r\neq e$. 而 $(b^r)^p=e$, 所以 $\operatorname{ord}b^r=p$.

从而由归纳法原理知结论成立.

□

命题 1.27

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 1.6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 1.4(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 1.24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 1.1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, 由定理 1.10(4)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 1.51

设 G 是一个 m 阶群, 则 G 是循环群的充要条件是对 m 的每个因数 m_1 存在唯一的 m_1 阶子群. ♡

证明 **必要性**: 设 $G = \langle a\rangle$. 从定理 1.47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 $0 < \dfrac{km}{m_1} < m$, 因而 $(a^{\frac{m}{m_1}})^k \neq 1$, 但 $(a^{\frac{m}{m_1}})^{m_1} = 1$, 故 $\langle a^{\frac{m}{m_1}}\rangle$ 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 1.49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 $0 < n < \dfrac{m}{k}$, 则 $0 < kn < m$, 从而 $(a^k)^n = a^{kn} \neq 1$. 另外 $(a^k)^{\frac{m}{k}} = 1$, 故 G_1 的阶为 $\dfrac{m}{k} = m_1$, 因而 $k = \dfrac{m}{m_1}$, 即 $G_1 = \langle a^{\frac{m}{m_1}}\rangle$.

充分性: 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 1.27(3)知 G 必是循环群.

□

第 2 章 群

2.1 群的生成组

定义 2.1

设 S 是群 G 的非空子集, 以 $\langle S\rangle$ 表示 G 的包含 S 的最小子群, 即 S **生成的子群**. 显然,$\langle S\rangle$ 是 G 中所有包含 S 的子群之交, 即 $\langle S\rangle = \bigcap\limits_{S<H} H$.

♣

笔记 由命题 1.7(2)知 $\langle S\rangle = \bigcap\limits_{S<H} H$ 是一个群, 故上述定义是良定义的.

定理 2.1

设 S 是群 G 的非空子集,S^{-1} 是 S 中所有元素的逆元构成的集合, 则

$$\langle S\rangle = \{x_1x_2\cdots x_m \mid x_i \in S\cup S^{-1}, 1\leqslant i\leqslant m, m\in\mathbb{N}\}.$$

进而若 S 在群 H 中, 则 $S\subseteq H$.

♡

证明 令 $\bar{S} = \{x_1x_2\cdots x_m \mid x_i \in S\cup S^{-1}, 1\leqslant i\leqslant m, m\in\mathbb{N}\}$. 由 $\langle S\rangle$ 为子群且 $S\subseteq\langle S\rangle$ 知 $S^{-1}\subseteq\langle S\rangle$, 因而 $S\subseteq\bar{S}\subseteq\langle S\rangle$. 又 $\langle S\rangle$ 是含 S 的最小子群, 故只需证明 $\bar{S}$ 为子群, 则 $\bar{S}\supseteq\langle S\rangle$.

设 $x_1x_2\cdots x_m\in\bar{S}, y_1y_2\cdots y_n\in\bar{S}$, 于是 $y_i^{-1}\in S\cup S^{-1}(1\leqslant i\leqslant m)$, 则有

$$(x_1x_2\cdots x_m)(y_1y_2\cdots y_n)^{-1} = x_1x_2\cdots x_my_n^{-1}y_{n-1}^{-1}\cdots y_2^{-1}y_1^{-1}\in\bar{S},$$

因而 $\bar{S}$ 为 G 的子群, 故 $\bar{S} = \langle S\rangle$.

□

定义 2.2

若 S 为群 G 的子集且 $G = \langle S\rangle$, 则称 S 为 G 的**生成组**. 若 G 有一个含有限个元素的生成组, 则称 G 是**有限生成的**.

若 $G = \langle a\rangle$ 为循环群, 则 a 本身就是生成组, 这时称 a 为 G 的**生成元**.

♣

定义 2.3 (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**, 也称为 n **阶置换群**, 其元素称为**置换**.

♣

定义 2.4

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 2.2

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**或**交代群**, 也称为 n **阶交错群**或**交代群**.

♡

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 $\operatorname{sgn}\tau^{-1} = \operatorname{sgn}\tau, \forall \tau \in S_n$, 故

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

由此知 A_n 为 S_n 的子群.

□

例题 2.1 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

□

例题 2.2 设 $G=S_3$, 又 $a=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, b=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$, 则 $S_3=\langle\{a,b\}\rangle$.

证明 事实上, 设 $G_1=\langle a\rangle$, 注意到

$$a^{-1}=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, a^2=(a^{-1})^2=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},$$

故由定理 2.1知 $G_1=\{a,a^{-1}\}$. 从而 G_1 为 S_3 的 2 阶子群且 $b\notin G_1$, 于是 $G_1\subset\langle\{a,b\}\rangle$. 设 $\langle\{a,b\}\rangle$ 的阶为 n, 则由Lagrange 定理知 $2\mid n$ 且 $2<n$. 又因为 $\langle\{a,b\}\rangle$ 是 G 的子群, 所以由Lagrange 定理知 $n\mid 6$. 因而有 $n=6$, 由此知 $S_3=\langle\{a,b\}\rangle$.

□

定义 2.5

设集合 $\{i_1,i_2,\cdots,i_r\}$ 为集合 $\{1,2,\cdots,n\}$ 的子集. 若 $\sigma\in S_n$ 满足

$$\sigma(i_j)=i_{j+1},\quad 1\leqslant j\leqslant r-1,$$
$$\sigma(i_r)=i_1,$$
$$\sigma(k)=k,\quad k\notin\{i_1,i_2,\cdots,i_r\},$$

则称 σ 为一个**长为 r 的轮换**或 r **轮换**, 这时记 $\sigma=(i_1i_2\cdots i_r)$. 特别地, 将 2 轮换 (ij) 称为**对换**. 将 S_n 中的幺元 id 记为长为 1 的轮换, 即 $\mathrm{id}=(i), i=1,2,\cdots,n$

若 $\sigma=(i_1i_2\cdots i_r)$ 与 $\sigma=(j_1j_2\cdots j_s)$ 是两个轮换且

$$\{i_1,i_2,\cdots,i_r\}\bigcap\{j_1,j_2,\cdots,j_s\}=\varnothing,$$

则称 σ 与 σ 为**不相交的轮换**.

显然, 一个 r 轮换 $(i_1i_2\cdots i_r)$ 有 r 种不同的表示,

$$(i_1i_2\cdots i_r)=(i_2i_3\cdots i_ri_1)=\cdots=(i_ri_1\cdots i_{r-1}).$$

♣

命题 2.1

(1) $[(i_1i_1')(i_2i_2')\cdots(i_ri_r')]^{-1}=(i_ri_r')(i_{r-1}i_{r-1}')\cdots(i_1i_1')$.

(2) $(i_1i_2\cdots i_r)^{-1}=(i_ri_{r-1}\cdots i_1)$. 特别地,$(i_1i_2)^{-1}=(i_2i_1)=(i_1i_2)$.

(3) 任何两个不相交的轮换的乘积是可以交换的.

(4) $(kl)(ka\cdots b)(lc\cdots d)=(ka\cdots blc\cdots d)$, 其中 $a,\cdots,b,c,\cdots,d,k,l$ 为互不相同的正整数.

(5) $(kl)(ka\cdots blc\cdots d)=(ka\cdots b)(lc\cdots d)$, 其中 $a,\cdots,b,c,\cdots,d,k,l$ 为互不相同的正整数.

(6) 对任意 r 轮换 $(i_1i_2\cdots i_r)$ 和 $\sigma\in S_n$, 都有

$$\sigma(i_1i_2\cdots i_r)\sigma^{-1}=(\sigma(i_1)\sigma(i_2)\cdots\sigma(i_r)).$$

(7) 任何轮换 $(i_1i_2\cdots i_r)$ 可写成如下对换之积

$$(i_1i_2\cdots i_r)=(i_1i_2)(i_2i_3)\cdots(i_{r-1}i_r)=(i_1i_r)(i_1i_{r-1})\cdots(i_1i_2).$$

♠

证明

(1)

(2)

(3) 设 $\sigma=(i_1\ i_2\ \cdots\ i_r)$ 与 $\tau=(j_1\ j_2\ \cdots\ j_s)$ 是两个不相交的轮换,a 是 X 中的任意一个数.

(a) 如果 $a\neq i_k, j_l(k=1,2,\cdots,r;l=1,2,\cdots,s)$, 则

$$\sigma\tau(a)=\sigma(a)=a,$$
$$\tau\sigma(a)=\tau(a)=a,$$

所以 $\sigma\tau(a)=\tau\sigma(a)$.

(b) 如果 $a=i_k(1\leqslant k\leqslant r)$, 则 $a,\sigma(a)\neq j_l(l=1,2,\cdots,s)$. 从而

$$\sigma\tau(a)=\sigma(a),$$

$$\tau\sigma(a)=\tau(\sigma(a))=\sigma(a),$$

所以 $\sigma\tau(a)=\tau\sigma(a)$.

(c) 同理可证, 如果 $a=j_l(1\leqslant l\leqslant s)$, 也有 $\sigma\tau(a)=\tau\sigma(a)$.

这就证明了结论.

(4)

(5)

(6) 对 $\forall l\in\{1,2,\cdots,n\}$, 若 $l\notin\{i_1,i_2,\cdots,i_r\}$, 则

$$\sigma(i_1i_2\cdots i_r)\sigma^{-1}(\sigma(l))=\sigma(i_1i_2\cdots i_r)(l)=\sigma(l)=(\sigma(i_1)\sigma(i_2)\cdots\sigma(i_r))(\sigma(l)).$$

若 $l\in\{i_1,i_2,\cdots,i_r\}$, 设 $l=i_j,j\in\{1,2,\cdots,r\}$, 则

$$\sigma(i_1i_2\cdots i_r)\sigma^{-1}(\sigma(i_j))=\sigma(i_1i_2\cdots i_r)(i_j)=\sigma(i_{j+1})=(\sigma(i_1)\sigma(i_2)\cdots\sigma(i_r))(\sigma(i_j)),\ j=1,2,\cdots,r-1;$$

$$\sigma(i_1i_2\cdots i_r)\sigma^{-1}(\sigma(i_r))=\sigma(i_1i_2\cdots i_r)(i_r)=\sigma(i_1)=(\sigma(i_1)\sigma(i_2)\cdots\sigma(i_r))(\sigma(i_r)).$$

故

$$\sigma(i_1i_2\cdots i_r)\sigma^{-1}(\sigma(l))=(\sigma(i_1)\sigma(i_2)\cdots\sigma(i_r))(\sigma(l)),\ \forall l\in\{i_1,i_2,\cdots,i_r\}.$$

即

$$\sigma(i_1i_2\cdots i_r)\sigma^{-1}=(\sigma(i_1)\sigma(i_2)\cdots\sigma(i_r)).$$

(7) 由对换的定义可得

$$(i_1i_2)(i_2i_3)\cdots(i_{r-1}i_r)(i_r)=i_1,$$

$$(i_1i_2)(i_2i_3)\cdots(i_{r-1}i_r)(k)=k,\quad k\notin\{i_1,i_2,\cdots,i_r\}.$$

故 $(i_1i_2\cdots i_r)=(i_1i_2)(i_2i_3)\cdots(i_{r-1}i_r)$.

再利用数学归纳法证明任何轮换 $(i_1i_2\cdots i_r)$ 可写成如下对换之积

$$(i_1i_2\cdots i_r)=(i_1i_r)(i_1i_{r-1})\cdots(i_1i_2).\tag{2.1}$$

当 $r=2$ 时,(2.1)式显然成立. 假设定理对 $r-1(r\geqslant 3)$ 成立, 并记 $a=(i_1i_2\cdots i_r)$, 于是有

$$(i_1i_r)(i_1i_{r-1})\cdots(i_1i_3)(i_1i_2)=(i_1i_3\cdots i_r)(i_1i_2)=a'.$$

当 $j\neq i_k$ 时,$a'(j)=j=a(j)$;

当 $j=i_k(k\geqslant 3)$ 时,$a'(j)=(i_1i_3\cdots i_r)(j)=a(j)$;

当 $j=i_1$ 时,$a'(i_1)=(i_1i_3\cdots i_r)(i_2)=i_2=a(i_1)$;

当 $j=i_2$ 时,$a'(i_2)=(i_1i_3\cdots i_r)(i_1)=i_3=a(i_2)$.

综上知 $a=a'$. 故知式(2.1)成立.

□

定理 2.3 (Ruffini 定理)

设 $a\in S_n$ 且 $a=\sigma_1\sigma_2\cdots\sigma_k$, 其中,$\sigma_i$ 为 r_i 轮换且当 $i\neq j$ 时,σ_i 与 σ_j 不相交,$1\leqslant i,j\leqslant k$, 则 a 的阶为 $r_1,r_2,\cdots,r_k$ 的最小公倍数 $[r_1,r_2,\cdots,r_k]$. 进而 σ_i 的阶为 r_i.

♡

证明 证法一:设 $m=[r_1,r_2,\cdots,r_s]$. 由命题 2.1(3)知不相交轮换的乘积是可以互相交换的, 因此

$$\sigma^m=(\sigma_1\sigma_2\cdots\sigma_s)^m=\sigma_1^m\sigma_2^m\cdots\sigma_s^m=(1),$$

从而 $\mathrm{ord}\sigma\mid m$.

另一方面, 设 $\sigma_1=(i_1\ i_2\ \cdots\ i_{r_1})$, 则对任意的 $i_j\in\{i_1,i_2,\cdots,i_{r_1}\}$, 由于 $\sigma_1,\sigma_2,\cdots,\sigma_s$ 为互不相交的轮换, 因此

$$\sigma_1^{\mathrm{ord}\sigma}(i_j)=\sigma_1^{\mathrm{ord}\sigma}\sigma_2^{\mathrm{ord}\sigma}\cdots\sigma_s^{\mathrm{ord}\sigma}(i_j)=\sigma^{\mathrm{ord}\sigma}(i_j)=i_j.$$

由此推出 $\sigma_1^{\mathrm{ord}\sigma}=(1)$, 从而 $r_1\mid\mathrm{ord}\sigma$. 同理可证 $r_i\mid\mathrm{ord}\sigma(i=1,2,\cdots,s)$. 于是

$$m=[r_1,r_2,\cdots,r_s]\mid\mathrm{ord}\sigma.$$

所以

$$\mathrm{ord}\sigma=[r_1,r_2,\cdots,r_s].$$

证法二: 对因子个数 k 用数学归纳法证明. 当 $k=1$ 时,$a=(i_1i_2\cdots i_{r_1})$ 是一个轮换. 对任何 $s(1\leqslant s\leqslant r_1)$ 有

$$a^s(j)=j,\quad j\neq i_1,i_2,\cdots,i_{r_1},$$

而

$$a^s(i_j)=\begin{cases}i_{s+j}, & j+s\leqslant r_1,\\ i_{s+j-r_1}, & j+s>r_1,\end{cases}$$

于是当 $s<r_1$ 时,$a^s\neq\mathrm{id}$, 而当 $s=r_1$ 时,$a^{r_1}=\mathrm{id}$, 故 a 的阶为 r_1. 由此可知 σ_i 的阶为 r_i.

设 $k-1(k\geqslant 2)$ 时定理成立. 设 $a=\sigma_1\sigma_2\cdots\sigma_k$, 令

$$a_1=\sigma_2\sigma_3\cdots\sigma_k,$$

于是由归纳假设知 a_1 的阶为 $[r_2,r_3,\cdots,r_k]$. 因为 σ_1 与 $\sigma_j(j=2,\cdots,n)$ 不相交, 所以可设 $\sigma_2,\sigma_3,\cdots,\sigma_k$ 中包含的文字 (作用的对象) 为 $\{i_{r_1+1},i_{r_1+2},\cdots,i_t\}$,$\sigma_1$ 中的文字 (作用的对象) 为 $\{i_1,i_2,\cdots,i_{r_1}\}$.

若 $j\neq i_l(1\leqslant l\leqslant t)$, 则 $\sigma_1(j)=a_1(j)=j$, 故 $\sigma_1a_1(j)=a_1\sigma_1(j)=j$.

若 $j=i_l$ 且 $1\leqslant l\leqslant r_1$, 则 $a_1(j)=j,\sigma_1(j)=i_{l'},l'\leqslant r_1$, 因而 $a_1\sigma_1(j)=i_{l'}=\sigma_1a_1(j)$.

若 $j=i_l$ 且 $t\geqslant l\geqslant r_1+1$, 则 $\sigma_1(i_l)=i_l,a_1(i_l)=i_{l'}(t\geqslant l'\geqslant r_1+1)$, 故有 $a_1\sigma_1(j)=i_{l'}=\sigma_1a_1(j)$.

总之有 $a_1\sigma_1=\sigma_1a_1$.

又设 $\beta\in\langle\sigma_1\rangle\cap\langle a_1\rangle$. 由定理 2.1知 $\beta=f_1f_2\cdots f_m$, 其中 $f_i\in\left\{\sigma_1,\sigma_1^{-1}\right\}\cap\left\{a_1,a_1^{-1}\right\},m\in\mathbb{N}$.

若 $j\neq i_l(1\leqslant l\leqslant t)$, 则 $\beta(j)=j$.

若 $j=i_l(1\leqslant l\leqslant r_1)$, 由 $\beta\in\langle a_1\rangle$, 则 $\beta(j)=j$. 若 $j=i_l(t\geqslant l\geqslant r_1+1)$, 由 $\beta\in\langle\sigma_1\rangle$, 则 $\beta(j)=j$.

故 $\beta=\mathrm{id}$, 即有 $\langle\sigma_1\rangle\cap\langle a_1\rangle=\{\mathrm{id}\}$.

设 m 为 $a=a_1\sigma_1$ 的阶, 则再由 $a_1\sigma_1=\sigma_1a_1$ 可得

$$a^m=a_1^m\sigma_1^m=\sigma_1^ma_1^m=\mathrm{id}.$$

因此 $\sigma_1^m=a_1^{-m}\in\langle\sigma_1\rangle\cap\langle a_1\rangle$. 又由 $\langle\sigma_1\rangle\cap\langle a_1\rangle=\{\mathrm{id}\}$ 知 $\sigma_1^m=a_1^{-m}=\mathrm{id}$, 从而 m 是 σ_1,a_1 的阶的公倍数, 即 $m\mid r_1,m\mid[r_2,\cdots,r_k]$. 再设 n 也是 $r_1,[r_2,\cdots,r_k]$ 的公倍数, 则

$$\sigma_1^n=a_1^n=\mathrm{id}\Longrightarrow a^n=\sigma_1^na_1^n=\mathrm{id}.$$

故 $m\mid n$. 因而 $a=\sigma_1a_1$ 的阶为 $[r_1,[r_2,\cdots,r_k]]=[r_1,r_2,\cdots,r_k]$.

□

定理 2.4

(1) 任意 n 阶置换 $a\in S_n$ 一定可写成互不相交的轮换之积. 即存在互不相交的轮换 $\sigma_1,\sigma_2,\cdots,\sigma_r$, 使得

$$a=\sigma_1\sigma_2\cdots\sigma_r.\tag{2.2}$$

(2) 设 σ 为一个 n 阶置换, 由定理 2.4(1)可设 σ 可表为不相交轮换 (包括 1 轮换) 的乘积

$$\sigma=\sigma_1\sigma_2\cdots\sigma_s,$$

在集合 $X=\{1,2,\cdots,n\}$ 中, 规定关系 “$\sim$”:

$$k\sim l\iff r\in\mathbb{Z},\ \sigma^r(k)=l.$$

(i) 证明: $\sim$ 是 X 的一个等价关系;

(ii) 证明: $k \sim l$ 的充分必要条件是 k 与 l 属于 σ 的同一个轮换. 进而 X 的所有等价类为

$$\{k \in \mathbb{N} \mid k \in \sigma_i\}, \quad i = 1, 2, \cdots, s.$$

(3) 如果不考虑因子的次序和乘积中 1 轮换的个数, 则分解式(2.2)是唯一的. ♡

注 在(2)定义的等价关系下, 对于置换

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 2 & 6 & 8 & 9 & 1 & 7 & 10 & 4 & 5 \end{pmatrix},$$

由于

$$\sigma = (1\ 3\ 6)(4\ 8\ 10\ 5\ 9)(2)(7),$$

所以集合 X 的所有等价类为

$$[2] = \{2\}, \quad [7] = \{7\}, \quad [1] = \{1, 3, 6\}, \quad [4] = \{4, 5, 8, 9, 10\}.$$

证明

(1) 证法一:对 X 的元素个数 n 用数学归纳法. 当 $n = 1$ 时,1 阶置换只有 $a = (1)$, 已经是轮换, 因此结论对 $n = 1$ 成立. 假定结论对 $n - 1$ 成立, 考察 n 阶置换

$$a = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ i_1 & i_2 & \cdots & i_{n-1} & i_n \end{pmatrix}.$$

(a) 如果 $i_n = n$, 即

$$a = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ i_1 & i_2 & \cdots & i_{n-1} & n \end{pmatrix}.$$

令

$$a_1 = \begin{pmatrix} 1 & 2 & \cdots & n-1 \\ i_1 & i_2 & \cdots & i_{n-1} \end{pmatrix},$$

则 a_1 是一个 $n - 1$ 阶置换. 由归纳假设,a_1 可表为一些不相交轮换的乘积

$$a_1 = \sigma_1\sigma_2\cdots\sigma_s.$$

将 σ_i 看作 n 阶置换, 即得

$$a = \sigma_1\sigma_2\cdots\sigma_s \cdot (n) = \sigma_1\sigma_2\cdots\sigma_s.$$

(b) 如果 $i_n \neq n$, 则有某个 $k(1 \leqslant k \leqslant n-1)$, 使得 $i_k = n$. 令

$$\beta = (i_k\ i_n)a = \begin{pmatrix} 1 & 2 & \cdots & k-1 & k & k+1 & \cdots & n-1 & n \\ i_1 & i_2 & \cdots & i_{k-1} & i_n & i_{k+1} & \cdots & i_{n-1} & n \end{pmatrix}.$$

由 (a) 所证,β 可表为一些不相交轮换的乘积. 设

$$\beta = a_1a_2\cdots a_s,$$

其中,$a_1, a_2, \cdots, a_s$ 为互不相交的轮换, 则

$$a = (i_k\ i_n)a_1a_2\cdots a_s.$$

如果每个 a_i 都不与 $(i_k\ i_n)$ 相交, 则

$$a = (i_k\ i_n)a_1a_2\cdots a_s$$

为不相交轮换的乘积. 如果有某个 a_i 与 $(i_k\ i_n)$ 相交, 则至多有一个 a_i 与 $(i_k\ i_n)$ 相交. 不妨设 $a_1 = (i_n\ a\ \cdots\ b)$, 则

$$a = (i_k\ i_n)(i_n\ a\ \cdots\ b)a_2a_3\cdots a_s$$

$$= (i_k\ i_n\ a\ \cdots\ b)a_2a_3\cdots a_s$$

为不相交轮换的乘积. 从而由归纳法知结论成立.

证法二:设 $a \in S_n$, 令 $\bar{F}_a = \{j \mid a(j) \neq j\}$. 显然有

$$\bar{F}_{\mathrm{id}} = \varnothing. \tag{2.3}$$

当 $a \neq \mathrm{id}$ 时,

$$|\bar{F}_a| \geqslant 2 \tag{2.4}$$

当且仅当 a 为对换时, 式(2.4)中等号成立. 下面不妨设 $a \neq \mathrm{id}$. 证明存在轮换 σ_1 满足

$$\begin{cases} \bar{F}_a = \bar{F}_{\sigma_1} \cup \bar{F}_{\sigma_1^{-1}a}, \\ \bar{F}_{\sigma_1} \cap \bar{F}_{\sigma_1^{-1}a} = \varnothing. \end{cases} \tag{2.5}$$

因 $a \neq \mathrm{id}$, 故由式(2.4)知有 $i_1 \in \bar{F}_a$. 令

$$i_2 = a(i_1), \quad i_3 = a(i_2), \quad \cdots, \quad i_k = a(i_{k-1}),$$

则 $i_1 \neq i_2$. 由于 $\bar{F}_a$ 是有限集, 故存在 $r \geqslant 3$, 使得 $i_1, i_2, \cdots, i_{r-1}$ 互不相同, 而 $i_r = i_t (1 \leqslant t \leqslant r-1)$. 现证 $t = 1$. 若不然, 则有

$$a(i_{t-1}) = i_t = i_r = a(i_{r-1}).$$

于是

$$i_{t-1} = i_{r-1},$$

即有 $t = r$, 矛盾, 故 $t = 1$. 令 $\sigma_1 = (i_1 i_2 \cdots i_{r-1})$, 显然

$$\sigma_1(i_k) = a(i_k),\ 1 \leqslant k \leqslant r-1, \quad \bar{F}_{\sigma_1} = \{i_1, i_2, \cdots, i_{r-1}\} \subseteq \bar{F}_a.$$

再令 $a_1 = \sigma_1^{-1}a$, 若 $l \notin \bar{F}_a$, 则 $l \notin \bar{F}_{\sigma_1^{-1}}$, 故 $a_1(l) = l (l \notin \bar{F}_{a_1})$, 因而 $\bar{F}_{a_1} \subseteq \bar{F}_a$. 于是 $\bar{F}_{a_1} \cup \bar{F}_{\sigma_1} \subseteq \bar{F}_a$. 反之, 若 $l \notin \bar{F}_{a_1} \cup \bar{F}_{\sigma_1}$, 则有 $a_1(l) = \sigma_1(l) = l$, 故 $a(l) = a_1\sigma_1^{-1}(l) = l$, 即 $l \notin \bar{F}_a$. 于是式(2.5)中第一个等式成立.

设 $i_k \in \bar{F}_{\sigma_1}$, 则有 $a_1(i_k) = \sigma_1^{-1}a(i_k) = \sigma_1^{-1}\sigma_1(i_k) = i_k$, 即 $i_k \notin \bar{F}_{a_1} = \bar{F}_{\sigma_1^{-1}a}$. 故(2.5)式中第二个等式也成立.

若 $a \neq \sigma_1$, 则 $\bar{F}_{\sigma_1^{-1}a} \neq \bar{F}_{\mathrm{id}} = \varnothing$. 从而 $\bar{F}_{\sigma_1^{-1}a} \neq \bar{F}_a$, 否则由(2.5)式知 $\bar{F}_{\sigma_1} = \varnothing$, 即 $\sigma_1 = \mathrm{id}$, 这与 $i_1, i_2, \cdots, i_{r-1}$ 互不相同矛盾! 再对 $\sigma_1^{-1}a$ 用上述方法同理可得另一轮换 $\sigma_2 = (j_1 j_2 \cdots j_{l-1})$, 使得

$$\bar{F}_{\sigma_2} = \{j_1, j_2, \cdots, j_{l-1}\} \subseteq \bar{F}_{\sigma_1^{-1}a}, \tag{2.6}$$

并且

$$\begin{cases} \bar{F}_{\sigma_1^{-1}a} = \bar{F}_{\sigma_2} \cup \bar{F}_{\sigma_2^{-1}\sigma_1^{-1}a}, \\ \bar{F}_{\sigma_2} \cap \bar{F}_{\sigma_2^{-1}\sigma_1^{-1}a} = \varnothing. \end{cases}$$

若 $a \neq \sigma_1\sigma_2$, 则同理有 $\bar{F}_{\sigma_2^{-1}\sigma_1^{-1}a} \neq \bar{F}_{\sigma_1^{-1}a}$. 从而 $\bar{F}_{\sigma_2^{-1}\sigma_1^{-1}a} \subset \bar{F}_{\sigma_1^{-1}a} \subset \bar{F}_a$. 由(2.5)式和(2.6)式知

$$\{i_1, i_2, \cdots, i_{r-1}\} \cap \{j_1, j_2, \cdots, j_{l-1}\} = \bar{F}_{\sigma_1} \cap \bar{F}_{\sigma_2} = \varnothing,$$

故 σ_1 与 σ_2 为不相交的轮换. 继续做下去. 由于 $\bar{F}_a$ 是有限的, 最后有 $s \in \mathbb{N}$, 使得互不相交的轮换 $\sigma_1, \sigma_2, \cdots, \sigma_s$ 满足

$$\bar{F}_{\sigma_s^{-1}\sigma_{s-1}^{-1}\cdots\sigma_1^{-1}a} = \varnothing,$$

即 $\sigma_s^{-1}\sigma_{s-1}^{-1}\cdots\sigma_1^{-1}a = \mathrm{id}$, 因而

$$a = \sigma_1\sigma_2\cdots\sigma_s,$$

即 S_n 中任何元素可表为互不相交的轮换之积.

(2) (i) 设 $\mathrm{ord}\,\sigma = m$, 对 $\forall j, k, l \in X$.

因为 $\sigma^m(j) = (1)j = j$, 所以 $j \sim j$, 于是 $\sim$ 具有反身性;

如果 $k \sim l$, 则存在 $r \in \mathbb{Z}$, 使 $\sigma^r(k) = l$, 于是 $\sigma^{-r}(l) = k$, 从而 $l \sim k$, 这说明 $\sim$ 具有对称性;

如果 $j \sim k, k \sim l$, 则存在 $r_1, r_2 \in \mathbb{Z}$, 使 $\sigma^{r_1}(j) = k, \sigma^{r_2}(k) = l$, 于是 $\sigma^{r_1+r_2}(j) = l$, 从而 $j \sim l$, 这说明 $\sim$ 具有传递性.

这就证明了 $\sim$ 是 X 的一个等价关系.

(ii) **必要性**: 设 $k \sim l$, 则存在 $r \in \mathbb{Z}$, 使 $\sigma^r(k) = l$. 设 k 属于轮换 σ_i, 则

$$l = \sigma^r(k) = (\sigma_1\sigma_2\cdots\sigma_s)^r(k) = \sigma_1^r\sigma_2^r\cdots\sigma_s^r(k) = \sigma_i^r(k),$$

即 l 也属于轮换 σ_i, 从而 k 与 l 属于 σ 的同一个轮换.

充分性: 如果 k 与 l 属于 σ 的同一个轮换 σ_i, 则必有 $r \in \mathbb{Z}$, 使 $\sigma_i^r(k) = l$, 从而

$$l = \sigma_i^r(k) = \sigma_1^r\sigma_2^r\cdots\sigma_s^r(k) = (\sigma_1\sigma_2\cdots\sigma_s)^r(k) = \sigma^r(k),$$

所以 $k \sim l$.

(3) 设 σ 为任一 n 阶置换,

$$\sigma = \sigma_1\sigma_2\cdots\sigma_s = \delta_1\delta_2\cdots\delta_t.$$

是 σ 的两个表为不相交轮换 (包括 1 轮换) 的乘积的分解式, 则 σ 在集合 $X = \{1, 2, \cdots, n\}$ 上规定关系 "$\sim$"

$$k \sim l \iff r \in \mathbb{Z},\ \sigma^r(k) = l.$$

由定理 2.4(2)(ii)知, 在此等价关系之下, 集合 X 的等价类的个数等于 σ 分解为不相交轮换 (包括 1 轮换) 的乘积的因子数, 所以 $s = t$. 又由定理 2.4(2)(ii)知,X 的一个等价类由属于 σ 的同一个轮换中的元素组成. 因此, 适当交换因子的次序, 可使 σ_i 与 δ_i 含有 X 的同一个等价类 X_i 中的元素. 从而, 对任意的 $x \in X$, 如果 $x \notin X_i$, 则有

$$\sigma_i(x) = x = \delta_i(x).$$

如果 $x \in X_i$, 也有

$$\sigma_i(x) = \sigma_1\sigma_2\cdots\sigma_s(x) = \sigma(x) = \delta_1\delta_2\cdots\delta_s(x) = \delta_i(x).$$

因此 $\sigma_i = \delta_i (i = 1, 2, \cdots, s)$. 这就证明了分解的唯一性.

□

推论 2.1

(1) 任何置换都可写成对换之积. 并且令 $S = \{(1i) \mid 2 \leqslant i \leqslant n\}$, 则有 $S_n = \langle S \rangle$.

(2) 将一个置换写成对换的乘积, 所用对换个数的奇偶性是唯一的.

♡

注 由定理 2.4(1)和命题 2.1(7)知, 任何置换至少可分解成两个不同的对换之积 (这里 (1) 中只证明了其中一种).

证明

(1) 由定理 2.4(1)知任何置换可分解为不相交的轮换之积, 又由命题 2.1(7)知任何轮换可分解为对换之积, 故任何置换都可分解为对换之积.

事实上,

$$(ij) = (1i)(1j)(1i). \tag{2.7}$$

由定理 2.4(1)知 $\forall a \in S_n$ 一定可写成轮换之积, 从而由命题 2.1(7)知 a 可写成对换之积. 再利用(2.7)式知 a 可写成 S 中元素之积, 再由定理 2.1可知 $a \in \langle S \rangle$, 即 $\langle S \rangle \supseteq S_n$. 又显然有 $\langle S \rangle \subseteq S_n$, 故 $\langle S \rangle = S_n$.

(2) 设 σ 为任一 n 阶置换, 并设 σ 已表为 s 个不相交轮换 (包括 1 轮换) 之积:$\sigma = \tau_1\tau_2\cdots\tau_s$. 定义

$$\mathcal{N}(\sigma) = (-1)^{n-s}.$$

显然 $\mathcal{N}(\sigma)$ 由 σ 唯一确定. 设 (ab) 为任一对换, 考察乘积 $(ab)\sigma$. 下证

$$\mathcal{N}((ab)\sigma) = -\mathcal{N}(\sigma). \tag{2.8}$$

如果 a, b 处于 σ 的同一个轮换

$$\tau_1 = (ac_1c_2\cdots c_kbd_1d_2\cdots d_h)$$

中, 则由命题 2.1(5)知

$$(ab)\sigma = (ac_1c_2\cdots c_k)(bd_1d_2\cdots d_h)\tau_2\tau_3\cdots\tau_s.$$

从而

$$\mathcal{N}((ab)\sigma) = (-1)^{n-s-1} = -\mathcal{N}(\sigma).$$

如果 a, b 分别处于 σ 的两个不同轮换

$$\tau_1 = (ac_1c_2\cdots c_k), \quad \tau_2 = (bd_1d_2\cdots d_h)$$

中, 则由命题 2.1(4)知

$$(ab)\sigma = (ac_1c_2\cdots c_kbd_1d_2\cdots d_h)\tau_3\tau_4\cdots\tau_s.$$

从而

$$\mathcal{N}((ab)\sigma) = (-1)^{n-s+1} = -\mathcal{N}(\sigma).$$

故(2.8)式成立.

设 σ 可分别表示为 h 个对换和 k 个对换的乘积

$$\sigma = (a_1b_1)(a_2b_2)\cdots(a_hb_h) = (c_1d_1)(c_2d_2)\cdots(c_kd_k),$$

则由(2.8)式可得

$$\mathcal{N}(\sigma) = \mathcal{N}(\sigma\cdot(1)) = \mathcal{N}((a_1b_1)(a_2b_2)\cdots(a_hb_h)\cdot(1)) = (-1)^h\mathcal{N}((1)) = (-1)^h.$$

由(2.8)式同理可得

$$\mathcal{N}(\sigma) = (-1)^k.$$

因此 $(-1)^h = (-1)^k$, 所以 h 与 k 有相同的奇偶性.

□

推论 2.2

(1) 对换都是奇置换.

(2) 置换是偶 (奇) 置换当且仅当其可表示为偶 (奇) 数个对换之积.

(3) 轮换是奇 (偶) 置换当且仅当其长度为偶 (奇) 数.

(4) 任何两个偶 (奇) 置换之积是偶置换.

(5) 一个偶置换与一个奇置换之积是奇置换.

(6) 一个偶 (奇) 置换的逆置换仍是一个偶 (奇) 置换.

(7) 置换 σ 与 σ^{-1} 具有相同的奇偶性.

♡

证明

(1) 由定理 2.2中奇置换定义知对换显然都是奇置换.

(2) 设 $\sigma \in S_n$, 则由推论 2.1知 $\sigma = \sigma_1\sigma_2\cdots\sigma_k$, 其中 σ_i 都是对换. 又注意到对换 $\sigma_i = (ij)$ 都是奇置换, 故 $\mathrm{sgn}\sigma_i = -1$. 由定理 2.2知 sgn 是 S_n 到 $\{-1, 1\}$ 的同态, 因此

$$\mathrm{sgn}\sigma = \mathrm{sgn}(\sigma_1\sigma_2\cdots\sigma_k) = (\mathrm{sgn}\sigma_1)(\mathrm{sgn}\sigma_2)\cdots(\mathrm{sgn}\sigma_k) = (-1)^k.$$

故 σ 是奇置换当且仅当 $\mathrm{sgn}\sigma = (-1)^k = -1$ 当且仅当 k 为奇数;

σ 是偶置换当且仅当 $\mathrm{sgn}\sigma = (-1)^k = 1$ 当且仅当 k 为偶数.

(3) 设 r 轮换 $(i_1i_2, \cdots i_r)$, 则由命题 2.1(7)知

$$(i_1i_2\cdots i_r) = (i_1i_r)(i_1i_{r-1})\cdots(i_1i_2).$$

由定理 2.2知 sgn 是 S_n 到 $\{-1, 1\}$ 的同态, 因此

$$\mathrm{sgn}(i_1i_2\cdots i_r) = \mathrm{sgn}(i_1i_r)\cdot\mathrm{sgn}(i_1i_{r-1})\cdots\mathrm{sgn}(i_1i_2) = (-1)^{r-1}.$$

故 $(i_1 i_2, \cdots i_r)$ 为偶置换当且仅当 $\operatorname{sgn}(i_1 i_2 \cdots i_r) = (-1)^{r-1} = 1$ 当且仅当 r 是奇数;
若 $(i_1 i_2, \cdots i_r)$ 为奇置换当且仅当 $\operatorname{sgn}(i_1 i_2 \cdots i_r) = (-1)^{r-1} = -1$ 当且仅当 r 是偶数;

(4)

(5)

(6)

(7) 如果 σ 可表示为 k 个对换的乘积

$$\sigma = (i_1\ j_1)(i_2\ j_2)\cdots(i_k\ j_k),$$

则

$$\sigma^{-1} = (i_k\ j_k)(i_{k-1}\ j_{k-1})\cdots(i_1\ j_1)$$

也可表示为 k 个对换的乘积. 所以 σ 与 σ^{-1} 具有相同的奇偶性.

□

定理 2.5

设 S_X 是置换群, 则有以下结论

(1) 若 S_X 中存在奇置换, 则 S_X 中奇置换的个数与偶置换的个数相同. 特别地, 在全体 n 阶置换 S_n 中, 奇置换与偶置换各有 $\frac{n!}{2}$ 个, 进而 $|A_n| = \frac{n!}{2}$.

(2) S_X 中所有偶置换的集合 H 是 S_X 的子群.

♡

证明

(1) 设 S_X 中有奇置换. 由于 S_X 是置换群, 所以 $(1) \in S_X$, 而 (1) 为偶置换. 所以 S_X 中既有奇置换又有偶置换. 以 O 与 E 分别表示 S_X 中奇置换与偶置换的集合. 设 σ 为 S_X 的任一奇置换, 则由推论 2.2(4)和推论 2.2(5)可得

$$\sigma O = \{\sigma\delta \mid \delta \in O\} \subseteq E,$$

$$\sigma E = \{\sigma\tau \mid \tau \in E\} \subseteq O.$$

因此

$$|O| = |\sigma O| \leqslant |E|, \quad |E| = |\sigma E| \leqslant |O|,$$

由此得 $|O| = |E|$. 这就证明了结论.

(2) 因 $(1) \in G$ 为偶置换, 所以 $(1) \in H$, 从而 H 非空. 又由推论 2.2(4)知两个偶置换的乘积仍是偶置换, 所以 H 关于置换的乘积封闭. 从而由命题 1.7(1)知 H 为 G 的子群.

□

例题 2.3 把下列置换分别写成不相交的轮换的乘积和对换的乘积, 并计算置换的奇偶性:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 6 & 5 & 2 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 4 & 1 & 5 & 3 \end{pmatrix}.$$

解 注意到

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 6 & 5 & 2 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 4 & 1 & 5 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 5 & 2 & 1 \end{pmatrix} = (1\ 6)(2\ 4\ 5).$$

再由命题 2.1(7)知

$$(1\ 6)(2\ 4\ 5) = (1\ 6)(2\ 4)(4\ 5) \quad \text{or} \quad (1\ 6)(2\ 5)(2\ 4).$$

故由推论 2.2(2)知这个置换是奇置换.

□

2.2 群集合上的作用

定义 2.6 (群作用)

设 G 是一个群,X 是一个非空集合. 若 $G\times X$ 到 X 的映射 f 满足

(1) $f(e,x)=x,\forall x\in X,e$ 为 G 的幺元;

(2) $f(g_1g_2,x)=f(g_1,f(g_2,x)),\forall g_1,g_2\in G,x\in X,$

则称 f 决定了**群 G 在 X 上的一个作用**.

群 G 可以多种方式作用在一个集合 X 上. 在不需要特别指出映射 f(即固定好一种作用方式) 时, 常记

$$f(g,x)=g(x),\quad \forall g\in G,x\in X.$$

此时 f 满足的条件 (1), (2) 相应地变为

(1) $e(x)=x,\forall x\in X,e$ 为 G 的幺元;

(2) $g_1g_2(x)=g_1(g_2(x)),\forall x\in X,g_1,g_2\in G.$

♣

定理 2.6

1. 设 G 是一个群, 取 $X=G$,

   (a). 若定义 f 为

   $$f(g,x)=L_g(x)=gx,\quad \forall g,x\in G.$$

   则 f 定义了 G 在 G 上的一个作用, 这种作用称为**左平移作用**.

   (b). 若定义 f_1 为

   $$f_1(g,x)=R_{g^{-1}}(x)=xg^{-1},\quad \forall g,x\in G,$$

   则 f_1 也定义了 G 在 G 上的一个作用, 这种作用称为**右平移作用**.

   (c). 若定义 f_2 为

   $$f_2(g,x)=\mathrm{ad}g(x)=gxg^{-1},\quad \forall g,x\in G,$$

   则 f_2 也定义了 G 在 G 上的一个作用, 称为**伴随作用**.

2. 设 H 为群 G 的子群, 取 $X=G/H$(H 在 G 中全体左陪集的集合). 定义 f 为

   $$f(g,xH)=gxH,\quad \forall g\in G,xH\in G/H,$$

   则 f 定义了 G 在 G/H 上的作用 (**左平移作用**). 特别地, 当 $H=\{e\}$ 时,f 恰是 G 在 G 上的左平移作用.

♡

证明

□

定义 2.7

设群 G 作用在集合 X 上. 若 $\forall x,y\in X,\exists g\in G$, 使 $y=g(x)$, 则称 G 在 X 上的作用是**可递的**,X 称为 (对于 G 的) **齐性空间**.

♣

定义 2.8

设群 G 作用在集合 X 上. 若 $g(x)=x(\forall g\in G,\forall x\in X)$, 则称 G 在 X 上的作用是**平凡的**.

♣

注 显然, 对任意群 G, 任意非空集合 X, 总可定义 G 在 X 上的平凡作用. 由上述定义知 G 在 G 上的伴随作用为平凡作用当且仅当 G 为 Abel 群.

定义 2.9

设群 G 作用在集合 X 上,e 为 G 的幺元, 若当且仅当 $g=e$ 时,$g(x)=x(\forall x\in X)$ 成立, 则称 G 在 X 上的作用是**有效的**.

♣

命题 2.2

群 G 在 G 上的左平移作用与右平移作用既是可递的又是有效的, 而 G 在 G/H 上的左平移作用是可递的.

♠

注 G 在 G 上的伴随作用的可递性与有效性都不能肯定.

G 在 G/H 上的左平移作用不一定是有效的.

证明

□

定义 2.10

设群 G 作用在集合 X 上,$x\in X$. 称 X 中的子集

$$O_x=\{g(x)\in X\mid g\in G\}$$

为 x 的**轨道**. G 中子集

$$S_x=\{g\in G\mid g(x)=x\}$$

称为 x 的**迷向子群**. 也称为 x 在 G 中的**稳定子**或**稳定化子**.

♣

注 容易验证 x 的迷向子群是 G 的子群.

命题 2.3

群 G 在集合 X 上的作用是可递的充要条件是对 $\forall x\in X$, 有 $X=O_x$.

进而对 $\forall x\in X$,G 在 O_x 上的作用都是可递的.

♠

证明 **必要性**: 对 $\forall x\in X$, 固定 x. 再对 $\forall y\in X$, 则由 G 在 X 上的作用是可递的知, 存在 $g\in G$, 使得 $y=g(x)\in O_x$. 故由 y 的任意性知 $X\subseteq O_x$. 又显然 $O_x\subseteq X$, 故 $X=O_x$.

充分性: 若对 $\forall x\in X$, 有 $X=O_x$, 则对 $\forall y\in X$, 都存在 $g\in G$, 使得 $y=g(x)$. 因此由 x,y 的任意性知 G 在 X 上的作用是可递的.

□

例题 2.4 设 $X=\mathbb{R}^n$ 为 n 维 Euclid 空间,$G=SO(n)$ 为 X 的特殊正交群,G 以通常方式作用在 X 上. 又设 $X=(1,0,\cdots,0)'$, 则易得

$$O_x=\{\boldsymbol{y}\mid \boldsymbol{y}\in X,|\boldsymbol{y}|=1\}=S^{n-1}$$

是 X 中 $n-1$ 维单位球面, 其中,$|\boldsymbol{y}|$ 为向量 $\boldsymbol{y}$ 的长度,

$$S_x=\{\mathrm{diag}(1,A)\mid A\in SO(n-1)\},$$

故 S_x 与 $n-1$ 维特殊正交群 $SO(n-1)$ 同构.

证明

□

定理 2.7

设群 G 作用在集合 X 上. 则有

(1) $O_x=O_y\iff O_x\cap O_y\neq\varnothing$.

(2) 在 X 中定义关系 R:

$$xRy\iff \exists g\in G,\text{使}y=g(x).$$

则 R 为等价关系且 x 所在的等价类为 x 的轨道 O_x, 进而 X 等价类 (所有轨道) 集合是 X 的一个分划. 即 X 是所有不同轨道的并

$$X = \bigsqcup_x O_x,$$

其中 x 取遍 X 的不同轨道的代表元素.

(3) 如果 X 为有限集, 则

$$|X| = \sum_{x\in X} |O_x|,$$

其中 x 取遍 X 的不同轨道的代表元素. ♡

证明

(1) 设 $O_x \cap O_y \neq \varnothing$. 任取 $z \in O_x \cap O_y$, 则存在 $g_1, g_2 \in G$, 使

$$g_1 x = z = g_2 y.$$

于是 $y = g_2^{-1} g_1 x \in O_x$, 由此得 $O_y \subseteq O_x$. 同理可证 $O_x \subseteq O_y$. 所以 $O_x = O_y$.

(2) 对 $\forall x, y, z \in X$, 由 $e(x) = x$ 知 xRx $(\forall x \in X)$, 由 $g(x) = y$ 得 $g^{-1}(y) = g^{-1}(g(x)) = g^{-1}g(x) = x$, 即 $xRy \Rightarrow yRx$, 再由 xRy, yRz 知 $\exists g_1, g_2 \in G$, 使得 $y = g_1(x), z = g_2(y)$, 故 $z = g_2 g_1(x)$, 即 xRz. 这就说明 R 是等价关系, 由 R 的定义知 x 的等价类为 O_x.

(3) 因为 X 是有限集, 所以至多只有有限多个不同的轨道. 由定理 2.7(2)知

$$X = \bigsqcup_{x\in X} O_{x_i}.$$

其中 x 取遍 X 的不同轨道的代表元素. 又因为 $O_{x_i} \cap O_{x_j} = \varnothing (i \neq j)$, 所以

$$|X| = \sum_{x\in X} |O_x|.$$

□

定理 2.8

设群 G 作用在集合 X 上.

(1) 对 $\forall g \in G$, 定义 X 到 X 的映射 σ 满足

$$\sigma_g(x) = g(x), \quad \forall x \in X \tag{2.9}$$

则定义的 σ_g 是 X 的可逆变换, 即 $\sigma_g \in S_X$.

(2) 定义的 G 到 S_X 的映射 σ 满足

$$\sigma(g) = \sigma_g, \forall g \in G.$$

其中 σ_g 的定义如(2.9)式. 则

(i) σ 是一个同态映射, 并且 G 在 X 上的作用有效当且仅当 σ 是单同态.

(ii) $\ker\sigma \lhd G$, G 在 O_x 上作用有效当且仅当 S_x 中所包含的 G 的正规子群仅为 $\{e\}$.

(3) 若 σ 是群 G 到 S_X 的同态, 则由

$$g(x) = \sigma(g)(x), \quad \forall g \in G, x \in X \tag{2.10}$$

定义了 G 在 X 的作用. ♡

证明

(1) 任取 $g \in G$, 由式(2.9)有

$$\sigma_{g^{-1}}\sigma_g(x) = g^{-1}(g(x)) = g^{-1}g(x) = e(x) = x, \quad \forall x \in X.$$

同样有

$$\sigma_g\sigma_{g^{-1}}(x)=x,\quad \forall x\in X.$$

故

$$\sigma_{g^{-1}}\sigma_g=\sigma_g\sigma_{g^{-1}}=\mathrm{id}_X,$$

因而 $\sigma_g\in S_X$ 且 $\sigma_{g^{-1}}=\sigma_g^{-1}$.

(2) (i) 取 $g_1,g_2\in G$, 对 $\forall x\in X$ 有

$$\sigma(g_1g_2)(x)=\sigma_{g_1g_2}(x)=g_1g_2(x)=g_1(g_2(x))=\sigma_{g_1}(\sigma_{g_2}(x))=\sigma_{g_1}\sigma_{g_2}(x)=\sigma(g_1)\sigma(g_2)(x),$$

即

$$\sigma(g_1g_2)=\sigma(g_1)\sigma(g_2),\quad \forall g_1,g_2\in G,$$

因而 σ 是 G 到 S_X 的同态. 注意到

$$g\in\ker\sigma\iff\sigma(g)=\sigma_g=\mathrm{id}_X,$$

即

$$g(x)=x,\quad \forall x\in X,$$

故 G 在 X 上作用有效当且仅当 $\ker\sigma=\{e\}$, 即 σ 是单射.

(ii) 设 σ 为 G 到 S_{O_x} 的映射, 满足 $\sigma(g)y=g(y)(\forall y\in O_x)$. 于是由定理 2.8知 σ 是同态且 G 在 O_x 上作用有效当且仅当 $\ker\sigma=\{e\}$. 由命题 1.21(1)知道 $\ker\sigma\lhd G$. 注意到

$$g\in\ker\sigma\iff\sigma(g)=\mathrm{id}_X\iff g(x)=x(\forall x\in X)\iff g\in S_x.\tag{2.11}$$

故 $\ker\sigma\subseteq S_x$, 因而若 S_x 中所含 G 的正规子群仅为 $\{e\}$, 则必有 $\ker\sigma=\{e\}$. 从而 G 在 O_x 上作用有效. 设 $N\lhd G, N\subseteq S_x$. 任取 $h\in N$, 对 $\forall y\in O_x$, 都存在 $g\in G$, 使得 $y=g(x)$. 由 $N\lhd G$ 知 $g^{-1}hg\in N\subseteq S_x$, 因而

$$h(y)=h(g(x))=gg^{-1}hg\,(x)=g(g^{-1}hg(x))=g(x)=y,\quad \forall y\in O_x.$$

由(2.11)式知 $h\in\ker\sigma$, 即 $N\subseteq\ker\sigma$. 所以若 G 在 O_x 上作用有效, 则 $\ker\sigma=\{e\}$, 由此知 $N=\{e\}$, 即 $\{e\}$ 为 S_x 所包含的唯一的 G 的正规子群.

(3) 因 σ 是 G 到 S_X 的同态, 由式(2.10)有

$$e(x)=\sigma(e)(x)=\mathrm{id}_X(x)=x,\quad \forall x\in X,$$

$$g_1(g_2(x))=\sigma(g_1)(\sigma(g_2)(x))=\sigma(g_1)\sigma(g_2)(x)=\sigma(g_1g_2)(x)=g_1g_2(x),\quad \forall x\in X,g_1,g_2\in G,$$

即 σ 定义了 G 在 X 上的作用.

□

定义 2.11

设群 G 作用在集合 X 与 X' 上, 若有 X 到 X' 上的一一对应 ϕ, 使

$$g(\phi(x))=\phi(g(x)),\quad \forall g\in G,x\in X,$$

则称 G 在 X,X' 上的**作用等价**.

♣

注 如果将 g 引起的 X,X' 上的置换仍以 g 来表示, 那么 G 在 X,X' 上的作用等价也就是对任何 $g\in G$,图 2.1是交换图.

如果在 G 作用的集合之间规定关系 $R:XRX'$, 若 G 在 X,X' 上作用等价. 这显然是一个等价关系, 因而从抽象的观点来看, 等价作用可以看成是一样的.

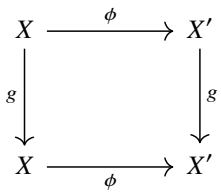

图 2.1

定理 2.9

设群 G 在 X 上的作用可递,$x \in X$, 则 G 在 X 上的作用与 G 在 G/S_x 上的作用 (左平移作用) 等价.

♡

注 这个定理表明 G 在每个轨道上的作用相当于 G 在某个左陪集空间上的作用.

证明 因 G 在 X 上的作用可递, 于是由命题 2.3有

$$X = O_x = \{g(x) \in X \mid g \in G\}.$$

作 G/S_x 到 X 的映射 ϕ 如下:

$$\phi(gS_x) = g(x), \quad \forall g \in G.$$

显然 ϕ 是满射. 由于 $g_1S_x = g_2S_x$ 当且仅当 $g_1^{-1}g_2 \in S_x$, 当且仅当 $g_1^{-1}g_2(x) = x$, 当且仅当 $g_1(x) = g_2(x)$, 因而 ϕ 是单射. 故 ϕ 是 G/S_x 到 X 上的一一对应. 又对 $\forall h \in G$ 有

$$\phi(h(gS_x)) = \phi(hgS_x) = hg(x) = h(\phi(gS_x)),$$

故 G 在 G/S_x 与 X 上的作用等价.

□

推论 2.3

设有限群 G 作用在集合 X 上,O_x 为 $x \in X$ 的轨道, 则 O_x 中元素个数 $|O_x| = [G : S_x]$, 因而

$$|G| = |O_x|\,|S_x|\,.$$

如果 X 还是有限集, 则

$$|X| = \sum_{x \in X} [G : S_{x_i}], \tag{2.12}$$

其中 x 取遍 X 的不同轨道的代表元素. 公式(2.12)称为**轨道公式**.

♡

证明 由定理 2.7(2)知 G 在 O_x 上作用可递, 故由定理 2.9知,G 在 X 上的作用与 G 在 G/S_x 上的作用等价, 即存在 X 到 G/S_x 的双射. 因此 $|O_x| = [G : S_x]$. 再由Lagrange 定理知

$$|G| = [G : S_x]\,|S_x| = |O_x|\,|S_x|\,,$$

再由定理 2.7(3)可得

$$|X| = \sum_{x \in X} [G : S_{x_i}],$$

其中 x 取遍 X 的不同轨道的代表元素.

□

定理 2.10

设 G 是一个群, 在伴随作用下. 对 $\forall g \in G$, 则 G 上的内自同构$\mathrm{ad}g$:

$$\mathrm{ad}g(x) = gxg^{-1}, \quad \forall x \in G. \tag{2.13}$$

满足

$$S_{g(x)} = \mathrm{ad}g(S_x) = gS_xg^{-1}.$$

♡

证明 设 $g(x)=y$ 且 $g_1\in S_y$, 即有 $y=g_1(y)$, 则 $g_1g(x)=g(x)$, 因而 $g_2=g^{-1}g_1g\in S_x$, 故 $g_1=gg_2g^{-1}\in \mathrm{ad}g(S_x)$. 反之, 若 $g_2\in S_x$, 则有

$$gg_2g^{-1}(y)=gg_2g^{-1}(g(x))=g(x)=y,$$

故 $gg_2g^{-1}\in S_y$. 这样就证明了 $S_y=\mathrm{ad}g(S_x)$.

□

定义 2.12

设 G 是一个群,$g\in G$, g 在伴随作用下的轨道称为以 g 为代表的**共轭类**, 记为 C_g. 若 $h\in C_g$, 则称 h 与 g **共轭**.

g 在伴随作用下的迷向子群, 称为 g 在 G 中的**中心化子**, 记作 $C_G(g)$. 在不混淆时, 简称为 g 的**中心化子**, 记作 $C(g)$. 若 $H\subseteq G$, 则将 H 中每个元素在 G 中的中心化子之交

$$C_G(H)=\bigcap_{h\in H}C_G(h)=\bigcap_{h\in H}F_h$$

称为 H 在 G 中的**中心化子**.

在伴随作用下, 对 $\forall g\in G$, 则 G 上的内自同构$\mathrm{ad}g$:

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

也称 $\mathrm{ad}g$ 为群 G 的**共轭变换**,x 在共轭变换下的像 gxg^{-1} 称为 x 的**共轭元**.

再定义 G 到 $\mathrm{Int}G$ 的同态ad 满足

$$\mathrm{ad}: g\to \mathrm{ad}g,\quad \forall g\in G.$$

称 $\ker\mathrm{ad}$ 为 G 的**中心**, 记作 $C(G)$ 或 $Z(G)$.

♣

定理 2.11

设 G 是一个群,$H\subseteq G$,$g\in G$, 在伴随作用下, 有

(1) $C_g=\{kgk^{-1}\mid k\in G\}$.

(2) $g,h\in G$共轭 $\Longleftrightarrow \exists k\in G$, 使$h=kgk^{-1}$.

(3) $C_G(g)=C(g)=\left\{k\in G\mid kgk^{-1}=g\right\}=\{k\in G\mid kg=gk\}$.

(4) $C_G(H)=\{g\in G\mid hgh^{-1}=g\}=\{g\in G\mid hg=gh,\forall\in H\}$.

(5) $C(G)=\left\{k\in G\mid kgk^{-1}=g,\forall g\in G\right\}=\{k\in G\mid kg=gk,\forall g\in G\}$.

♡

证明

(1) 由定义知

$$C_g=\{\mathrm{ad}k(g)\in G\mid k\in G\}=\left\{kgk^{-1}\in G\mid k\in G\right\}.$$

(2) 由定理 2.11(1)知

$$C_g=\left\{kgk^{-1}\in G\mid k\in G\right\},$$

则

$$g,h\in G\text{共轭}\Longleftrightarrow h\in C_g\Longleftrightarrow \exists k\in G,\text{使}h=kgk^{-1}.$$

(3) 由定义知

$$\begin{aligned}C_G(H)&=\bigcap_{h\in H}C_G(h)=\bigcap_{h\in H}F_h=\bigcap_{h\in H}\left\{g\in G\mid ghg^{-1}=h\right\}\\&=\left\{g\in G\mid ghg^{-1}=h,\forall h\in H\right\}=\{g\in G\mid gh=gh,\forall h\in H\}.\end{aligned}$$

(4) 由定义知

$$C_G(g)=C(g)=\{k\in G\mid \mathrm{ad}k(g)=g\}=\left\{k\in G\mid kgk^{-1}=g\right\}=\{k\in G\mid kg=gk\}.$$

(5) 由定义知

$$C(G)=\ker \mathrm{ad}=\{k\in G\mid \mathrm{ad}(k)=\mathrm{id}_G\}=\{k\in G\mid \mathrm{ad}k=\mathrm{id}_G\}$$
$$=\left\{k\in G\mid kgk^{-1}=g,\forall g\in G\right\}=\{k\in G\mid kg=gk,\forall g\in G\}.$$

□

定理 2.12

设 G 是一个群,$g\in G$, 则有

(1) $C(g)=C(g^{-1})$.

(2) 设 $A<G$, 则 $C_G(C_G(C_G(A)))=C_G(A)$.

(3) $C(G)$ 是 G 的正规子群且 $\mathrm{ad}G\cong G/C(G)$.

(4) G 中共轭关系为等价关系, 因而 G 的共轭类的集合是 G 的一个分划. 即 X 是所有不同轨道的并

$$X=\bigsqcup_x O_x,$$

其中 x 取遍 X 的不同共轭类的代表元素.

(5) 若 G 是有限群, 则 $|C_g|=[G:C(g)]$, 并且

$$|G|=|C(G)|+\sum_{x\in G}[G:C(x)], \tag{2.14}$$

其中 x 取遍非中心的元素的共轭类的代表元. 公式(2.14)称为**群方程**.

(6) $h\in C(G)\iff |C_h|=1\iff h\in\bigcap_{g\in G}C(g)$. 进而 $C(G)=\bigcap_{g\in G}C(g)$.

♡

证明

(1) 只需注意到

$$C(g)=\left\{k\in G\mid kgk^{-1}=g\right\}=\left\{k\in G\mid \left(kgk^{-1}\right)^{-1}=g^{-1}\right\}=\left\{k\in G\mid kg^{-1}k^{-1}=g^{-1}\right\}=C\left(g^{-1}\right).$$

(2) 令 $B=C_G(C_G(A))$, 要证 $C_G(B)=C_G(A)$. 利用定理 2.11(4).

设 $x\in C_G(A)$. 对于任一 $y\in B=C_G(C_G(A))$, 则 y 与 x 可换, 即 x 和 y 可换, 即 $x\in C_G(B)$. 故 $C_G(A)\subseteq C_G(B)$.

反之, 设 $y\in C_G(B)$, 即 y 与 B 中任一元可换. 因为 $C_G(A)$ 中任一元与 A 中任一元可换, 故 A 中任一元与 $C_G(A)$ 中的元可换, 于是

$$A\subseteq C_G(C_G(A))=B.$$

从而 y 与 A 中任一元可换, 即 $y\in C_G(A)$. 故 $C_G(B)\subseteq C_G(A)$. 从而 $C_G(B)=C_G(A)$.

(3) 由定理 2.8(2)(ii)知 $C(G)\lhd G$. 再由群的同态基本定理知 $\mathrm{ad}G$ 与 $G/C(G)$ 同构.

(4) 由定理 2.7(2)即得.

(5) 由推论 2.3得

$$|G|=\sum_x[G:C(x)], \tag{2.15}$$

其中 x 取遍不同的共轭类的代表元素. 又由于

$$[G:C(x)]=1\iff G=C(x)\iff x\in C(G),$$

所以在(2.15)式中把值为 1 的项加到求和号外面来即得

$$|G|=|C(G)|+\sum_x[G:C(x)],$$

其中 x 取遍非中心的元素的共轭类的代表元.

(6) 由定理 2.11可得

$$h\in C(G)\Longleftrightarrow h\in\{k\in G\mid kg=gk,\forall g\in G\}\Longleftrightarrow hg=gh,\forall g\in G$$
$$\Longleftrightarrow ghg^{-1}=h,\forall g\in G\Longleftrightarrow C_h=\left\{ghg^{-1}\mid g\in G\right\}=\{h\}\Longleftrightarrow |C_h|=1;$$

$$h \in C(G) \Longleftrightarrow h \in \{k \in G \mid kg = gk, \forall g \in G\} \Longleftrightarrow hg = gh, \forall g \in G$$
$$\Longleftrightarrow h \in \{k \in G \mid kg = gk\}, \forall g \in G \Longleftrightarrow h \in C(g), \forall g \in G \Longleftrightarrow h \in \bigcap_{g \in G} C(g).$$

□

定理 2.13 (Cauchy 定理)

设 G 为有限群,$|G| = n$, 则对 n 的任一素因子 p,G 必有阶为 p 的元素.

证明 对 n 应用数学归纳法. 当 $n = 2$ 时, 结论显然成立. 假定结论对所有阶小于 n 的群成立. 考察 n 阶群 G 的群方程:

$$|G| = |C(G)| + \sum_{i=1}^{t} [G : C(x_i)],$$

其中 x_i 取遍非中心的元素的共轭类的代表元,t 为 G 中所有不同轨道的个数.

(a) 如果 $p \mid |C(G)|$, 则由命题 1.26知 $C(G)$ 含有阶为 p 的元素, 从而 G 含有阶为 p 的元素.

(b) 如果 $p \nmid |C(G)|$, 则因为 $p \mid |G|$, 所以至少存在一个 x_i, 使 $p \nmid [G : C(x_i)]$, 即 $p \nmid \dfrac{|G|}{|C(x_i)|}$. 又 $p \mid |G|$, 故 $p \mid |C(x_i)|$. 因为 $\dfrac{n}{|C(x_i)|} = \dfrac{|G|}{|C(x_i)|} = [G : C(x_i)] > 1$, 所以 $|C(x_i)| < n$. 由归纳假设知 $C(x_i)$ 含有阶为 p 的元素, 因此 G 含有阶为 p 的元素.

从而由归纳法原理知结论成立.

□

定义 2.13

设群 G 作用在集合 X 上,$g \in G$,$x \in X$.

(1) 如果 $g(x) = x$, 则称 x 为 g 的一个**不动元素** (fixed element).g 的全部不动元素的集合称为 g 的**不动元素集** (the set of fixed elements), 记作 F_g.

(2) 如果对任意的 $g \in G$, 都有 $g(x) = x$, 则称 x 为 G 的一个**不动元素**.G 的全部不动元素的集合称为 G 的**不动元素集**, 记作 F_G.

定理 2.14 (Burnside 引理)

设有限群 G 作用在有限集合 X 上,n 表示 X 在 G 的作用下的不同轨道数, 则

$$n = \frac{1}{|G|} \sum_{g \in G} |F_g|, \tag{2.16}$$

其中 $|F_g|$ 表示 g 的不动元素的个数.

证明 对任意的 $x \in X$,$g \in G$, 定义

$$\delta(g, x) = \begin{cases} 1, & g(x) = x, \\ 0, & g(x) \neq x. \end{cases}$$

由定义知

$$|F_g| = \sum_{x \in X} \delta(g, x), \quad |S_x| = \sum_{g \in G} \delta(g, x),$$

则

$$\sum_{g \in G} |F_g| = \sum_{g \in G} \left(\sum_{x \in X} \delta(g, x) \right) = \sum_{x \in X} \left(\sum_{g \in G} \delta(g, x) \right) = \sum_{x \in X} |S_x|.$$

如果 $x \in O_{x_i}$, 则 $O_x = O_{x_i}$, 从而由推论 2.3可得

$$|S_x| = \frac{|G|}{|O_x|} = \frac{|G|}{|O_{x_i}|} = |S_{x_i}|,$$

所以, 如果 $x_1, x_2, \cdots, x_n$ 为 n 个不同轨道的代表元素, 则由定理 2.7(2)和推论 2.3可得

$$\begin{aligned}\sum_{g\in G}|F_g| &= \sum_{x\in X=\bigsqcup_{i=1}^{n} O_{x_i}} |S_x| = \sum_{i=1}^{n}\sum_{x\in O_{x_i}} |S_x| \\ &= \sum_{i=1}^{n}\sum_{x\in O_{x_i}} |S_{x_i}| = \sum_{i=1}^{n} |O_{x_i}||S_{x_i}| \\ &= \sum_{i=1}^{n} |G| = n|G|.\end{aligned}$$

由此得

$$n = \frac{1}{|G|}\sum_{g\in G}|F_g|.$$

□

定理 2.15

设 H 是群 G 的子群, 则

(1) $\forall g \in G, H_1 = gHg^{-1}$ 也是 G 的子群, 并且 $H_1 \cong G$, 称 H_1 为 H 的**共轭子群**;

(2) 群 G 的子集 $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$ 也是 G 的子群, 而且 $H \lhd N_G(H)$,$N_G(H)$ 称为 H 在 G 中的**正规化子**, 也简称为 H 的**正规化子**.

♡

证明

(1) 以 e 表示 G 的幺元. 因为 $e = geg^{-1} \in H_1$, 故 $H_1 \neq \varnothing$. 设 $h_1, h_2 \in H$, 于是

$$(gh_1g^{-1})(gh_2g^{-1}) = g(h_1h_2)g^{-1},\ (gh_1g^{-1})^{-1} = gh_1^{-1}g^{-1} \in H_1.$$

由此知 H_1 是 G 的子群.

令

$$\begin{aligned}\phi : H &\to gHg^{-1} \\ x &\mapsto gxg^{-1}.\end{aligned}$$

显然, ϕ 为 H 到 gHg^{-1} 的一个良定义的映射.

设 $x, y \in H$, 如果 $\phi(x) = \phi(y)$, 即 $gxg^{-1} = gyg^{-1}$, 则 $x = y$, 所以 ϕ 为 H 到 gHg^{-1} 的单映射.

对任意的 $x \in gHg^{-1}$, 有 $y = g^{-1}xg \in H$, 使

$$\phi(y) = gyg^{-1} = g(g^{-1}xg)g^{-1} = x,$$

所以 ϕ 为 H 到 gHg^{-1} 满映射.

对任意的 $x, y \in H$, 有

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

所以 ϕ 为 H 到 gHg^{-1} 的同构映射, 即

$$\phi :\ H \cong gHg^{-1}.$$

(2) G 在 G 的伴随作用下,H 的迷向子群恰为 $N_G(H)$, 故 $N_G(H)$ 是 G 的子群. 因 H 是 G 的子群且 $H \subseteq N_G(H)$, 故 H 是 $N_G(H)$ 的子群. 又 $\forall g \in N_G(H), gHg^{-1} = H$, 因此 $H \lhd N_G(H)$.

□

定理 2.16

设 H 是群 G 的子群, 则

(1) G 中与 H 共轭的子群的个数为 $[G:N_G(H)]$;

(2) $H \lhd G \iff N_G(H)=G$.

♡

证明

(1) 设 H 的共轭子群到 $G/N_G(H)$ 的映射 f, 满足

$$f(gHg^{-1})=gN_G(H), \quad \forall g\in G.$$

显然 f 是满射. 因为 $gHg^{-1}=g_1Hg_1^{-1}$ 当且仅当 $H=g^{-1}g_1H(g^{-1}g_1)^{-1}$ 当且仅当 $g^{-1}g_1\in N_G(H)$ 当且仅当 $gN_G(H)=g_1N_G(H)$, 所以 f 是单射. 因此 f 是 H 的共轭子群到 $G/N_G(H)$ 的双射. 从而 G 中与 H 共轭的子群的个数与 $|G/N|$ 相等, 即 G 中与 H 共轭的子群的个数为 $[G:N_G(H)]$.

(2) 因为 $H\lhd G$ 当且仅当 $\forall g\in G, gHg^{-1}=H$, 所以由 $N_G(H)$ 的定义知 $N_G(H)=G$.

□

命题 2.4

有限群 G 的一个真子群的全部共轭子群之并不能覆盖整个群 G.

♠

注 这个结论对无限群不成立. 例如, 令 $G=GL(n,\mathbb{C})$, H 是 n 阶上三角可逆复矩阵作成的真子群. 由 Jordan 标准型知任一 n 阶可逆阵 A 相似于其 Jordan 标准型, 而可逆矩阵的 Jordan 标准型都是 H 中的元, 这表明 G 是 H 的所有共轭子群之并.

证明 设 H 是 G 的真子群, 则由定理 2.16(1)知 H 共有 $[G:N_G(H)]$ 个共轭子群. 令 Σ 是 H 的所有共轭子群之并, 则 (幺元单独计数)

$$|\Sigma|\leqslant(|H|-1)[G:N_G(H)]+1=\frac{|G|}{|N_G(H)|}\cdot|H|-[G:N_G(H)]+1.$$

若 H 是正规子群, 则由定理 2.16(2)知 $N_G(H)=G$, 于是

$$|\Sigma|\leqslant|H|-1+1=|H|<|G|.$$

若 H 不是正规子群, 则由定理 2.16(2)知 $N_G(H)\neq G$, 于是 $[G:N_G(H)]>1$,

$$|\Sigma|\leqslant\frac{|G|}{|H|}\cdot|H|-[G:N_G(H)]+1<|G|-1+1=|G|.$$

综合以上, $|\Sigma|<|G|$, 即 H 的全部共轭子群之并不能覆盖 G.

□

例题 2.5 令 $G=GL(n,\mathbb{C})$, P 是主对角线上的元均为 1 的 $n\times n$ 上三角方阵全体形成的 G 的子群. 确定 $N_G(P)$, $C_G(P)$ 和 P 的中心 $Z(P)$.

解 由矩阵的乘法直接计算可知与任一 n 阶主对角线为 1 的上三角矩阵可换的矩阵必为上三角矩阵, 且形如

$$J_n(\lambda,\mu)=\begin{pmatrix}\lambda & 0 & \cdots & 0 & \mu\\ & \lambda & \cdots & 0 & 0\\ & & \ddots & \vdots & \vdots\\ & & & \lambda & 0\\ & & & & \lambda\end{pmatrix},$$

其中 $\mu\in\mathbb{C}$. 要看出这一点, 只要取主对角线为 1 且 $(i,i+1)$ 处为 1, 其余全为 0 的上三角矩阵即可,$i=1,\cdots,n-1$. 因此

$$C_G(P)=\{J_n(\lambda,\mu)\mid\lambda,\mu\in\mathbb{C},\lambda\neq0\}.$$

由此即知 $Z(P)=\{J_n(1,\mu)\mid\mu\in\mathbb{C}\}$.

下面求

$$N_G(P) := \{A \in GL(n,\mathbb{C}) \mid AP = PA\}$$
$$= \{A \in GL(n,\mathbb{C}) \mid AJA^{-1} \subseteq P,\ A^{-1}JA \subseteq P,\ \forall J \in P\}.$$

首先, 所有 n 阶上三角可逆矩阵均在 $N_G(P)$ 中. 我们断言:$N_G(P)$ 恰是所有 n 阶上三角可逆矩阵作成的群.

设 A 是 n 阶可逆矩阵且 A 不是上三角的. 设 a_{ij} 是 A 中主对角线以下的非零元且 i 最大, 即

$$a_{ij} \neq 0, i > j;\ \text{且若} a_{st} \neq 0, s > t, \text{则} i \geqslant s.$$

令 J 是主对角线全为 1 且 $(j, j+1)$ 处为 1, 其余全为 0 的矩阵. 则 AJ 是将 A 的第 j 列加到第 $j+1$ 列后得到的矩阵, 从而 AJ 不是上三角的.

下证 $A \notin N_G(P)$. 否则存在 $B \in P$ 使得 $AJ = BA$, 注意到 AJ 的第 $(i, j+1)$ 处元是

$$a_{i,j} + a_{i,j+1}.$$

但 BA 是对 A 施行一系列初等行变换得到的, 这些行变换是将大数行的若干倍加到小数行. 由 A 的选取知 BA 的 $(i, j+1)$ 处元与 A 的 $(i, j+1)$ 处元相同, 均为 $a_{i,j+1}$, 从而 $AJ \neq BA$, 矛盾. 所以 $A \notin N_G(P)$. 即 $N_G(P)$ 恰是所有 n 阶上三角可逆矩阵作成的群.

□

2.3 Sylow 子群

定义 2.14 (p 群)

设 p 是素数. 若群 G 的阶是 p 的方幂, 即 $|G| = [G : e] = p^k (k \in \mathbb{N})$, e 为 G 的幺元, 则称 G 是一个 ***p* 群**.

♣

定理 2.17

设 p 群 G 作用在集合 X 上, $|X| = n$, $t = |\{x \in X \mid g(x) = x, \forall g \in G\}|$, 则有下列结论:

(1) $t \equiv n \pmod{p}$. 也即 $n \equiv t \pmod{p}$.

(2) 当 $(n, p) = 1$ 时, $t \geqslant 1$. 即 $\exists x \in X$, 使 $g(x) = x (\forall g \in G)$. 也即 $\exists x \in X$, 使 $O_x = \{x\}$. 亦即 X 中必有不动元素.

(3) G 的中心 $C(G) \neq \{e\}$.

♡

注 由(2.17)式知 $\{x \in X \mid g(x) = x, \forall g \in G\}$ 中的元素 x 的轨道都只包含其自身一个元素即 $O_x = \{x\}, |O_x| = 1$. 故 t 就是只包含一个元素的 X 的轨道的个数.

证明

(1) 由定理 2.7(2)及 $|X| = n$, 可设 X 的轨道分解为

$$X = O_{x_1} \bigsqcup O_{x_2} \bigsqcup \cdots \bigsqcup O_{x_m},$$

其中 $O_{x_1}, O_{x_2}, \cdots, O_{x_m} (m \leqslant n)$ 为 X 中所有不同的轨道. 注意到

$$x \in \{x \in X \mid g(x) = x, \forall g \in G\} \Longleftrightarrow g(x) = x (\forall g \in G)$$
$$\Longleftrightarrow O_x = \{g(x) \in X \mid g \in G\} = \{x\} \Longleftrightarrow |O_x| = 1,$$

故

$$\{x \in X \mid g(x) = x, \forall g \in G\} = \{x \in X \mid O_x = \{x\}\} = \{x \in X \mid |O_x| = 1\}. \tag{2.17}$$

从而对 $\forall x, y \in \{x \in X \mid g(x) = x, \forall g \in G\}$ 且 $x \neq y$, 有 $O_x = \{x\} \neq \{y\} = O_y$. 因此 $x, y \in \{x_1, x_2, \cdots, x_m\}$. 故 $\{x \in X \mid g(x) = x, \forall g \in G\} \subseteq \{x_1, x_2, \cdots, x_m\}$. 于是

$$n = |O_{x_1}| + \cdots + |O_{x_m}| = \sum_{|O_{x_i}|=1} |O_{x_i}| + \sum_{|O_{x_i}|\neq 1} |O_{x_i}|$$

$$= \sum_{x_i \in \{x \in X \mid g(x)=x, \forall g \in G\}} 1 + \sum_{|O_{x_i}| \neq 1} |O_{x_i}| = t + \sum_{|O_{x_i}| \neq 1} |O_{x_i}|.$$

由推论 2.3知 $|O_{x_i}| \mid |G|$. 由 G 为 p 群, $|O_{x_i}| > 1$, 故 $p \mid |O_{x_i}|$, 因而结论 (1) 成立.

(2) $(n, p) = 1$, 由结论 (1) 知 $t \neq 0$, 故结论 (2) 成立.

(3) 考虑 G 在 G 上的伴随作用. 由定理 2.11(5)知

$$C(G) = \{x \in G \mid \mathrm{ad}x(g) = \mathrm{id}_G(g) = g, \forall g \in G\}.$$

自然 $e \in C(G)$, 故 $|C(G)| \geqslant 1$. 又 $p \mid |G|$, 由结论 (1)(取 $X = C(G)$) 知 $|G| \equiv |C(G)| \pmod{p}$, 故 $|C(G)| > 1$, 即 $C(G) \neq \{e\}$.

□

引理 2.1

设 p 是素数, $n = p^l m, (m, p) = 1$. 若 $k \in \mathbb{N}, k \leqslant l$, 则

$$p^{l-k} || \mathrm{C}_n^{p^k},$$

其中 $||$ 表示恰能整除, 即 $p^{l-k} \mid \mathrm{C}_n^{p^k}$ 但 $p^{l-k+1} \nmid \mathrm{C}_n^{p^k}$, $\mathrm{C}_n^{p^k}$ 是组合数.

♡

证明 当 $1 \leqslant i \leqslant p^k - 1$ 时,i 都有分解 $i = j_i p^t$, 其中, $(j_i, p) = 1$, 于是有 $t < k \leqslant l$, 而此时

$$n - i = p^l m - p^t j = p^t (p^{l-t} m - j_i),$$
$$p^k - i = p^t (p^{k-t} - j_i),$$

因而 $p^t || (n - i), p^t || (p^k - i)$. 又

$$\mathrm{C}_n^{p^k} = \frac{n}{p^k} \frac{n-1}{p^k - 1} \cdots \frac{n - (p^k - 1)}{p^k - (p^k - 1)} = \frac{n}{p^k} \cdot \prod_{i=1}^{p^k - 1} \frac{n - i}{p^k - i}$$
$$= \frac{p^l m}{p^k} \cdot \prod_{i=1}^{p^k - 1} \frac{p^t \left(p^{l-t} m - j_i\right)}{p^t \left(p^{k-t} - j_i\right)} = p^{l-k} \cdot m \prod_{i=1}^{p^k - 1} \frac{p^{l-t} m - j_i}{p^{k-t} - j_i}.$$

注意到 $(m \prod_{i=1}^{p^k - 1} \frac{p^{l-t} m - j_i}{p^{k-t} - j_i}, p) = 1$, 故由此知 $p^{l-k} || \mathrm{C}_n^{p^k}$.

□

定理 2.18 (Sylow 第一定理)

设 G 是一个阶为 $p^l m$ 的群, 其中, p 为素数, $l \geqslant 1, (p, m) = 1$, 则对任何 $1 \leqslant k \leqslant l$, G 中一定有 p^k 阶子群.

♡

证明 令 X 是 G 中所有含 p^k 个元素的子集的集合, 即

$$X = \{A \subseteq G \mid |A| = p^k\}.$$

显然 $|X| = \mathrm{C}_n^{p^k}$, 其中 $n = p^l m$.

$G \times X$ 到 X 上的映射

$$f(g, A) = gA = \{ga | a \in A\}$$

定义了 G 在 X 上的作用. 于是由定理 2.7(2)知 X 有轨道分解

$$X = \bigsqcup O_A, \quad |X| = \sum |O_A|.$$

由引理 2.1知 $p^{l-k} || \mathrm{C}_n^{p^k}$, 即 $p^{l-k} || |X|$. 因而 $\exists A \in X$, 使 $p^{l-k} \mid |O_A|, p^{l-k+1} \nmid |O_A|$. 从而存在 t, 使 $(p, t) = 1$ 且 $|O_A| = p^{l-k} t$. 设 F_A 是 A 的迷向子群, 于是由推论 2.3及Lagrange 定理可得

$$|O_A| = [G : F_A] = \frac{p^l m}{[F_A : e]} = \frac{p^l m}{|F_A|} \Longrightarrow |O_A| \cdot |F_A| = p^l m$$
$$\Longrightarrow p^{l-k} t \cdot |F_A| = p^l m \Longrightarrow |F_A| t = p^k.$$

又 $(p,t)=1$, 故 $p^k \mid |F_A|$. 若 $p^{k+1} \mid |F_A|$, 则存在 c, 使 $|F_A| = p^{k+1}c$, 从而由上式知

$$p^l m = |O_A| \cdot |F_A| = p^{l-k}t \cdot p^{k+1}c = p^{l+1}tc \implies m = ptc,$$

这与 $(p,m)=1$ 矛盾! 故 $p^{k+1} \nmid |F_A|$, 因此 $p^k \parallel |F_A|$.

另一方面, 对 $g \in F_A$ 有 $gA = A$, 即 $g(a) = ga \in A (\forall a \in A)$. 于是 $F_A \cdot a \subseteq A$, 故再由命题 1.6知

$$|F_A \cdot a| = |F_A| \leqslant |A| = p^k.$$

由此知 $|F_A| = p^k$, 即 F_A 是一个 p^k 阶子群.

□

定义 2.15 (Sylow p 子群)

设群 G 的阶为 $p^l m$, p 为素数且 $(p,m)=1$, 则 G 的 p^l 阶子群称为 G 的 **Sylow p 子群**.

♣

注 Sylow 第一定理肯定了 Sylow p 子群的存在性, 故上述定义是良定义的.

命题 2.5

设 P 为群 G 的一个 Sylow p 子群, 则对 $\forall a \in P$, 都存在 $k \in \mathbb{N}$, 使得 $\operatorname{ord} a = p^k$.

♠

注 这个命题表明:Sylow p 子群的元素的阶都是 p 的方幂.

证明 设 $|P| = p^l$, 则由定理 1.47知 $\operatorname{ord} a \mid |P|$, 故存在 $k \in \mathbb{N}$, 使得 $\operatorname{ord} a = p^k$.

□

定理 2.19 (Sylow 第二定理)

设群 G 的阶为 $p^l m$, p 为素数, $(p,m)=1$. 又 P 是 G 的一个 Sylow p 子群, H 是 G 的一个 p^k 阶子群, 则 $\exists g \in G$, 使 $H \subseteq gPg^{-1}$. 特别地, G 的 Sylow p 子群是相互共轭的.

♡

证明 将 G 在 G/P 上的左平移作用限制在 H 上, 于是得到 H 在 G/P 上的左平移作用

$$h(gP) = hgP, \quad \forall h \in H, g \in G.$$

由Lagrange 定理知

$$[G:e] = [G:P][P:e] \iff |G| = |G/P|\,|P| \iff p^l m = |G/P|\,p^l \iff |G/P| = m.$$

又 $|H| = p^k$, $(p,m)=1$, 故由定理 2.17(2)知 G/P 中含有元素 gP, 其轨道仅含 gP, 即 $hgP = gP (\forall h \in H)$, 故存在 p_1, p_2, 使 $hgp_1 = gp_2$, 从而 $h = gp_2p_1^{-1}g^{-1} \in gpg^{-1}$. 因此 $H \subseteq gPg^{-1}$.

特别地, 若 H 也是 G 的一个 Sylow p 子群, 则 $|H| = p^l$, 再由命题 1.6知 $|H| = p^l = |P| = |gPg^{-1}|$. 又由之前证明知 $H \subseteq gPg^{-1}$, 从而 $H = gPg^{-1}$. 由定理 2.15知 H, P 相互共轭.

□

推论 2.4

设群 G 的阶为 $p^l m$, p 为素数, $(p,m)=1$. 又 P 是 G 的一个 Sylow p 子群, 则

(1) 群 G 中 Sylow p 子群的集合是 $X = \{gPg^{-1} \mid g \in G\}$, 即 P 的共轭子群构成的集合.

(2) $G \times X$ 到 X 的映射

$$f(g, P_1) = g(P_1) = gP_1g^{-1}, \quad \forall g \in G, P_1 \in X.$$

是群 G 在 X 上的作用. 并且 G 在 X 上的作用 f 是可递的.

♡

证明

(1) 任取 $g \in G$, 对 $\forall p_1, p_2 \in P$, 有 $(gp_1g^{-1})(gp_2g^{-1})^{-1} = gp_1p_2^{-1}g^{-1} \in gPg^{-1}$, 因此 gPg^{-1} 是 G 的子群. 又由命题 1.6知 $|P| = |gPg^{-1}| = p^l$, 故 gPg^{-1} 也是 G 的 Sylow p 子群.

又若 P_1 是 G 的另一 Sylow p 子群. 由Sylow 第二定理知 $\exists g_1 \in G$, 使得 $g_1 P g_1^{-1} = P_1$, 因而 $X = \{gPg^{-1} | g \in G\}$ 是 G 中 Sylow p 子群的集合.

(2) 根据群作用的定义容易验证 f 是群 G 在 X 上的一个作用. 对 $\forall P_1, P_2 \in \{X\}$, 由Sylow 第二定理知 P_1, P_2 共轭, 即存在 $g \in G$, 使

$$P_1 = gP_2g^{-1} = g(P_1) = f(g, P_1).$$

故 G 在 X 上的作用 f 是可递的.

□

定理 2.20 (Sylow 第三定理)

设群 G 的阶为 $p^l m$, p 为素数, $(p, m) = 1$. 又设 G 中 Sylow p 子群的个数为 k, 则 k 也是 G 中任意一个 Sylow p 子群的共轭子群的个数. 并且有

(1) 当且仅当 $k = 1$ 时, G 的 Sylow p 子群 $P \lhd G$;

(2) $k | m$, $k \equiv 1 \pmod{p}$.

♡

证明 设 P 是 G 的一 Sylow p 子群. 则由推论 2.4(1)知 $X = \{gPg^{-1} | g \in G\}$ 是 G 中 Sylow p 子群的集合. 从而 k 也是 G 中任意一个 Sylow p 子群的共轭子群的个数.

(1) 若 $|X| = 1$, 即 $gPg^{-1} = P(\forall g \in G)$, 故由正规子群定义知 $P \lhd G$. 反之, 若 $P \lhd G$, 则 $gPg^{-1} = P(\forall g \in G)$, 故 $|X| = 1$. 这样就证明了结论 (1).

(2) 由推论 2.4(1)知 $X = \{gPg^{-1} | g \in G\}$ 是 G 中 Sylow p 子群的集合. 现设 $|X| = k$, 由推论 2.4(2)知 $G \times X$ 到 X 的映射

$$f(g, P_1) = gP_1g^{-1}, \quad \forall g \in G, P_1 \in X.$$

定义了 G 在 X 上的作用. 设 F_P 为 P 的迷向子群, 即

$$F_P = \{g \in G, |gPg^{-1} = P\}.$$

显然, $P \lhd F_P$, 故由Lagrange 定理知 $|P| \,|\, |F_P|$, 即 $p^l \,|\, |F_P|$, 因而存在 t, 使得

$$|F_P| = p^l t. \tag{2.18}$$

于是由Lagrange 定理知

$$|G| = [G : F_P]|F_P| \iff p^l m = [G : F_P]p^l t \iff m = [G : F_P]t \Longrightarrow [G : F_P] \,|\, m, t \,|\, m. \tag{2.19}$$

又注意到 G 在 X 上的作用下 P 的轨道为 $O_P = X$, 故由推论 2.3知

$$k = |X| = [G : F_P].$$

因此再结合(2.19)式得 $k \,|\, m$.

将上面 G 在 X 上的作用限制为 P 在 X 上的作用, 显然 $P \in X$, P 在 X 上的作用下 P 的轨道 $O'_P = \{P\}$. 若另有 $P_1 \in X$, 在 P 作用下的轨道 $O'_{P_1} = \{P_1\}$, 即有 $gP_1g^{-1} = P_1(\forall g \in P)$. 由Sylow 第二定理, $\exists h \in G$, 使得 $P_1 = hPh^{-1}$, 因而

$$g(hPh^{-1})g^{-1} = hPh^{-1}(\forall g \in P) \iff (h^{-1}gh)P(h^{-1}gh)^{-1} = P(\forall g \in P).$$

故 $h^{-1}gh \in F_P(\forall g \in P)$, 从而 $hPh^{-1} \subseteq F_P$. 因此 $h^{-1}Ph$, P 均为 F_P 的子群. 由(2.19)式知 $t \,|\, m$, 又因为 $(p, m) = 1$, 所以 $(p, t) = 1$. 而由(2.18)知 $|F_P| = p^l t$, $|P| = p^l$, 再由命题 1.6知 $|h^{-1}Ph| = |P| = p^l$, 故 $h^{-1}Ph$, P 均为 F_P 的 Sylow p 子群. 又 $P \lhd F_P$, 故由结论 (1) 知 $h^{-1}Ph = P$, 故 $P = P_1$. 这就说明包含一个元素的 X 的轨道仅有一个. 注意到

$$P' \in \{P' \in X \mid g(P') = gP'g^{-1} = P', \forall g \in P\} \iff O_{P'} = \{g(P') = gP'g^{-1} = P' \mid g \in P\} = \{P'\},$$

故

$$\{P' \in X \mid g(P') = gP'g^{-1} = P', \forall g \in P\} = \{P' \in X \mid O_{P'} = \{P'\}\} = \{P\}.$$

即 $|\{P' \in X \mid g(P') = gP'g^{-1} = P', \forall g \in P\}| = 1$. 故由定理 2.17(1)知 $k \equiv 1 \pmod{p}$.

□

定义 2.16 (单群)

一个群如果没有非平凡的正规子群就称为**单群**.

命题 2.6

阶数大于 2 的循环群都不是单群

证明 因为循环群都是 Abel 群, 所以其子群都是正规子群. 又有阶数大于 2, 故一定有非平凡的正规子群.

□

例题 2.6 设群 G 的阶为 72, 则 G 不是单群.

注 Sylow 定理在群论中有许多应用, 其一就是判断某些有限群不是单群.

解 $72 = 2^3 \cdot 3^2$. 设 G 中 Sylow 3 子群的个数为 k, 于是由Sylow 第三定理知有 t, 使得 $k = 3t + 1$, $k|8$, 因而 $t = 0$ 或 $t = 1$.

若 $t = 0$, 则 $k = 1$. 此时再由Sylow 第三定理知 Sylow 3 子群为 G 的正规子群, 故 G 不是单群.

若 $t = 1$, 则 $k = 4$. 设 $X = \{P_1, P_2, P_3, P_4\}$ 为 G 的 Sylow 3 子群的集合, 由推论 2.4(2)知有 G 在 X 上的作用

$$g(P_1) = gP_1g^{-1}, \quad \forall g \in G, P_1 \in X.$$

并且这个 G 在 X 上的作用是可递的. 由定理 2.8知有 G 到 $S_X = S_4$ 中的同态 σ 满足

$$\sigma(g) = \sigma_g, \forall g \in G,$$

其中 $\sigma_g : X \to X, P \longmapsto g(P) = gPg^{-1}$. 于是由群的同态基本定理知 $\ker\sigma \lhd G$ 且 $G/\ker\sigma$ 与 S_4 的一个子群 $\sigma(G)$ 同构, 而 $|S_4| = 24 < 72$, 于是

$$[G : \ker\sigma] = |\sigma(G)| \leqslant |S_4| = 24 < 72 = |G|.$$

再利用Lagrange 定理可得

$$|G| = [G : \ker\sigma]|\ker\sigma| \implies |\ker\sigma| = \frac{|G|}{[G : \ker\sigma]} \geqslant \frac{72}{24} > 1.$$

因此 $\ker\sigma \neq \{e\}$.

注意到

$$\ker\sigma = \{g \in G \mid \sigma(g) = \mathrm{id}_G\} = \{g \in G \mid gPg^{-1} = P, \forall P \in X\},$$

又由 G 在 X 上的作用可递知对 $P_1, P_2 \in X$, 存在 $g_1 \in G$, 使 $P_2 = g(P_1) = g_1P_1g_1^{-1}$. 若 $\ker\sigma = G$, 则 $g_1 \in \ker\sigma$, 从而

$$P_2 = g_1P_1g_1^{-1} = P_1,$$

这与 $P_1 \neq P_2$ 矛盾! 因此 $\ker\sigma \neq G$. 故 $\ker\sigma$ 是 G 的非平凡正规子群, 因而 G 不是单群.

□

命题 2.7

设 p, q 都是素数, $p < q$, $p \nmid (q-1)$. 证明 pq 阶群一定是循环群.

证明 设 P, Q 分别为 pq 阶群 G 的 p, q 阶子群. 于是由Sylow 第三定理 (2), 可设 P, Q 共轭子群的个数分别为 $sp + 1, tq + 1 (s, t \in \mathbb{N})$. 由推论 2.4(1)知,$P$ 的共轭子群都是 G 的 Sylow p 子群,Q 的共轭子群都是 G 的 Sylow p 子群. 因此

$$sp + 1 = q, \quad tq + 1 = p.$$

由 $p < q$, 于是 $t = 0$, 因而 Q 是 G 的唯一的 q 阶子群. 若 $s \neq 0$, 则 $sp + 1 = q$, 这与 $p \nmid (q-1)$ 矛盾. 于是 $s = 0$, 因而 P 是 G 的唯一的 p 阶子群.

因为 p,q 都是素数且 $p<q$, 所以 $|P\cup Q|\leqslant p+q<pq=|G|$, 因此 $G\neq Q\cup P$. 对 $\forall a\in G\backslash(P\cup Q)$, 则 $\langle a\rangle\neq P,Q$, 从而由 P,Q 分别是 G 的唯一 p,q 阶子群知 $\langle a\rangle$ 的阶既不是 p 也不是 q. 又由Lagrange 定理知 $|\langle a\rangle|=|\ pq$, 于是 $|\langle a\rangle|=pq$, 因此 $G=\langle a\rangle$ 为循环群.

□

命题 2.8

设 G 是有限 Abel 群, 则 g 对应到 g^k 是 G 的一个自同构当且仅当 k 和 $|G|$ 互素.

♠

证明 **充分性**: 设 $|G|$ 与 k 互素, 令

$$\alpha: G\to G,\ \alpha(g)=g^k,\ \forall g\in G.$$

因 G 是 Abel 群, 故

$$\alpha(g_1g_2)=(g_1g_2)^k=g_1^kg_2^k=\alpha(g_1)\alpha(g_2).$$

因此 α 是群同态. 设 $\alpha(g)=\alpha(h)$, 即 $(h^{-1}g)^k=1$. 又由定理 1.47知 $h^{-1}g$ 的阶是 $|G|$ 的因子, 由题设知 k 和 $h^{-1}g$ 的阶互素. 由定理 1.48(4)可推出 $1=\operatorname{ord}1=\operatorname{ord}(h^{-1}g)^k=\operatorname{ord}(h^{-1}g)$, 故 $h=g$, 即 α 是单射. 设 $l|G|+mk=1$, 则对任一 $g\in G$, 由定理 1.47有

$$g=g^{l|G|+mk}=(g^m)^k.$$

这表明 α 是满射, 即 α 是群 G 的自同构.

必要性: 设 $\alpha: G\to G,\ \alpha(g)=g^k,\ \forall g\in G$ 是群自同构. 则对任一 $g\in G$, g 与 $g^k=\alpha(g)$ 的阶相同. 另一方面, 根据定理 1.48(4)知

$$\operatorname{ord}g^k=\frac{\operatorname{ord}g}{(k,\operatorname{ord}g)},$$

即知 k 和 $\operatorname{ord}g$ 互素, 对 $\forall g\in G$ 成立.

证法一:设 $|G|=p_1^{k_1}p_2^{k_2}\cdots p_s^{k_s}$, 其中 $p_1,p_2,\cdots,p_s$ 两两互素. 由Cauchy 定理知, 对 $|G|$ 的任一素因子 p_i, 都存在 p 阶元 $g\in G$, 故 k 与 p_i 互素, 从而 k 与 $|G|$ 互素.

证法二:对 $|G|$ 用数学归纳法证明 k 与 $|G|$ 互素. 假设结论对阶小于 $|G|$ 的有限 Abel 群都成立.

若 $\exists g\in G$, s.t. $|G|=\operatorname{ord}g$, 则已证. 设 $\operatorname{ord}g<|G|,\forall g\in G$. 令 $1\neq a\in G,\operatorname{ord}a=n<|G|$, 则由定理 1.47知 $n\mid|G|$, 从而 $(k,n)=1$. 考虑 G 的商群 $\overline{G}=G/\langle a\rangle$, 则 $|\overline{G}|=\dfrac{|G|}{n}<|G|$. 记 $g\langle a\rangle=\overline{g},\forall g\in G$, 再考虑由 α 诱导的映射 $\overline{\alpha}$:

$$\overline{\alpha}:\overline{G}\longrightarrow\overline{G},\ \overline{g}\longmapsto\overline{g^k}.$$

因 G 是 Abel 群, 故显然 $\overline{\alpha}$ 是 $\overline{G}$ 的自同态. 由 $(|G|,k)=1$ 知存在 $l,m\in\mathbb{N}$, 使得 $l_1|G|+m_1k=1$. 从而对 $\forall\overline{g}\in\overline{G}$, 由定理 1.47有

$$g=g^{l_1|G|+m_1k}=(g^{m_1})^k.$$

因此 $\overline{\alpha}(\overline{g^{m_1}})=\overline{g}$, 故 $\overline{\alpha}$ 是满自同态. 下证 $\overline{\alpha}$ 作为 $\overline{G}$ 的自同态也是单射. 若 $\overline{\alpha}(\overline{g})=\overline{\alpha}(\overline{h})$, 即 $(h^{-1}g)^k\in\langle a\rangle$, 则

$$(h^{-1}g)^{kn}=1\Longrightarrow(h^{-1}g)^n=1.$$

由 $(k,n)=1$, 可设 $ln+mk=1$, 于是

$$h^{-1}g=\left(h^{-1}g\right)^{ln+mk}=((h^{-1}g)^k)^m\in\langle a\rangle.$$

即 $\overline{h}=\overline{g}$, 故 $\overline{\alpha}$ 是单射. 因此 $\overline{\alpha}$ 是 $\overline{G}$ 上自同构. 于是由归纳假设知 $(k,\dfrac{|G|}{n})=1$. 而已知 $(k,n)=1$ 且 $n\mid|G|$, 从而 $(k,|G|)=(k,\dfrac{|G|}{n}\cdot n)=1$.

□

2.4 有限单群

定义 2.17 (有限单群)

若有限群 G 无非平凡的正规子群, 则称 G 为**有限单群**.

♣

定理 2.21

设 G 为 Abel 群且 $G \neq \{e\}$,e 为 G 的幺元, 则 G 为单群的充分必要条件是 G 的阶为素数. 这时 G 必为循环群.

♡

证明 由命题 1.8(1) Abel 群 G 的任何子群都是 G 的正规子群, 故 Abel 群 G 为单群当且仅当 G 无非平凡子群.

若 G 是有限阶的, 当 G 的阶为素数时, 由推论 1.9(1)知 G 只有平凡子群. 当 G 无非平凡子群时, 若 G 的阶不是素数, 又 $G \neq \{e\}$, 故 $|G|$ 是不为 1 的合数. 由因式分解定理知存在素数 p 以及正整数 m,l, 使 $|G| = p^l m$ 且 $(p,m) = 1$. 从而 m,l 不同时为 1, 否则与 $|G|$ 不为素数矛盾! 故 $|G| > p$. 由Sylow 第一定理知 G 中一定有 p 阶子群 H, 而 $1 < p < |G|$, 故 H 必是 G 的非平凡子群, 矛盾! 因此 G 无非平凡子群当且仅当 G 的阶为素数. 此时, 由命题 1.24知 $\forall a \in G$ 且 $a \neq e$ 有 $G = \langle a \rangle$.

若 G 是无限阶的, 则 $\langle a \rangle \lhd G (\forall a \in G, a \neq e)$. 若 $\langle a \rangle$ 是有限阶的, 则 $\langle a \rangle$ 是非平凡的. 若 $\langle a \rangle$ 是无限阶的, 则 $\langle a^2 \rangle$ 是非平凡的, 因为 $a, -a \notin \langle a^2 \rangle$. 即任何无限阶的 Abel 群都有非平凡的正规子群. 故此时 G 必不是单群.

□

定理 2.22

(1) 当 $n \geqslant 3$ 时,A_n 由所有的 3 轮换生成, 即 $A_n = \langle \{(ijk)\} \rangle$;

(2) 当 $n \geqslant 5$ 时, 任意 3 轮换 (ijk) 在 A_n 中的共轭类由所有的 3 轮换构成, 即

$$C_{(ijk)} = \{(i'j'k') \mid i', j', k' = 1, 2, \cdots, n\}.$$

♡

证明

(1) 由推论 2.2知 $a \in A_n$ 当且仅当 a 可表示为偶数个对换之积. 由推论 2.1知

$$\langle \{(ijk)\} \rangle = \{(i_1 j_1 k_1) \cdots (i_m j_m k_m) \mid i_s, j_s, k_s \in \{1, 2, \cdots, n\}, 1 \leqslant s \leqslant m, m \in \mathbb{N}\}.$$

设 i,j,k,l 且互不相等. 由

$$(ij)(ij) = \mathrm{id}, \quad (ij)(ik) = (ikj),$$

$$(ik)(jl) = (ik)(ij)(ij)(jl) = (ijk)(jli)$$

知 A_n 中元素都可写成 3 轮换之积, 因此 $A_n \subseteq \langle \{(ijk)\} \rangle$.

设 $(i_1 j_1 k_1) \cdots (i_m j_m k_m) \in \langle \{(ijk)\} \rangle$, 则由命题 2.1(7)知

$$(i_s j_s k_s) = (i_s k_s)(i_s j_s), \quad s = 1, 2, \cdots, m.$$

故 $(i_1 j_1 k_1) \cdots (i_m j_m k_m)$ 可写成偶数个对换之积, 故 $(i_1 j_1 k_1) \cdots (i_m j_m k_m) \in A_n$. 因此 $\langle \{(ijk)\} \rangle \subseteq A_n$. 故 $A_n = \langle \{(ijk)\} \rangle$.

(2) $\forall \sigma \in S_n$, 由命题 2.1(6)知

$$\sigma(ijk)\sigma^{-1} = (\sigma(i)\sigma(j)\sigma(k)). \tag{2.20}$$

于是 $C_{(ijk)} \subseteq \{(i'j'k')\}$. 反之, 对任意 3 轮换 $(i'j'k')$, 当 $n \geqslant 5$ 时, 首先 $\exists \sigma \in S_n$, 使 $\sigma(i) = i', \sigma(j) = j', \sigma(k) = k'$. 若 $\sigma \in A_n$, 则由(2.20)式可得

$$(i'j'k') = (\sigma(i)\sigma(j)\sigma(k)) = \sigma(ijk)\sigma^{-1} \in C_{(ijk)}.$$

若 $\sigma \notin A_n$, 由 $n \geqslant 5$ 有 $i_1, i_2 \notin \{i,j,k\}$. 故由推论 2.2知 $\sigma(i_1 i_2) \in A_n$. 再由命题 2.1(6)知

$$(i'j'k') = (\sigma(i)\sigma(j)\sigma(k)) = ((\sigma(i_1 i_2)(i))(\sigma(i_1 i_2)(j))(\sigma(i_1 i_2)(k))) = \sigma(i_1 i_2)(ijk)(\sigma(i_1 i_2))^{-1} \in C_{(ijk)}.$$

即仍有 $(i'j'k') \in C_{(ijk)}$. 综上知 $C_{(ijk)} = \{(i'j'k')\}$.

□

定理 2.23

当 $n \geqslant 5$ 时,A_n 是非 Abel 有限单群.

♡

证明 对 $\alpha \in S_n$, 令 $\bar{F}_\alpha = \{j \mid \alpha(j) \neq j\}$. 显然有

(1) $\bar{F}_\alpha = \{i, j\}$ 当且仅当 $\alpha = (ij)$;

(2) $\bar{F}_\alpha = \{i, j, k\}$ 当且仅当 $\alpha = (ijk)$或$(ijk)^{-1}$;

(3) 对 $\forall \alpha \in A_n$ 且 $\alpha \neq \mathrm{id}$, 又由推论 2.2知 α 可写成偶数个对换之积, 从而一定有 $|\bar{F}_\alpha| \geqslant 3$.

设 $H \lhd A_n$ 且 $H \neq \{\mathrm{id}\}$. 取 $\tau \in H$, 使

$$|\bar{F}_\tau| = \min\{|\bar{F}_\alpha| \mid \alpha \in H, \alpha \neq \mathrm{id}\}. \tag{2.21}$$

显然 $|\bar{F}_\tau| \geqslant 3$. 若 $|\bar{F}_\tau| = 3$, 则 τ 是 3 轮换. 显然 $\tau \in H$, 由正规子群定义和定理 2.11(1)知

$$\alpha\tau\alpha^{-1} \in H,\ \forall \alpha \in A_n \implies C_\tau = \{\alpha\tau\alpha^{-1} \mid \alpha \in A_n\} \subseteq H.$$

再由定理 2.22(1)和定理 2.22(2)知

$$A_n = \langle\{(ijk)\}\rangle \subseteq \{(ijk) \mid i, j, k = 1, 2, \cdots, n\} = C_\tau \subseteq H,$$

故 $H = A_n$. 这就证明了 A_n 为有限单群. 又 A_n 的阶不是素数, 故由定理 2.21知 A_n 不是 Abel 群.

若 $|\bar{F}_\tau| > 3$. 由定理 2.4(1), 可将 τ 分解为不相交轮换之积, 分两种情况讨论. 一种在分解中只出现对换, 另一种在分解中有长度大于 2 的轮换.

(a) 若 τ 可分解为互不相交的对换之积, 又由最开始得到的情况 (1)知 τ 不可能是对换, 故可设 $\tau = (i_1i_2)(i_3i_4)\cdots$ 且 $i_1, i_2, i_3, i_4, \cdots$ 互不相同. 由 $n \geqslant 5$ 有 $j \neq i_1, i_2, i_3, i_4$, 令 $\phi = (i_3i_4j)$, 则由推论 2.2知 $\phi \in A_n$. 由 $H \lhd A_n$ 有 $\tau_1 = \tau^{-1}(\phi\tau\phi^{-1}) \in H$. 于是由命题 2.1(6)可得

$$\tau_1 = (\tau^{-1}\phi\tau)\phi^{-1} = (\tau^{-1}(i_3)\tau^{-1}(i_4)\tau^{-1}(j))(i_4i_3j) = (i_4i_3\tau^{-1}(j))(i_4i_3j).$$

若 $j \notin \bar{F}_\tau$, 即 $\tau(j) = \tau^{-1}(j) = j$. 则有

$$\tau_1 = (i_4i_3j)(i_4i_3j) = (i_3i_4j),$$

这时 $|\bar{F}_{\tau_1}| = |\{i_3, i_4, j\}| = 3 < |\bar{F}_\tau|$, 这与(2.21)式中 $|\bar{F}_\tau|$ 的最小值定义矛盾!

若 $j \in \bar{F}_\tau$, 则 $\tau = (i_1i_2)(i_3i_4)\cdots\left(j\tau^{-1}(j)\right)\cdots$ 且 $i_1, i_2, i_3, i_4, j, \tau^{-1}(j)$ 互不相同. 由 $j \neq i_1, i_2, i_3, i_4$ 知 $|\bar{F}_\tau| \geqslant 5$, 又 τ 可写成对换之积, 故 $|\bar{F}_\tau|$ 必为偶数, 因此 $|\bar{F}_\tau| \geqslant 6$. 此时由命题 2.1(5)可得

$$(i_4i_3\tau^{-1}(j))(i_4i_3j) = \left(i_4\tau^{-1}(j)\right)(i_4i_3)(i_4i_3j) = \left(i_4\tau^{-1}(j)\right)(i_4)(i_3j) = \left(i_4\tau^{-1}(j)\right)(i_3j).$$

于是

$$|\bar{F}_{\tau_1}| = |\{i_3, i_4, j, \tau^{-1}(j)\}| = 4 < |\bar{F}_\tau|.$$

这也(2.21)式中 $|\bar{F}_\tau|$ 的最小值定义矛盾! 因而 $\tau = (i_1i_2)(i_3i_4)\cdots$ 是不可能的.

(b) 设 τ 的分解中有长度大于 2 的轮换, 即

$$\tau = (i_1i_2i_3\cdots)\cdots.$$

因为 $(i_1i_2i_3i_4)$ 为奇置换, 故 $\tau \neq (i_1i_2i_3i_4)$, 由此知 $|\bar{F}_\tau| > 4$, 即 $|\bar{F}_\tau| \geqslant 5$. 因而存在 $j, k \neq i_1, i_2, i_3$, 使 $j, k \in \bar{F}_\tau$. 令 $\phi = (i_3jk)$,$\tau_1 = \tau^{-1}\phi\tau\phi^{-1}$, 由 $H \lhd A_n$ 有 $\tau_1 = \tau^{-1}(\phi\tau\phi^{-1}) \in H$. 于是由命题 2.1(6)可得

$$\tau_1 = (\tau^{-1}\phi\tau)\phi^{-1} = (\tau^{-1}(i_3)\tau^{-1}(j)\tau^{-1}(k))(ji_3k) = (i_2\tau^{-1}(j)\tau^{-1}(k))(ji_3k).$$

由 $i_1, i_2, i_3, j, k \in \bar{F}_\tau$ 知

$$\bar{F}_{\tau_1} = \left\{i_2, i_3, j, k, \tau^{-1}(j), \tau^{-1}(k)\right\} \subseteq \bar{F}_\tau.$$

(注意上式中 $\tau^{-1}(j),\tau^{-1}(k)$ 可能等于 i_1,i_2,i_3) 又注意到

$$\tau_1(i_1)=\tau^{-1}\phi\tau\phi^{-1}(i_1)=\tau^{-1}\phi\tau(i_1)=\tau^{-1}\phi(i_2)=\tau^{-1}(i_2)=i_1,$$

即 $i_1\notin\bar{F}_{\tau_1}$, 但 $i_1\in\bar{F}_\tau$, 则有 $\bar{F}_{\tau_1}\subset\bar{F}_\tau$, 亦即 $|\bar{F}_{\tau_1}|<|\bar{F}_\tau|$. 这也与(2.21)式中 $|\bar{F}_\tau|$ 的最小值定义矛盾! 故 $|\bar{F}_\tau|=3$. 综上可知 $H=A_n$, 即 A_n 为单群.

□

命题 2.9

对于 $n\leqslant 4$,A_n 的结构为

(1) $A_1=A_2=\{\mathrm{id}\}$;

(2) $A_3=\langle(123)\rangle$ 为三阶循环群;

(3) A_4 的阶为 12, A_4 含有一个非平凡的正规子群

$$\{\mathrm{id},(12)(34),(13)(24),(14)(23)\}.$$

此群与 **Klein 四元数群**同构, 也记为 K_4, 而且 K_4 也是 S_4 的正规子群.

证明

□

2.5 群的直积

定义 2.18 (外直积)

设 $G_1,G_2,\cdots,G_n$ 是 n 个群, 构造集合 $G_1,G_2,\cdots,G_n$ 的笛卡尔积

$$G=\{(a_1,a_2,\cdots,a_n)\mid a_i\in G_i,\ i=1,2,\cdots,n\},$$

并在 G 中定义乘法运算

$$(a_1,a_2,\cdots,a_n)\cdot(b_1,b_2,\cdots,b_n)=(a_1b_1,a_2b_2,\cdots,a_nb_n),\ \forall(a_1,a_2,\cdots,a_n),(b_1,b_2,\cdots,b_n)\in G,$$

则 G 关于上述定义的乘法构成群, 称为群 $G_1,G_2,\cdots,G_n$ 的**外直积**, 记作 $G=G_1\times G_2\times\cdots\times G_n$.

注

(1) 如果 $e_1,e_2,\cdots,e_n$ 分别是群 $G_1,G_2,\cdots,G_n$ 的单位元, 则 $(e_1,e_2,\cdots,e_n)$ 是 $G_1\times G_2\times\cdots\times G_n$ 的单位元;

(2) 设 $(a_1,a_2,\cdots,a_n)\in G$, 则 $(a_1,a_2,\cdots,a_n)^{-1}=(a_1^{-1},a_2^{-1},\cdots,a_n^{-1})$;

(3) 当 $G_1,G_2,\cdots,G_n$ 都是加群时,G_1 与 G_2 的外直积也可记作 $G_1\oplus G_2\oplus\cdots\oplus G_n$.

定理 2.24

设 $G=G_1\times G_2\times\cdots\times G_n$ 是 n 个群 $G_1,G_2,\cdots,G_n$ 的外直积, 则

(1) G 是有限群的充分必要条件是 $G_1,G_2,\cdots,G_n$ 都是有限群. 并且, 当 G 是有限群时, 有

$$|G|=|G_1|\cdot|G_2|\cdots|G_n|;$$

(2) G 是交换群的充分必要条件是 $G_1,G_2,\cdots,G_n$ 都是交换群;

(3) $G_1\times G_2\times\cdots\times G_n\cong G_{\sigma(1)}\times G_{\sigma(2)}\times\cdots\times G_{\sigma(n)},\ \forall\sigma\in S_n$.

(4) 若 $a_1,a_2,\cdots,a_n$ 分别是 $G_1,G_2,\cdots,G_n$ 中的有限阶元素, 则对 $(a_1,a_2,\cdots,a_n)\in G_1\times G_2\times\cdots\times G_n$, 有

$$\mathrm{ord}(a_1,a_2,\cdots,a_n)=[\mathrm{ord}\,a_1,\mathrm{ord}\,a_2,\cdots,\mathrm{ord}a_n].$$

(5) $C(G)=C(G_1)\times C(G_2)\times\cdots\times C(G_n)$.

(6) 若 $G_1,G_2,\cdots,G_n$ 分别是 $m_1,m_2,\cdots,m_n$ 阶的循环群, 则 G 是循环群的充要条件是

$(m_1, m_2, \cdots, m_n) = 1.$ ♡

证明

(1) 由笛卡尔积的定义易得.

(2) 如果 G_1 与 G_2 都是交换群, 则对任意的 $(a_1, a_2, \cdots, a_n), (b_1, b_2, \cdots, b_n) \in G$, 有

$$\begin{aligned}&(a_1, a_2, \cdots, a_n) \cdot (b_1, b_2, \cdots, b_n)\\ &= (a_1b_1, a_2b_2, \cdots, a_nb_n)\\ &= (b_1a_1, b_2a_2, \cdots, b_na_n)\\ &= (b_1, b_2, \cdots, b_n) \cdot (a_1, a_2, \cdots, a_n).\end{aligned}$$

所以 G 是交换群.

反之, 如果 G 是交换群, 那么对任意的 $a_1, b_1 \in G_1, a_2, b_2 \in G_2$, 有

$$(a_1, a_2, \cdots, a_n) \cdot (b_1, b_2, \cdots, b_n) = (b_1, b_2, \cdots, b_n) \cdot (a_1, a_2, \cdots, a_n),$$

即

$$(a_1b_1, a_2b_2, \cdots, a_nb_n) = (b_1a_1, b_2a_2, \cdots, b_na_n).$$

因此 $a_ib_i = b_ia_i$, $i = 1, 2, \cdots, n$. 从而 $G_i (i = 1, 2, \cdots, n)$ 都是交换群.

(3) 对 $\forall \sigma \in S_n$, 构造映射

$$\phi : G_1 \times G_2 \times \cdots \times G_n \longrightarrow G_{\sigma(1)} \times G_{\sigma(2)} \times \cdots \times G_{\sigma(n)},$$

$$(a_1, a_2, \cdots, a_n) \longmapsto (a_{\sigma(1)}, a_{\sigma(2)}, \cdots, a_{\sigma(n)}), \quad \forall (a_1, a_2, \cdots, a_n) \in G_1 \times G_2 \times \cdots \times G_n,$$

因为 σ 是双射, 所以 ϕ 也是双射, 且

$$\begin{aligned}&\phi((a_1, a_2, \cdots, a_n)(b_1, b_2, \cdots, b_n))\\ &= \phi(a_1b_1, a_2b_2, \cdots, a_nb_n)\\ &= (a_{\sigma(1)}b_{\sigma(1)}, a_{\sigma(1)}b_{\sigma(2)}, \cdots, a_{\sigma(1)}b_{\sigma(n)})\\ &= (a_2, a_1)(b_2, b_1) = \phi(a_1, a_2) \cdot \phi(b_1, b_2).\end{aligned}$$

因此 ϕ 是 $G_1 \times G_2 \times \cdots \times G_n$ 到 $G_{\sigma(1)} \times G_{\sigma(2)} \times \cdots \times G_{\sigma(n)}$ 的同构映射, 即

$$G_1 \times G_2 \times \cdots \times G_n \cong G_{\sigma(1)} \times G_{\sigma(2)} \times \cdots \times G_{\sigma(n)}.$$

(4) 当 $n = 1$ 时, 结论显然成立. 假设结论对 $n - 1$ 成立, 现在考虑 n 的情况.

设 $a_i \in G_i$, $i = 1, 2, \cdots, n$, 记 $b = (a_2, \cdots, a_n) \in G_2 \times \cdots \times G_n$,$\operatorname{ord} a_1 = m$, 则由归纳假设知

$$\operatorname{ord} b = \operatorname{ord}(a_2, \cdots, a_n) = [\operatorname{ord} a_2, \cdots, \operatorname{ord} a_n].$$

再记 $\operatorname{ord} b = n$, $s = [m, n]$,e_1 为 G_1 的幺元,e_2 为 $G_2 \times \cdots \times G_n$ 的幺元. 则

$$(a_1, b)^s = (a_1^s, b^s) = (e_1, e_2).$$

从而 (a_1, b) 的阶有限, 设其为 t, 则由上式得 $t \mid s$.

又因为

$$(e_1, e_2) = (a_1, b)^t = (a_1^t, b^t),$$

所以 $a_1^t = e_1, b^t = e_2$. 于是 $m \mid t$, 且 $n \mid t$, 从而 t 是 m 和 n 的公倍数. 而 s 是 m 和 n 的最小公倍数, 因此 $s \mid t$.

结合以上讨论得 $s = t$, 即

$$\begin{aligned}\operatorname{ord}(a_1, a_2, \cdots, a_n) &= \operatorname{ord}(a_1, b) = [\operatorname{ord} a_1, \operatorname{ord} b]\\ &= [\operatorname{ord} a_1, [\operatorname{ord} a_2, \cdots, \operatorname{ord} a_n]]\end{aligned}$$

$$= [\operatorname{ord} a_1, \operatorname{ord} a_2, \cdots, \operatorname{ord} a_n].$$

故由数学归纳法知结论成立.

(5) 设 $a = (a_1, a_2, \cdots, a_n) \in C(G)$, 则对任意的 $x = (x_1, x_2, \cdots, x_n) \in G$, 由 $ax = xa$ 得 $a_i \in C(G_i), i = 1, 2, \cdots, n$, 因此

$$a = (a_1, a_2, \cdots, a_n) \in C(G_1) \times C(G_2) \times \cdots \times C(G_n).$$

另一方面, 设 $a = (a_1, a_2, \cdots, a_n) \in C(G_1) \times C(G_2) \times \cdots \times C(G_n)$, 则对任意的 $x = (x_1, x_2, \cdots, x_n) \in G$, 有

$$ax = (a_1x_1, a_2x_2, \cdots, a_nx_n) = (x_1a_1, x_2a_2, \cdots, x_na_n) = xa.$$

所以 $a = (a_1, a_2, \cdots, a_n) \in C(G)$. 因此

$$C(G) = C(G_1) \times C(G_2) \times \cdots \times C(G_n).$$

(6) 设 $G_1 = \langle a_1 \rangle, G_2 = \langle a_2 \rangle, \cdots, G_n = \langle a_n \rangle, e_1, e_2, \cdots, e_n$ 分别为 $G_1, G_2, \cdots, G_n$ 的幺元.

必要性: 设 $G_1 \times G_2 \times \cdots \times G_n$ 是循环群. 若 $(m_1, m_2, \cdots, m_n) = t \neq 1$, 则由于 $\operatorname{ord} a_i = m_i$, $i = 1, 2, \cdots, n$. 而 $a_i^{\frac{m_i}{t}}$ 的阶都是 t, 因此由定理 1.47知

$$\langle (e_1, \cdots, \underbrace{a_i^{\frac{m_i}{t}}}_{\text{第}i\text{个位置}}, \cdots, e_n) \rangle, \ i = 1, 2, \cdots, n$$

都是循环群 $G_1 \times G_2 \times \cdots \times G_n$ 中的 n 个不同的 t 阶子群. 而这与定理 1.50(3)(iii)矛盾! 故 $(m_1, m_2, \cdots, m_n) = 1$.

充分性: 设 $(m_1, m_2, \cdots, m_n) = 1$, 则由定理 2.24(4) 和定理 2.24(1)可得

$$\begin{aligned} |\langle (a_1, a_2, \cdots, a_n) \rangle| &= \operatorname{ord}(a_1, a_2, \cdots, a_n) = [m_1, m_2, \cdots, m_n] \\ &= m_1 m_2 \cdots m_n = |G_1| \cdot |G_2| \cdots |G_n| \\ &= |G_1 \times G_2 \times \cdots \times G_n|. \end{aligned}$$

又 $\langle (a_1, a_2, \cdots, a_n) \rangle \subseteq G_1 \times G_2 \times \cdots \times G_n$, 故 $\langle (a_1, a_2, \cdots, a_n) \rangle = G_1 \times G_2 \times \cdots \times G_n$. 因此 $G_1 \times G_2 \times \cdots \times G_n$ 是循环群.

□

定义 2.19

设 A, B, G 都是群, 若有 G 的正规子群 N 与 A 同构, 而商群 G/N 与 B 同构, 则称 G 是 B **过** A **的扩张**, N 称为该扩张的**核**, 简称**扩张核**. ♣

注 显然, 若 N 是 G 的正规子群, 则 G 是 G/N 过 N 的扩张, 扩张核为 N.

定义 2.20

设 G 是 B 过 A 的扩张, N 为扩张核, λ 是 A 到 N 上的同构,μ 是 G 到 B 上的同态且 μ 满足 $\ker \mu = N$. 1 为 A 的幺元, $1'$ 为 B 的幺元, i 是 $\{1\}$ 到 A 的映射, $i(1) = 1$. $0'$ 是 B 到 $\{1'\}$ 的映射, $0'(b) = 1'(\forall b \in B)$. 于是有群及其映射的序列 (以 $1, 1'$ 代替 $\{1\}, \{1'\}$)

$$1 \xrightarrow{i} A \xrightarrow{\lambda} G \xrightarrow{\mu} B \xrightarrow{0'} 1',$$

每个映射都是群的同态映射, 并且前一映射的像恰是后一映射的核, 即

$$i(1) = \ker \lambda, \quad \lambda(A) = \ker \mu, \quad \mu(G) = \ker 0'.$$

这样的序列称为 **(短) 正合序列**. 以后记 (短) 正合序列时, i 与 $0'$ 省略不写, 同时也将 $1'$ 记为 1. ♣

注 由定理 1.32知存在 G 到 G/N 的自然群同态 μ_1. 由 $G/N \cong B$ 可设 G/N 到 B 的同构 f, 则 $\mu = f\mu_1$ 就是 G 到 B 的同态. 由命题 1.22知 $\ker \mu_1 = N$, 从而

$$\mu(N) = f\mu_1(N) = f(N) = 1'.$$

故 $N \subseteq \ker\mu$. 再设 $x \in \ker\mu$, 则

$$\mu(x) = f\mu_1(x) = 1' \implies \mu_1(x) = f^{-1}(1') = N \implies x \in \ker\mu_1 = N.$$

故 $\ker\mu \subseteq N$. 综上可得 $\lambda(A) = N = \ker\mu$. 故上述定义中的同态 μ 是良定义的.

命题 2.10

若群 A, B, G 之间有 (短) 正合序列

$$1 \longrightarrow A \xrightarrow{\lambda} G \xrightarrow{\mu} B \longrightarrow 1,$$

即存在 G 的正规子群 N, 还存在 λ 是 A 到 N 上的同构, 以及 μ 是 G 到 B 上的同态且 μ 满足 $\ker\mu = N$. 则 λ 是 A 到 G 的单同态,μ 是 G 到 B 的满同态, 并且 G 是 B 过 A 的扩张.

♠

证明

□

定理 2.25

设 A, B, G, G' 是群.

(1) 若 G 是 B 过 A 的扩张, G 与 G' 同构, 则 G' 也是 B 过 A 的扩张;

(2) 若 G, G' 都是 B 过 A 的扩张且有 G 到 G' 的同态 f, 使图 2.2为交换图, 则 f 是 G 到 G' 上的同构, 这时称 G 与 G' 是 B 过 A 的**等价扩张**.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & A & \xrightarrow{\lambda} & G & \xrightarrow{\mu} & B & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \mathrm{id}_A} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \mathrm{id}_B} & & \\
1 & \longrightarrow & A & \xrightarrow[\lambda']{} & G' & \xrightarrow[\mu']{} & B & \longrightarrow & 1
\end{array}$$

图 2.2

♡

证明

(1) 设 A, B, G 对应的 (短) 正合序列为

$$1 \longrightarrow A \xrightarrow{\lambda} G \xrightarrow{\mu} B \longrightarrow 1,$$

f 是 G 到 G' 上的同构. 令 $\lambda' = f\lambda, \mu' = \mu f^{-1}$. 由命题 2.10知 λ 是 A 到 G 的单同态且 $\lambda(A) = N$. 从而 λ' 是单同态且 $\lambda'(A) = f(\lambda(A))$ 与 A 同构. $\mu' = \mu f^{-1}$ 是 G' 到 B 上的同态, 又注意到

$$\mu'\left(\ker\mu'\right) = 1' \iff \mu\left(f^{-1}\left(\ker\mu'\right)\right) = 1' \iff f^{-1}\left(\ker\mu'\right) = \ker\mu \iff \ker\mu' = f\left(\ker\mu\right),$$

故

$$\ker\mu' = \ker(\mu f^{-1}) = f(\ker\mu) = f(\lambda(A)) = \lambda'(A).$$

因而 G' 是 B 过 A 的扩张.

(2) 先证 $\ker f = \{1\}$, 即 f 是单射. 若 $x \in \ker f$, 则 $\mu(x) = \mu' f(x) = \mu'(1) = 1$ 知 $x \in \ker\mu = \lambda(A)$, 因而 $\exists y \in A$, 使得 $x = \lambda(y)$. 于是 $\lambda'(y) = f(\lambda(y)) = f(x) = 1$. 由 (1) 的证明知 λ' 是单射, 故 $y = 1$, 于是 $x = \lambda(1) = 1$, 即 $\ker f = \{1\}$.

下面证 $f(G) = G'$, 即 f 是满映射. 设 $x' \in G'$, 由命题 2.10知 μ 是 G 到 B 的满同态, 即 $\mu(G) = B$, 从而 $\exists x \in G$, 使 $\mu(x) = \mu'(x')$, 但 $\mu = \mu' f$, 故

$$\mu'(f(x)) = \mu(x) = \mu'(x') \iff 1 = \left(\mu'(x')\right)^{-1}\mu'(f(x)) = \left(\mu'(x')^{-1}\right)\mu'(f(x)) = \mu'((x')^{-1}f(x)).$$

因而 $(x')^{-1}f(x) \in \ker\mu' = \lambda'(A) = f\lambda(A)$. 故 $\exists a \in A$, 使 $(x')^{-1}f(x) = f(\lambda(a)) \in f(G)$, 于是 $x' \in f(G)$, 即 f 是满映射.

□

定理 2.26

设群 G 是群 B 过群 A 的扩张, 对应的 (短) 正合序列为

$$1 \longrightarrow A \xrightarrow{\lambda} G \xrightarrow{\mu} B \longrightarrow 1,$$

扩张核为 $N = \lambda(A) = \ker \mu$.

(1) 若有 G 的子群 H 满足 $G = HN, H \cap N = \{1\}$, 则 $\mu|_H$ 是 H 到 B 上的同构, 此时 $(\mu|_H)^{-1} = \nu$ 是 B 到 G 中的同态且 $\mu\nu = \mathrm{id}_B$;

(2) 若存在 B 到 G 的同态 ν, 使得 $\mu\nu = \mathrm{id}_B$, 则 $\nu(B) = H$ 是 G 的子群,ν 是 B 到 $H = \nu(B)$ 上的同构且 $G = HN, H \cap N = \{1\}$.

♡

证明

(1) 由 $\ker(\mu|_H) = H \cap \ker \mu = H \cap N = \{1\}$ 知 $\mu|_H$ 是 H 到 B 的单射, 又 $\forall b \in B, \exists x \in G$, 使 $\mu(x) = b$, 而 $G = HN$, 故 $\exists y \in H, z \in N$, 使 $x = yz$. 于是 $b = \mu(x) = \mu(y)\mu(z) = \mu(y)$, 故 $\mu|_H$ 是 H 到 B 上的满映射, 于是 $\mu|_H$ 是 H 到 B 上的同构. 从而 ν 是 B 到 H 中的同构, 故 ν 是 B 到 G 中的同态. 又 $\mu\nu(b) = \mu(y) = b$, 故 $\mu\nu = \mathrm{id}_B$.

(2) 由命题 1.21(1)知 $\nu(B) = H$ 是 G 的子群. 由 $\mu\nu = \mathrm{id}_B$ 知 $x = \mu\nu(x) = \mu(1) = 1, \forall x \in \ker \nu$, 即 $\ker \nu \subseteq \{1\}$, 因此 $\ker \nu = \{1\}$, 故 ν 是 B 到 $H = \nu(B)$ 上的同构, 若 $x \in N \cap H$, 则由 $x \in N = \ker \mu$ 知 $\mu(x) = 1$, 由 $x \in H = \nu(B)$ 知存在 $b \in B$, 使 $x = \nu(b)$. 从而

$$1 = \mu(x) = \mu\nu(b) = \mathrm{id}_B(b) = b.$$

故 $x = \nu(b) = \nu(1) = 1$, 即 $H \cap N = \{1\}$.

对 $\forall b \in B$, 由 $\mu\nu = \mathrm{id}_B$ 知 $\mu(\nu(b)) = \mathrm{id}_B(b) = b$ 且 $\nu(b) \in H$, 故 $\mu|_H$ 是 H 到 B 上的满同态. 设 $x \in G$, 则 $\mu(x) \in B$. 于是 $\exists y \in H$, 使 $\mu(y) = \mu(x)$, 因而 $\mu(y^{-1}x) = 1$, 即 $z = y^{-1}x \in \ker \mu = N$ 有 $x = yz \in HN$, 故 $G = HN$.

□

定义 2.21

设 G 是一个群,$N \lhd G$,H 是 G 的子群, 且 $H \cap N = \{1\}, G = HN$, 则称 G 是 N 与 H 的**半直积**, 记为 $G = H \ltimes N$. 如果 H 还是 G 的正规子群, 则称 G 是 N 与 H 的**内直积**, 记为 $G = H \otimes N$.

♣

定义 2.22

设 G 是群 B 过群 A 的扩张, N 是扩张的核.

(1) 如果存在 G 的子群 H, 使 $H \cap N = \{1\}, G = HN$, 那么称此扩张为**非本质扩张**. 若 H 还是 G 的正规子群, 则称此扩张为**平凡扩张**.

(2) 如果 $N \subseteq C(G)$, 那么称此扩张为**中心扩张**.

♣

例题 2.7

1. 对整数加群 $\mathbb{Z}$, 它的正规子群 $2\mathbb{Z}$ 与 $\mathbb{Z}$ 同构, 而 $\mathbb{Z}/2\mathbb{Z} = \mathbb{Z}_2$ 是 2 阶循环群, 因而 $\mathbb{Z}$ 是 $\mathbb{Z}_2$ 过 $2\mathbb{Z}$ 的扩张. 由于 $\mathbb{Z}$ 的任何子群都不同构于 $\mathbb{Z}_2$, 因而这个扩张不是非本质扩张.
2. 设 $n \geqslant 3$. A_n 是 S_n 的正规子群, $\langle(12)\rangle$ 是 S_n 的 2 阶子群, $\langle(12)\rangle \cap A_n = \{\mathrm{id}\}, S_n = \langle(12)\rangle A_n$, 但 $\langle(12)\rangle$ 不是 S_n 的正规子群, 故 $S_n = \langle(12)\rangle \ltimes A_n$.
3. 3 阶循环群过 5 阶循环群的扩张 G 是 15 阶群. 由命题 2.7知这种扩张必然是平凡扩张, 即 $G = \langle a\rangle \otimes \langle b\rangle$, 其中, a, b 分别为 G 的 3 阶元素与 5 阶元素.

证明

□

定理 2.27

设 A, B 是 G 的子群.

(1) $G = AB, A \cap B = \{1\}$ 当且仅当 $\forall g \in G, \exists a \in A, b \in B$, 使得 $g = ab$ 且这种表示唯一.

(2) G 是 A 和 B 的内直积的充分必要条件是 G 满足如下两个条件:

(i) G 中每个元素可唯一地表为 ab 的形式, 其中 $a \in A, b \in B$;

(ii) A 中每个元素与 B 中任意元素可交换, 即: 对任意 $a \in A, b \in B$, 有 $ab = ba$.

♡

证明

(1) 由 $G = AB, A \cap B = \{1\}$ 知 $\forall g \in G, \exists a \in A, b \in B$, 使 $g = ab$. 若另有 $g = a'b', a' \in A, b' \in B$, 则 $a^{-1}a' = bb'^{-1} \in A \cap B = \{1\}$, 于是 $a = a', b = b'$.

反之, 若 $\forall g \in G, \exists a \in A, b \in B$, 使 $g = ab$, 则 $G = AB$. 又若 $c \in A \cap B$, 由 $c = 1 \cdot c = c \cdot 1$ 的表示唯一可知 $c = 1$, 故 $A \cap B = \{1\}$.

(2) 由定理 1.13(2)知条件 (i) 成立当且仅当 $A, B \lhd G$. 又由定理 2.27(1)知条件 (ii) 成立当且仅当 $G = AB, A \cap B = \{1\}$. 故 $G = A \otimes B$ 当且仅当 G 同时满足条件 (i)(ii).

□

定理 2.28

(1) 如果群 G 是正规子群 H 和 K 的内直积, 则 $H \times K \cong G$.

(2) 如果群 $G = G_1 \times G_2$, 则存在 G 的正规子群 G_1' 和 G_2', 且 G_i' 与 G_i 同构 $(i = 1, 2)$, 使得 $G = G_1' \otimes G_2'$.

♡

注 从这个定理可以看到, 群的内外直积的概念在同构意义下是一致的, 所以有时可不对内外直积加以区分, 而统称为**群的直积**.

证明

(1) 如果群 G 是正规子群 H 和 K 的内直积. 定义映射

$$\begin{aligned} \phi : H \times K &\longrightarrow G, \\ (h, k) &\longmapsto hk, \ \forall (h, k) \in H \times K, \end{aligned}$$

则由于 $G = HK$, 故 ϕ 是满射. 又由定理 2.27(2)知 G 中元素为 hk 形式时表法唯一, 故 ϕ 是单射. 又对任意的 $(h_1, k_1), (h_2, k_2) \in H \times K$, 由于 H 中的元素与 K 中的元素可交换, 故

$$\begin{aligned} \phi((h_1, k_1) \cdot (h_2, k_2)) &= \phi(h_1h_2, k_1k_2) = (h_1h_2)(k_1k_2) \\ &= (h_1k_1)(h_2k_2) = \phi(h_1, k_1) \cdot \phi(h_2, k_2), \end{aligned}$$

所以 ϕ 是同构映射, 从而 $H \times K \cong G$.

(2) 如果 $G = G_1 \times G_2$. 令

$$G_1' = \{(a_1, e_2) \mid a_1 \in G_1\}, \ G_2' = \{(e_1, a_2) \mid a_2 \in G_2\},$$

则容易验证 G_1', G_2' 都是 G 的子群, 且对任意的 $(a_1, a_2) \in G$,

$$(a_1, a_2) = (a_1, e_2)(e_1, a_2) \in G_1'G_2'.$$

这一表法是唯一的, 且对任意的 $(a_1, e_2) \in G_1', (e_1, a_2) \in G_2'$, 有

$$(a_1, e_2) \cdot (e_1, a_2) = (a_1, a_2) = (e_1, a_2) \cdot (a_1, e_2),$$

所以由定理 2.27(2)知 G 是 G_1' 与 G_2' 的内直积. 而

$$\phi_1 : a_1 \longmapsto (a_1, e_2)$$

以及

$$\phi_2 : a_2 \longmapsto (e_1, a_2)$$

分别为 G_1 到 G_1' 和 G_2 到 G_2' 的同构映射.

□

定理 2.29

设 A, B 是两个群, 则一定存在 B 过 A 的平凡扩张 $G = A \times B$, 并且 G 在同构意义下唯一.

♡

证明 在 $G = A \times B = \{(a,b) \mid a \in A, b \in B\}$ 中定义乘法

$$(a_1,b_1)(a_2,b_2) = (a_1a_2, b_1b_2), \quad \forall (a_i,b_i) \in G, i = 1,2.$$

容易验证 G 是群, 幺元为 $(1,1')$, 其中, $1, 1'$ 分别为 A, B 的幺元. $\forall (a,b) \in G, (a,b)^{-1} = (a^{-1}, b^{-1})$, 而且

$$A' = \{(a,1') \mid a \in A\}, \quad B' = \{(1,b) \mid b \in B\}$$

都是 G 的正规子群. 又 $G = A'B'$, $A' \cap B' = \{(1,1')\}$, 于是 $G = A' \otimes B'$.

又映射 λ: $\lambda(a) = (a,1')(\forall a \in A)$ 是 A 到 G 的单同态, $\lambda(A) = A'$, 故 λ 是 A 到 A' 的同构. 而映射 μ: $\mu((a,b)) = b$ 则是 G 到 B 上的同态, 并且 $\ker \mu = A' = \lambda(A)$, $\mu|_{B'}$ 是 B' 到 B 上的同构. 即有 (短) 正合序列

$$1 \longrightarrow A \xrightarrow{\lambda} G \xrightarrow{\mu} B \longrightarrow 1,$$

故由命题 2.10知 G 是 B 过 A 的扩张, 扩张核为 A'. 由 $G = A' \otimes B'$ 及 $A \cong A', B \cong B'$ 知

$$G = A'B', \quad A' \cap B' = \{1\}, \quad B' \lhd G.$$

故 G 是 B 过 A 的平凡扩张.

设 G_1 也是 B 过 A 的平凡扩张, 于是 $G_1 = A_1 \otimes B_1$. 设 λ_1 为 A 到 A_1 的同构, γ_1 是 B 到 B_1 的同构, 令

$$f((a,b)) = \lambda_1(a)\gamma_1(b), \quad \forall a \in A, b \in B.$$

由 $G_1 = A_1 \otimes B_1$ 知 $G_1 = A_1B_1, A_1 \cap B_1 = \{1\}$ 且 $A_1, B_1 \lhd G_1$. 从而由定理 1.13(2)知

$$a_1b_1 = b_1a_1, \quad \forall a_1 \in A_1, b_1 \in B_1.$$

于是对 $\forall (a,b), (a',b') \in G$, 有

$$\begin{aligned} f((a,b)(a',b')) &= f((aa', bb')) = \lambda_1(aa')\gamma_1(bb') \\ &= \lambda_1(a)\lambda_1(a')\gamma_1(b)\gamma_1(b') = \lambda_1(a)\gamma_1(b)\lambda_1(a')\gamma_1(b') \\ &= f((a,b))f((a',b')). \end{aligned}$$

因此 f 是 G 到 G_1 的同态.

设 $a_1b_1 \in A_1B_1 = G_1$, 则由 λ_1 是 A 到 A_1 的同构,γ_1 是 B 到 B_1 的同构可知, 存在 $a \in A$,$b \in B$, 使

$$\lambda_1(a) = a_1, \gamma_1(b) = b_1 \Longrightarrow f((a,b)) = \lambda_1(a)\gamma_1(b) = a_1b_1.$$

故 f 是满同态.

设 $f((a,b)) = f((a',b')) \in G_1$, 则

$$\lambda_1(a)\gamma_1(b) = f((a,b)) = f((a',b')) = \lambda_1(a')\gamma_1(b').$$

由定理 2.27(1)知 $\lambda_1(a) = \lambda_1(a')$,$\gamma_1(b) = \gamma_1(b')$. 又 λ_1 是 A 到 A_1 的同构,γ_1 是 B 到 B_1 的同构, 故

$$a = a', b = b' \Longrightarrow (a,b) = (a',b').$$

因此 f 是单同态. 综上可知 f 是 G 到 G_1 的同构.

□

定义 2.23

若 $N_1, N_2, \cdots, N_k$ 都是群 G 的正规子群, 并且

$$G = N_1N_2\cdots N_k, \ \text{其中} N_i \cap \prod_{j=1}^{i-1} N_j = \{1\}, \ i = 1,2,\cdots,k.$$

则称 G 是 $N_1, N_2, \cdots, N_k$ 的**内直积**, 记为

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

♣

定理 2.30

(1) 如果群 G 是有限多个子群 $N_1, N_2, \cdots, N_n$ 的内直积, 则

$$G = N_1 \otimes N_2 \otimes \cdots N_n \cong N_1 \times N_2 \times \cdots \times N_n.$$

(2) 设有限群 $N_1, N_2, \cdots, N_k$ 的内直积为 G, 即 $G = N_1 \otimes N_2 \otimes \cdots \otimes N_k$, 则

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

(3) 设群 $N_1, N_2, \cdots, N_k$ 的内直积为 G, 即 $G = N_1 \otimes N_2 \otimes \cdots \otimes N_k$, 则对 $\forall i, j \in \{1, 2, \cdots, k\}$, 有

$$n_i n_j = n_j n_i, \ \forall n_i \in N_i, n_j \in N_j.$$

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

$$N_1 \otimes N_2 \otimes \cdots \otimes N_k \lhd G.$$

(5) 设 $N_1, N_2, \cdots, N_k$ 都是群 G 的正规子群, 则群 G 满足

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

的充要条件是 G 中任一元素可分解为 $N_i (1 \leqslant i \leqslant k)$ 中元素的积且这种分解是唯一的.

♡

证明

(1) 对 n 用数学归纳法. 当 $n = 2$ 时, 由定理 2.28(1)知结论成立.

假定结论对 $n-1$ 成立. 考察 G 是 n 个正规子群 $N_1, N_2, \cdots, N_n$ 的内直积的情形. 令 $K = N_1 N_2 \cdots N_{n-1}$, 则由命题 1.8(5)知 K 为 G 的正规子群, 由命题 1.8(2)知 $N_i (i = 1, 2, \cdots, n-1)$ 为 K 的正规子群. 从而由内直积的定义可得,G 为 K 与 N_n 的内直积,K 为正规子群 $N_1, N_2, \cdots, N_{n-1}$ 的内直积. 于是由定理 2.28(1)及归纳假设得

$$G \cong K \times N_n, \quad K \cong N_1 \times N_2 \times \cdots \times N_{n-1}.$$

因此

$$G \cong N_1 \times N_2 \times \cdots \times N_n.$$

(2) 由定理 2.30(1)知

$$N_1 \otimes N_2 \otimes \cdots N_k \cong N_1 \times N_2 \times \cdots N_k.$$

再由定理 2.24(1)可得

$$|N_1 \otimes N_2 \otimes \cdots \otimes N_k| = |N_1 \times N_2 \times \cdots \times N_k| = |N_1|\,|N_2| \cdots |N_k|\,.$$

(3) 由内直积的定义和命题 1.8(6)立得.

(4) 由内直积的定义和命题 1.8(5)立得.

(5) **必要性**: 由内直积的定义知 $G = N_1 N_2 \cdots N_k$ 且 $N_i \cap \prod_{j=1}^{i-1} N_j = \{1\} (i \neq j)$, 则显然 G 中任一元素 g 可分解为 $N_i (1 \leqslant i \leqslant k)$ 中元素的积. 设 $g = n_1 n_2 \cdots n_k = n_1' n_2' \cdots n_k'$, 则

$$n_k' n_k^{-1} = n_1 (n_1')^{-1} n_2 (n_2')^{-1} \cdots n_{k-1} (n_{k-1}')^{-1} \in (N_1 N_2 \cdots N_{k-1}) \cap N_k = \{1\}.$$

从而 $n_k' n_k^{-1} = 1$, 所以

$$n_k = n_k', \quad \text{且} n_1 n_2 \cdots n_{k-1} = n_1' n_2' \cdots n_{k-1}'.$$

对等式 $n_1n_2\cdots n_{k-1}=n_1'n_2'\cdots n_{k-1}'$ 进行同样的讨论, 又可得

$$n_{k-1}=n_{k-1}', \quad \text{且} n_1n_2\cdots n_{n-2}=n_1'n_2'\cdots n_{n-2}'.$$

以此类推, 最后可得 $n_i=n_i'(i=1,2,\cdots,n)$. 因此 g 的分解唯一.

充分性: 由 G 中任一元素可分解为 $N_i(1\leqslant i\leqslant k)$ 中元素的积知 $G\subseteq N_1N_2\cdots N_k$. 又因为 $N_i\lhd G(i=1,2,\cdots,k)$, 所以 $N_1N_2\cdots N_k\subseteq G$. 故 $G=N_1N_2\cdots N_k$. 若存在 $i\in\{1,2,\cdots,k\}$, 使得 $N_i\cap\prod\limits_{j=1}^{i-1}N_j\neq\{1\}$. 取 $1\neq n_i\in N_i\cap\prod\limits_{j=1}^{i-1}N_j$, 则存在 $n_j'\in N_j$, $j=1,2,\cdots,i-1$ 且 $n_1',n_2',\cdots,n_{i-1}'$ 不全为 1, 使得 $n_i=n_1'n_2'\cdots n_{i-1}'$. 从而

$$n_i=1\cdots\underbrace{n_i}_{\text{第}i\text{个位置}}\cdots 1=n_1'n_2'\cdots n_{i-1}'\cdot 1\cdots 1\in N_1N_2\cdots N_k,$$

这与 n_i 的分解唯一矛盾! 故 $N_i\cap\prod\limits_{j=1}^{i-1}N_j=\{1\},i=1,2,\cdots,k$. 因此

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

□

命题 2.11

设 G 为有限群,$|G|=p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k},p_1,p_2,\cdots,p_k$ 为互不相等的素数. 又每个 Sylow p_i 子群 $P_i\lhd G$. 则

$$G=P_1\otimes P_2\otimes\cdots\otimes P_k.$$

♠

证明 由Sylow 第三定理 (1)知 P_i 是 G 中唯一的 Sylow p_i 子群 $(i=1,2,\cdots,k)$. 由条件知 $|P_i|=p_i^{a_i},i=1,2,\cdots,k$. 再由定理 2.30(2)知

$$\left|\prod_{i=1}^{k}P_i\right|=|P_1||P_2|\cdots|P_k|=p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}=|G|.$$

显然 $\prod\limits_{i=1}^{k}P_i\subseteq G$, 故 $G=\prod\limits_{i=1}^{k}P_i$.

由命题 2.5知对 $\forall x_i\in P_i\backslash\{1\},i=1,2,\cdots,k$, 都存在 $k_i\in\mathbb{N}\backslash\{0\}$, 使

$$\operatorname{ord}x_i=p_i^{k_i},\quad i=1,2,\cdots,k.$$

又因为 $p_1,\cdots,p_k$ 是互不相同的素数, 所以

$$\operatorname{ord}\prod_{j\neq i}x_j=\prod_{j\neq i}p_j^{k_j}\neq p_i^{k_i}=\operatorname{ord}x_i,\quad i=1,2,\cdots,k.$$

因此 $P_i\cap\prod\limits_{j\neq i}P_j=\{1\},i=1,2,\cdots,k$. 从而 $P_i\cap P_j=\{1\}(i\neq j)$.

综上可知

$$G=\prod_{i=1}^{k}P_i,\quad P_i\lhd G,\quad 1\leqslant i\leqslant k,$$

$$P_i\cap\prod_{j\neq i}P_j=\{1\},\quad 1\leqslant i\leqslant k,$$

故 $G=P_1\otimes P_2\otimes\cdots\otimes P_k$.

□

2.6 可解群和幂零群

定义 2.24 (换位子)

设 g_1, g_2 是群 G 中的两个元素, 称

$$[g_1, g_2] = g_1^{-1} g_2^{-1} g_1 g_2$$

为 g_1 与 g_2 的**换位子**.

♣

定义 2.25 (换位子群)

若 H, K 是群 G 的两个子群, 称

$$[H, K] = \langle \{[h, k] \mid h \in H,\ k \in K\} \rangle$$

为 H 与 K 的**换位子群**.

♣

命题 2.12

设 H, K 是群 G 的两个子群, 则

(1) $\alpha([g_1, g_2]) = [\alpha(g_1), \alpha(g_2)], \quad \forall \alpha \in \mathrm{Aut}G,\ g_1, g_2 \in G.$

(2) $\alpha([H, K]) = [\alpha(H), \alpha(K)], \quad \forall \alpha \in \mathrm{Aut}G.$

(3) 若 $H \lhd G$, 则 G/H 为 Abel 群的充要条件是 $H \supseteq [G, G]$.

♠

证明

(1) 从换位子的定义即得.

(2) 因为 $\forall a \in H, b \in K$, 有 $\alpha(a) \in \alpha(H), \alpha(b) \in \alpha(K)$. 注意到

$$\alpha([a, b]) = \alpha(aba^{-1}b^{-1}) = \alpha(a)\alpha(b)\alpha(a)^{-1}\alpha(b)^{-1} = [\alpha(a), \alpha(b)],$$

故 $\alpha([H, K]) = [\alpha(H), \alpha(K)]$.

(3) G/H 为 Abel 群, 当且仅当对 $\forall a, b \in G$, $(aH)(bH) = (bH)(aH)$, 即 $abH = baH, \forall a, b \in G$, 当且仅当 $[a, b] = a^{-1}b^{-1}ab \in H, \forall a, b \in G$, 即 $H \supseteq [G, G]$.

□

引理 2.2

设 H, K 是群 G 的子群, 则有

(1) $[H, K] = \{1\} \iff H \subseteq C_G(K)$;

(2) $[H, K] \subseteq K \iff H \subseteq N_G(K)$,
$[H, K] \subseteq H \iff K \subseteq N_G(H)$;

(3) 若 $H \lhd G, K \lhd G$, 则 $[H, K] \lhd G$ 且 $[H, K] \subseteq H \cap K$. 特别地, 由 $G \lhd G$ 知 $[G, G] \lhd G$;

(4) 当 H_1, K_1 分别为 H, K 的子群时有 $[H_1, K_1] \subseteq [H, K]$.

(5) 设 H, K 是两个群,$N \lhd H, K$, 则

$$[H, K] \subseteq N \iff [H/N, K/N] = N \iff H/N \subseteq C(K/N).$$

♡

证明

(1) $[H, K] = \{1\}$ 当且仅当对 $\forall h \in H, k \in K$ 有

$$[h, k] = 1 \iff h^{-1}k^{-1}hk = 1 \iff hk = kh \iff hkh^{-1} = k,$$

即 $h \in C_G(K), \forall h \in H$, 即 $H \subseteq C_G(K)$.

(2) 先证 $[H, K] \subseteq K \iff H \subseteq N_G(K)$. 若 $[H, K] \subseteq K$, 则

$$[h, k] \in K, \quad [h^{-1}, k^{-1}] \in K, \quad \forall k \in K,\ h \in H.$$

对 $\forall h\in H$, 设 $k\in K$, 则由 $[h,k]\in K$ 知存在 $k_1\in K$, 使

$$h^{-1}k^{-1}hk=k_1\Longleftrightarrow hkk_1^{-1}=kh\Longleftrightarrow k=hkk_1^{-1}h^{-1}\in hKh^{-1},$$

故 $K\subseteq hKh^{-1}$. 再设 $hkh^{-1}\in hKh^{-1}$, 则由 $[h^{-1},k^{-1}]\in K$ 知存在 $k_2\in K$, 使

$$hkh^{-1}k^{-1}=k_1\Longleftrightarrow hkh^{-1}=kk_1\in K,$$

故 $hKh^{-1}\subseteq K$. 因此 $hKh^{-1}=K,,\forall h\in H$. 即 $h\in N_G(K),\forall h\in H$. 故 $H\subseteq N_G(K)$.
反之, 若 $H\subseteq N_G(K)$, 对 $\forall h\in H,\ k\in K$, 有 $hKh^{-1}=K$, 从而存在 $h_1\in H,\ k_1\in K$, 使

$$k=h_1k_1h_1^{-1}\Longleftrightarrow k^{-1}=h_1k_1^{-1}h_1^{-1}.$$

于是

$$[h,k]=h^{-1}k^{-1}hk=h^{-1}h_1k_1^{-1}h_1^{-1}hk=(h^{-1}h_1)k_1^{-1}(h^{-1}h_1)^{-1}k.$$

注意到 $(h^{-1}h_1)k_1^{-1}(h^{-1}h_1)^{-1}\in hKh^{-1}$, 所以存在 $k_2\in K$, 使 $(h^{-1}h_1)k_1^{-1}(h^{-1}h_1)^{-1}=k_2$. 从而

$$[h,k]=(h^{-1}h_1)k_1^{-1}(h^{-1}h_1)^{-1}k=k_2k\in K,\ \forall k\in K,h\in H.$$

故 $[H,K]\subseteq K$.
再证 $[H,K]\subseteq H\iff K\subseteq N_G(H)$. 若 $[H,K]\subseteq H$, 则

$$[h,k]\in H,\quad [h^{-1},k^{-1}]\in H,\quad \forall k\in K,\ h\in H.$$

对 $\forall k\in K$, 设 $h\in H$, 则由 $[h,k]\in H$ 知存在 $h_1\in H$, 使

$$h^{-1}k^{-1}hk=h_1\Longleftrightarrow hk=khh_1\Longleftrightarrow h=khh_1k^{-1}\in kHk^{-1},$$

故 $H\subseteq kHk^{-1}$. 再设 $khk^{-1}\in kHk^{-1}$, 则由 $[h^{-1},k^{-1}]\in H$ 知存在 $h_2\in H$, 使

$$hkh^{-1}k^{-1}=h_1\Longleftrightarrow khk^{-1}=h^{-1}h_1\in H,$$

故 $kHk^{-1}\subseteq H$. 因此 $kHk^{-1}=H,\forall k\in K$. 即 $k\in N_G(H),\forall k\in K$. 故 $K\subseteq N_G(H)$.
反之, 若 $K\subseteq N_G(H)$, 对 $\forall h\in H,\ k\in K$, 有 $kHk^{-1}=H$, 从而存在 $h_1\in H,\ k_1\in K$, 使

$$h=k_1h_1k_1^{-1}.$$

于是

$$[h,k]=h^{-1}k^{-1}hk=h^{-1}k^{-1}k_1h_1k_1^{-1}k=h^{-1}(k^{-1}k_1)h_1(k^{-1}k_1)^{-1}.$$

注意到 $(k^{-1}k_1)h_1(k^{-1}k_1)^{-1}\in kHk^{-1}$, 所以存在 $h_2\in H$, 使 $(k^{-1}k_1)h_1(k^{-1}k_1)^{-1}=h_2$. 从而

$$[h,k]=h^{-1}(k^{-1}k_1)h_1(k^{-1}k_1)^{-1}=h^{-1}h_2\in H.$$

故 $[H,K]\subseteq H$.

(3) 设 $H\lhd G,K\lhd G$, 于是对 $\forall\alpha=L_gR_{g^{-1}}\in \mathrm{Int}G$, 由命题 2.12(2)有

$$g[H,K]g^{-1}=\alpha([H,K])=[\alpha(H),\alpha(K)]=[gHg^{-1},gKg^{-1}]=[H,K],$$

即 $[H,K]\lhd G$. 由 $H\lhd G,K\lhd G$ 知

$$gHg^{-1}=H,\quad gKg^{-1}=K,\quad \forall g\in G.$$

故

$$kHk^{-1}=H,\quad \forall k\in K;$$

$$hKh^{-1}=K,\quad \forall h\in H.$$

即 $K\subseteq N_G(H)$, $H\subseteq N_G(K)$. 再由结论 (2) 知 $[H,K]\subseteq H\cap K$.

(4) 此结论是显然的.

(5) 由引理 2.2(1)知

$$[H/N,K/N]=N\Longleftrightarrow H/N\subseteq C(K/N).$$

于是对 $\forall a \in H, b \in K$, 有

$$N = [aN, bN] = (a^{-1}N)(b^{-1}N)(aN)(bN) = (a^{-1}b^{-1}ab)N = [a, b]N.$$

这也当且仅当

$$[a, b] \in N, \quad \forall a \in H, b \in K.$$

即 $[H, K] \subseteq N$.

□

定义 2.26

幺元为 1 的群 G 中的子群序列

$$G = G_1 \supseteq G_2 \supseteq \cdots \supseteq G_t \supseteq G_{t+1} = \{1\}.$$

若满足 $G_i \lhd G_{i-1} (2 \leqslant i \leqslant t+1)$, 则称之为**次正规序列**,$t$ 称为此序列的**长度**.$G_{i-1}/G_i (2 \leqslant i \leqslant t+1)$ 称为此序列的**因子**. 若在上述序列中还有 $G_i \lhd G (1 \leqslant i \leqslant t+1)$, 则称此序列为**正规序列**.

若两个次正规序列 (正规序列)

$$G = G_1' \supseteq G_2' \supseteq \cdots \supseteq G_r' \supseteq G_{r+1}' = \{1\},$$

$$G = G_1 \supseteq G_2 \supseteq \cdots \supseteq G_t \supseteq G_{t+1} = \{1\}$$

满足 $\forall G_i' (1 \leqslant i \leqslant r+1), \exists G_{i_j} = G_i' (1 \leqslant i_j \leqslant t+1)$, 则称此序列 $\{G_j\}$ 是序列 $\{G_i'\}$ 的**加细**.

♣

例题 2.8 $S_3 \supset A_3 \supset \{\mathrm{id}\}$ 是 S_3 的正规序列.

证明

□

例题 2.9 $S_4 \supset A_4 \supset K_4 \supset \{\mathrm{id}\}$ 是 S_4 的正规序列, 而 $S_4 \supset A_4 \supset K_4 \supset \langle (12)(34) \rangle \supset \{\mathrm{id}\}$ 是 S_4 的次正规序列, 后者是前者作为次正规序列的加细.

证明

□

定义 2.27

在群 G 中分别归纳地定义 G 的子群序列 $\{G^{(k)}\}, \{\Gamma_k(G)\}, \{C_k(G)\}$ 为

$$G^{(0)} = G, \quad G^{(k)} = [G^{(k-1)}, G^{(k-1)}], \quad k > 0;$$

$$\Gamma_1(G) = G, \quad \Gamma_k(G) = [G, \Gamma_{k-1}(G)], \quad k > 1;$$

$$C_0(G) = \{1\}, \quad C_k(G)/C_{k-1}(G) = C(G/C_{k-1}(G)), \quad k > 0.$$

分别称群 G 中序列

$$G = G^{(0)} \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \cdots,$$

$$G = \Gamma_1(G) \supseteq \Gamma_2(G) \supseteq \cdots,$$

$$C_0(G) \subseteq C_1(G) \subseteq C_2(G) \subseteq \cdots$$

为 G 的**导出列**、**降中心列**和**升中心列**.

若有 $k \in \mathbb{N}$, 使 $G^{(k)} = \{1\}$, 则称 G 是**可解群**. 若有 $k \in \mathbb{N}$, 使 $\Gamma_k(G) = \{1\}$, 则称 G 是**幂零群**.

♣

注 显然有

$$G^{(0)} = G \supseteq [G, G] = G^{(1)}.$$

假设 $G^{(k-1)} \supseteq G^{(k)}$, 则由引理 2.2(4)可得

$$G^{(k)} = [G^{(k-1)}, G^{(k-1)}] \supseteq [G^{(k)}, G^{(k)}] = G^{(k+1)}.$$

故由数学归纳法知

$$G = G^{(0)} \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \cdots .$$

因此 G 的导出列是良定义的.

显然有

$$\Gamma_1(G) = G \supseteq [G, G] = \Gamma_2(G).$$

假设 $\Gamma_{k-1}(G) \supseteq \Gamma_k(G)$, 则由引理 2.2(4)可得

$$\Gamma_k(G) = [G, \Gamma_{k-1}(G)] \supseteq [G, \Gamma_k(G)] = \Gamma_{k+1}(G).$$

故由数学归纳法知

$$G = \Gamma_1(G) \supseteq \Gamma_2(G) \supseteq \cdots .$$

因此 G 的降中心列是良定义的.

由定理 2.12(3)知 $C_1(G) = C(G) \lhd G$. 设 π_1 是 G 到 $G/C_1(G)$ 上的自然同态. 令

$$C_2(G) = \pi_1^{-1}(C(G/C_1(G))),$$

则由定理 2.12(3)知 $\pi_1(C_2(G)) = C(G/C_1(G)) \lhd G/C_1(G)$, 再由定理 1.39(2)知 $C_2(G) \lhd \pi_1^{-1}(G/C_1(G)) = G$. 因为 $\pi_1(C_1(G)) = \{1\} \subseteq C(G/C_1(G))$, 所以

$$C_1(G) \subseteq \pi_1^{-1}(C(G/C_1(G))) = C_2(G).$$

从而由命题 1.8(2)知 $C_1(G) \lhd C_2(G)$. 将 π_1 看作限制在 $C_2(G)$ 上的同态, 则由群的同态基本定理知

$$C_2(G)/C_1(G) = C_2(G)/\ker\pi_1|_{C_2(G)} \cong \pi_1|_{C_2(G)}(C_2(G)) = C(G/C_1(G)).$$

因此

$$C_2(G)/C_1(G) = C(G/C_1(G)).$$

再令 π_2 是 G 到 $G/C_2(G)$ 上的自然同态, 则

$$C_3(G) = \pi_2^{-1}(C(G/C_2(G))),$$

同理可得

$$C_2(G) \lhd C_3(G), \quad C_3(G)/C_2(G) = C(G/C_2(G)).$$

如此进行下去, 即得所有 $C_k(G)$. 因此 G 的升中心列是良定义的.

命题 2.13

(1) 若 G 是一个群, 则 $G^{(k_1+k_2)} = (G^{(k_1)})^{(k_2)}, \Gamma_{k_1+k_2}(G) = \Gamma_{k_2}\left(\Gamma_{k_1}(G)\right), \ \forall k_1, k_2 \in \mathbb{N}.$

(2) 若 A 是群 B 的子群, 则 $A^{(k)} \subseteq B^{(k)}, \Gamma_k(A) \subseteq \Gamma_k(B), \ \forall k \in \mathbb{N}.$

(3) 若 f 是群 G 到群 B 的同态, 则 $(f(G))^{(k)} = f(G^{(k)}), \Gamma_k(f(G)) = f(\Gamma_k(G)), \ \forall k \in \mathbb{N}.$

(4) 设 A, B 是两个群, 则

$$(nA \times B)^{(k)} = A^{(k)} \times B^{(k)}, \quad \forall k \in \mathbb{N}.$$

$$\Gamma_k(A \times B) = \Gamma_k(A) \times \Gamma_k(B), \quad \forall k \in \mathbb{N}.$$

(5) 设 π_k 群是 G 到 $G/C_k(G)(k \in \mathbb{N})$ 上的自然同态, 则

$$C_{k+1}(G) = \pi_k^{-1}(C(G/C_k(G))), \quad \forall k \in \mathbb{N}.$$

(6) 设 G 是一个群, 则对 $\forall a \in G$, 有

$$a \in C_{k+1}(G) \Longleftrightarrow [a,b] \in C_k(G), \forall b \in G.$$

(7) 设 G 是一个群, 则

$$G^{(k+1)} \lhd G^{(k)}, \quad G^{(k)} \lhd G, \quad k = 0,1,\cdots.$$

$$\Gamma_{k+1}(G) \lhd \Gamma_k(G), \quad \Gamma_k(G) \lhd G, \quad k = 0,1,\cdots.$$

$$C_k(G) \lhd C_{k+1}(G), \quad C_k(G) \lhd G, \quad k = 0,1,\cdots.$$

♠

证明

(1) 对 $\forall k_1 \in \mathbb{N}$, 都有

$$G^{(k_1+1)} = [G^{(k_1)}, G^{(k_1)}] = (G^{(k_1)})^{(1)}.$$

假设 $G^{(k_1+k_2-1)} = (G^{(k_1)})^{(k_2-1)}$, 则

$$G^{(k_1+k_2)} = [G^{(k_1+k_2-1)}, G^{(k_1+k_2-1)}] = [(G^{(k_1)})^{(k_2-1)}, (G^{(k_1)})^{(k_2-1)}] = (G^{(k_1)})^{(k_2)}.$$

故由数学归纳法知

$$G^{(k_1+k_2)} = (G^{(k_1)})^{(k_2)}, \quad \forall k_2 \in \mathbb{N}.$$

再由 k_1 的任意性可得

$$G^{(k_1+k_2)} = (G^{(k_1)})^{(k_2)}, \quad \forall k_1, k_2 \in \mathbb{N}.$$

对 $\forall k_1 \in \mathbb{N}$, 都有

$$\Gamma_{k_1+1}(G) = \left[G, \Gamma_{k_1}(G)\right] = \Gamma_1\left(\Gamma_{k_1}(G)\right).$$

假设 $\Gamma_{k_1+k_2-1}(G) = \Gamma_{k_2-1}\left(\Gamma_{k_1}(G)\right)$, 则

$$\Gamma_{k_1+k_2}(G) = \left[G, \Gamma_{k_1+k_2-1}(G)\right] = \left[G, \Gamma_{k_2-1}\left(\Gamma_{k_1}(G)\right)\right] = \Gamma_{k_2}\left(\Gamma_{k_1}(G)\right).$$

故由数学归纳法知

$$\Gamma_{k_1+k_2}(G) = \Gamma_{k_2}\left(\Gamma_{k_1}(G)\right), \quad \forall k_2 \in \mathbb{N}.$$

再由 k_1 的任意性可得

$$\Gamma_{k_1+k_2}(G) = \Gamma_{k_2}\left(\Gamma_{k_1}(G)\right), \quad \forall k_1, k_2 \in \mathbb{N}.$$

(2) 由条件知 $A^{(0)} = A \subseteq B = B^{(0)}$. 假设 $A^{(k-1)} \subseteq B^{(k-1)}$, 则由引理 2.2(4)知

$$A^{(k)} = \left[A^{(k-1)}, A^{(k-1)}\right] \subseteq \left[B^{(k-1)}, B^{(k-1)}\right] = B^{(k)}.$$

故由数学归纳法知

$$A^{(k)} \subseteq B^{(k)}, \quad \forall k \in \mathbb{N}.$$

由条件知 $\Gamma_1(A) = A \subseteq B = \Gamma_1(B)$. 假设 $\Gamma_{k-1}(A) \subseteq \Gamma_{k-1}(B)$, 则由引理 2.2(4)知

$$\Gamma_k(A) = [A, \Gamma_{k-1}(A)] \subseteq [B, \Gamma_{k-1}(B)] = \Gamma_k(B).$$

故由数学归纳法知

$$\Gamma_k(A) \subseteq \Gamma_k(B), \quad \forall k \in \mathbb{N}.$$

(3) 显然 $f\left(G^{(0)}\right) = f(G) = (f(G))^{(0)}$. 假设 $f\left(G^{(k-1)}\right) = (f(G))^{(k-1)}$. 任取 $f\left(a^{-1}b^{-1}ab\right) \in f\left(\left[G^{(k-1)}, G^{(k-1)}\right]\right) = f\left(G^{(k)}\right)$, 则 $a, b \in G^{(k-1)}$, 进而

$$f(a), f(b) \in f\left(G^{(k-1)}\right) = (f(G))^{(k-1)}.$$

从而

$$f\left(a^{-1}b^{-1}ab\right)=f(a)^{-1}f(b)^{-1}f(a)f(b)\in\left[(f(G))^{(k-1)},(f(G))^{(k-1)}\right]=(f(G))^{(k)}.$$

故 $f\left(G^{(k)}\right)\subseteq(f(G))^{(k)}$. 再任取 $f(a)^{-1}f(b)^{-1}f(a)f(b)\in\left[(f(G))^{(k-1)},(f(G))^{(k-1)}\right]=(f(G))^{(k)}$, 则

$$f(a),f(b)\in(f(G))^{(k-1)}=f\left(G^{(k-1)}\right),$$

进而由命题 1.5(i)知 $a,b\in G^{(k-1)}$. 从而

$$f(a)^{-1}f(b)^{-1}f(a)f(b)=f\left(a^{-1}b^{-1}ab\right)\in f\left(\left[G^{(k-1)},G^{(k-1)}\right]\right)=f\left(G^{(k)}\right).$$

故 $f\left(G^{(k)}\right)\supseteq(f(G))^{(k)}$. 因此 $f\left(G^{(k)}\right)=(f(G))^{(k)}$. 故由数学归纳法知 $f\left(G^{(k)}\right)=(f(G))^{(k)},\forall k\in\mathbb{N}$.

显然 $\Gamma_1(f(G))=f(G)=f(\Gamma_1(G))$. 假设 $\Gamma_{k-1}(f(G))=f(\Gamma_{k-1}(G))$. 任取 $f\left(a^{-1}b^{-1}ab\right)\in f([G,\Gamma_{k-1}(G)])=f(\Gamma_k(G))$, 则 $a\in G,b\in\Gamma_{k-1}(G)$, 进而

$$f(a)\in f(G),\quad f(b)\in f(\Gamma_{k-1}(G))=\Gamma_{k-1}(f(G)).$$

从而

$$f\left(a^{-1}b^{-1}ab\right)=f(a)^{-1}f(b)^{-1}f(a)f(b)\in\left[f(G),\Gamma_{k-1}(f(G))\right]=\Gamma_k(f(G)).$$

因此 $f(\Gamma_k(G))\subseteq\Gamma_k(f(G))$. 再任取 $f(a)^{-1}f(b)^{-1}f(a)f(b)\in\left[f(G),\Gamma_{k-1}(f(G))\right]=\Gamma_k(f(G))$, 则

$$f(a)\in f(G),\quad f(b)\in\Gamma_{k-1}(f(G))=f(\Gamma_{k-1}(G)).$$

进而由命题 1.5(i)知 $a\in G,b\in\Gamma_{k-1}(G)$. 从而

$$f(a)^{-1}f(b)^{-1}f(a)f(b)=f\left(a^{-1}b^{-1}ab\right)\in f([G,\Gamma_{k-1}(G)])=f(\Gamma_k(G)).$$

因此 $\Gamma_k(f(G))\subseteq f(\Gamma_k(G))$. 综上可知 $\Gamma_k(f(G))=f(\Gamma_k(G))$. 故由数学归纳法可知

$$\Gamma_k(f(G))=f(\Gamma_k(G)),\quad\forall k\in\mathbb{N}.$$

(4) 显然 $(A\times B)^{(0)}=A\times B=A^{(0)}\times B^{(0)}$. 假设 $(A\times B)^{(k-1)}=A^{(k-1)}\times B^{(k-1)}$, 则

$$(A\times B)^{(k)}=\left[(A\times B)^{(k-1)},(A\times B)^{(k-1)}\right]=\left[A^{(k-1)}\times B^{(k-1)},A^{(k-1)}\times B^{(k-1)}\right].\tag{2.22}$$

下证 $\left[A^{(k-1)}\times B^{(k-1)},A^{(k-1)}\times B^{(k-1)}\right]=A^{(k)}\times B^{(k)}$. 任取 $[(a_1,b_1),(a_2,b_2)]\in\left[A^{(k-1)}\times B^{(k-1)},A^{(k-1)}\times B^{(k-1)}\right]$, 则

$$a_i\in A^{(k-1)},\quad b_i\in B^{(k-1)},\quad i=1,2.$$

从而

$$\begin{aligned}[(a_1,b_1),(a_2,b_2)]&=\left(a_1^{-1},b_1^{-1}\right)\left(a_2^{-1},b_2^{-1}\right)(a_1,b_1)(a_2,b_2)=\left(a_1^{-1}a_2^{-1}a_1a_2,b_1^{-1}b_2^{-1}b_1b_2\right)\\&=([a_1,a_2],[b_1,b_2])\in\left[A^{(k-1)},A^{(k-1)}\right]\times\left[B^{(k-1)},B^{(k-1)}\right]=A^{(k)}\times B^{(k)}.\end{aligned}$$

故 $\left[A^{(k-1)}\times B^{(k-1)},A^{(k-1)}\times B^{(k-1)}\right]\subseteq A^{(k)}\times B^{(k)}$. 再任取

$$([a_1,a_2],[b_1,b_2])\in A^{(k)}\times B^{(k)}=\left[A^{(k-1)},A^{(k-1)}\right]\times\left[B^{(k-1)},B^{(k-1)}\right],$$

则

$$a_i\in A^{(k-1)},\quad b_i\in B^{(k-1)},\quad i=1,2.$$

从而

$$\begin{aligned}([a_1,a_2],[b_1,b_2])&=\left(a_1^{-1}a_2^{-1}a_1a_2,b_1^{-1}b_2^{-1}b_1b_2\right)=\left(a_1^{-1},b_1^{-1}\right)\left(a_2^{-1},b_2^{-1}\right)(a_1,b_1)(a_2,b_2)\\&=[(a_1,b_1),(a_2,b_2)]\in\left[A^{(k-1)}\times B^{(k-1)},A^{(k-1)}\times B^{(k-1)}\right].\end{aligned}$$

故 $A^{(k)}\times B^{(k)}\subseteq\left[A^{(k-1)}\times B^{(k-1)},A^{(k-1)}\times B^{(k-1)}\right]$. 因此 $\left[A^{(k-1)}\times B^{(k-1)},A^{(k-1)}\times B^{(k-1)}\right]=A^{(k)}\times B^{(k)}$. 再结合(2.22)式可得

$$(A\times B)^{(k)}=A^{(k)}\times B^{(k)}.$$

故由数学归纳法可知

$$(A\times B)^{(k)}=A^{(k)}\times B^{(k)},\quad \forall k\in\mathbb{N}.$$

显然 $\Gamma_1(A\times B)=A\times B=\Gamma_1(A)\times\Gamma_1(B)$. 假设 $\Gamma_{k-1}(A\times B)=\Gamma_{k-1}(A)\times\Gamma_{k-1}(B)$, 则

$$\Gamma_k(A\times B)=[A\times B,\Gamma_{k-1}(A\times B)]=[A\times B,\Gamma_{k-1}(A)\times\Gamma_{k-1}(B)]. \tag{2.23}$$

下证 $[A\times B,\Gamma_{k-1}(A)\times\Gamma_{k-1}(B)]=\Gamma_k(A)\times\Gamma_k(B)$. 任取 $[(a_1,b_1),(a_2,b_2)]\in[A\times B,\Gamma_{k-1}(A)\times\Gamma_{k-1}(B)]$, 则

$$a_1\in A,\quad b_1\in B,\quad a_2\in\Gamma_{k-1}(A),\quad b_2\in\Gamma_{k-1}(B).$$

从而

$$\begin{aligned}[(a_1,b_1),(a_2,b_2)]&=\left(a_1^{-1},b_1^{-1}\right)\left(a_2^{-1},b_2^{-1}\right)(a_1,b_1)(a_2,b_2)=\left(a_1^{-1}a_2^{-1}a_1a_2,b_1^{-1}b_2^{-1}b_1b_2\right)\\&=([a_1,a_2],[b_1,b_2])\in[A,\Gamma_{k-1}(A)]\times[B,\Gamma_{k-1}(B)]=\Gamma_k(A)\times\Gamma_k(B).\end{aligned}$$

因此 $[A\times B,\Gamma_{k-1}(A)\times\Gamma_{k-1}(B)]\subseteq\Gamma_k(A)\times\Gamma_k(B)$. 再任取

$$([a_1,a_2],[b_1,b_2])\in\Gamma_k(A)\times\Gamma_k(B)=[A,\Gamma_{k-1}(A)]\times[B,\Gamma_{k-1}(B)],$$

则

$$a_1\in A,\quad a_2\in\Gamma_{k-1}(A),\quad b_1\in B,\quad b_2\in\Gamma_{k-1}(B).$$

从而

$$\begin{aligned}([a_1,a_2],[b_1,b_2])&=\left(a_1^{-1}a_2^{-1}a_1a_2,b_1^{-1}b_2^{-1}b_1b_2\right)=\left(a_1^{-1},b_1^{-1}\right)\left(a_2^{-1},b_2^{-1}\right)(a_1,b_1)(a_2,b_2)\\&=[(a_1,b_1),(a_2,b_2)]\in[A\times B,\Gamma_{k-1}(A)\times\Gamma_{k-1}(B)].\end{aligned}$$

因此 $\Gamma_k(A)\times\Gamma_k(B)\subseteq[A\times B,\Gamma_{k-1}(A)\times\Gamma_{k-1}(B)]$. 故 $[A\times B,\Gamma_{k-1}(A)\times\Gamma_{k-1}(B)]=\Gamma_k(A)\times\Gamma_k(B)$. 再由(2.23)式可得

$$\Gamma_k(A\times B)=\Gamma_k(A)\times\Gamma_k(B).$$

故由数学归纳法可知

$$\Gamma_k(A\times B)=\Gamma_k(A)\times\Gamma_k(B),\quad \forall k\in\mathbb{N}.$$

(5) 由 G 的升中心列的定义可得

$$\pi_k(C_{k+1}(G))=C_{k+1}(G)/C_k(G)=C(G/C_k(G)),\quad \forall k\in\mathbb{N}.$$

(6) 由命题 2.13(5)可得

$$\begin{aligned}&a\in C_{k+1}(G)=\pi_k^{-1}(C(G/C_k(G)))\Longleftrightarrow\pi_k(a)\in\pi_k(C_{k+1}(G))\\&\Longleftrightarrow aC_k(G)\in C_{k+1}(G)/C_k(G)=C(G/C_k(G))\\&\Longleftrightarrow(aC_k(G))(bC_k(G))=(bC_k(G))(aC_k(G)),\forall b\in G\\&\Longleftrightarrow[a,b]C_k(G)=a^{-1}b^{-1}abC_k(G)=C_k(G),\forall b\in G\\&\Longleftrightarrow[a,b]\in C_k(G),\forall b\in G.\end{aligned}$$

(7) 由引理 2.2(3)知

$$G^{(k)}=[G^{(k-1)},G^{(i-1)}]\lhd G^{(k-1)},k=1,2,\cdots.$$

又显然 $G^{(0)}=G\lhd G$. 假设 $G^{(k-1)}\lhd G$, 则由引理 2.2(3)可得

$$G^{(k)}=\left[G^{(k-1)},G^{(k-1)}\right]\lhd G.$$

故由数学归纳法知 $G^{(k)}\lhd G,k=1,2,\cdots$.

显然 $\Gamma_1(G)=G\lhd G$. 假设 $\Gamma_{k-1}(G)\lhd G$, 则由引理 2.2(3)可得

$$\Gamma_k(G)=[G,\Gamma_{k-1}(G)]\lhd G.$$

故由数学归纳法知 $\Gamma_k(G) \lhd G, k = 1, 2, \cdots$. 又 $\Gamma_k(G) \subseteq \Gamma_{k-1}(G), k = 1, 2, \cdots$, 再由命题 1.8(2)知

$$\Gamma_k(G) \lhd \Gamma_{k-1}(G), \ k = 1, 2, \cdots .$$

显然 $C_0(G) = \{1\} \lhd G$. 假设 $C_k(G) \lhd G$. 设 π_k 是 G 到 $G/C_k(G)$ 的自然同态, 则由命题 2.13(5)知

$$C_{k+1}(G) = \pi_k^{-1}\left(C\left(G/C_k(G)\right)\right), \quad k = 0, 1, \cdots .$$

由定理 2.12(3)知 $C(G/C_k) \lhd G/C_k$. 再由定理 1.39(2)知

$$C_{k+1}(G) = \pi_k^{-1}\left(C\left(G/C_k(G)\right)\right) \lhd G, \quad k = 0, 1, \cdots .$$

故由数学归纳法知

$$C_k(G) \lhd G, \quad k = 0, 1, \cdots .$$

再由命题 1.8(2)知

$$C_k(G) \lhd C_{k+1}(G), \quad k = 0, 1, \cdots .$$

□

命题 2.14

Abel 群是幂零群, 也是可解群. 特别地, 循环群都是幂零群, 也都是可解群. ♠

证明

因为循环群都是 Abel 群, 所以循环群都是幂零群, 也都是可解群.

□

例题 2.10 设 $G = S_3$, 于是 $G^{(1)} = \Gamma_2(G) = A_3$, 因而 $G^{(2)} = \{1\}$, 但 $\Gamma_3(G) = A_3 = \Gamma_2(G)$, 故当 $k \geqslant 2$ 时均有 $\Gamma_k(G) = A_3 \neq \{1\}$, 故 S_3 是可解群但不是幂零群.

证明

□

定理 2.31

(1) 设 G 是可解群,A 是可解群 G 的子群, 则 A 也是可解群.

(2) 设 G 是可解群,f 是群 G 到群 G_1 的同态, 则 $f(G)$ 也是可解群.

(3) 设群 G 是群 B 过群 A 的扩张, 则 G 可解的充分必要条件是 A, B 都是可解群. ♡

证明

(1) 由 G 是可解群知, 存在 $k_0 \in \mathbb{N}$, 使得 $G^{(k_0)} = \{1\}$. 再由命题 2.13(2)知 $A^{(k_0)} \subseteq G^{(k_0)} = \{1\}$, 故 $A^{(k_0)} = \{1\}$, 即 A 是可解群.

(2) 由 G 是可解群知, 存在 $k_0 \in \mathbb{N}$, 使得 $G^{(k_0)} = \{1\}$. 再由命题 2.13(3)知 $(f(G))^{(k_0)} = f\left(G^{(k_0)}\right) = \{1\}$, 故 $f(G)$ 是可解群.

(3) 由 G 是 B 过 A 的扩张, 故可假定 $A \lhd G, B = G/A$. 又设 π 是 G 到 B 的自然同态. 由命题 2.13(2)知

$$A^{(k)} \subseteq G^{(k)}, \ k = 0, 1, \cdots . \tag{2.24}$$

由命题 2.13(3)知

$$B^{(k)} = \pi(G^{(k)}), \ k = 0, 1, \cdots . \tag{2.25}$$

若 G 可解, 则存在 $k_0 \in \mathbb{N}$, 使得 $G^{(k_0)} = \{1\}$. 于是由(2.24)式得 $A^{(k_0)} \subseteq G^{(k_0)} = \{1\}$, 故 $A = \{1\}$, 即 A 可解. 再由(2.25)式得 $B^{(k_0)} = \pi(G^{(k_0)}) = \pi(\{1\}) = \{1\}$, 故 B 可解.

反之, 若 A, B 可解, 则存在 k_1, k_2, 使 $A^{(k_1)} = B^{(k_2)} = \{1\}$, 故由(2.25)式得 $\pi(G^{(k_2)}) = B^{k_2} = \{1\}$, 即 $G^{(k_2)} \subseteq \ker\pi = A$. 由命题 2.13(2)知 $(G^{(k_1)})^{(k)} \subseteq A^{(k)}, \forall k \in \mathbb{N}$. 因而再由命题 2.13(1)知 $G^{(k_1+k_2)} = (G^{(k_1)})^{(k_2)} \subseteq A^{(k_2)} = \{1\}$, 故 $G^{(k_1+k_2)} = \{1\}$, 于是 G 可解.

□

定理 2.32

设 G 是有限群, 则下列条件等价:

(1) G 是可解群;

(2) 存在 G 的正规序列

$$G = G_1 \supseteq G_2 \supseteq \cdots \supseteq G_r = \{1\},$$

使 G_i/G_{i+1} 为 Abel 群,$1 \leqslant i \leqslant r-1$;

(3) 存在 G 的次正规序列

$$G = G_1' \supseteq G_2' \supseteq \cdots \supseteq G_s' = \{1\},$$

使 G_i'/G_{i+1}' 为 Abel 群,$1 \leqslant i \leqslant s-1$;

(4) 存在 G 的次正规序列

$$G = G_1'' \supseteq G_2'' \supseteq \cdots \supseteq G_t'' = \{1\},$$

使 G_i''/G_{i+1}'' 为素数阶群,$1 \leqslant i \leqslant t-1$.

♡

注 由这个定理的证明知: **群 G 是可解群的充要条件是 G 的导出列都是正规序列且因子都是 Abel 群.**

证明 (1) $\Rightarrow$ (2). 由于 G 可解, 故有 $k \in \mathbb{N}$, 使 $G^{(k)} = \{1\}$. 再由命题 2.13(7)知 G 中有正规序列

$$G = G^0 \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \cdots \supseteq G^{(k)} = \{1\}.$$

因为 $G^{(i)} = \left[G^{(i-1)}, G^{(i-1)}\right], G^{(i)} \lhd G^{(i-1)}$, 所以由命题 2.12(3)知 $G^{(i-1)}/G^{(i)}$ 是 Abel 群, 故 G 的导出列满足 (2) 的要求.

(2) $\Rightarrow$ (3). 由于正规序列必为次正规序列, 故条件 (2) 成立一定有条件 (3) 成立.

(3) $\Rightarrow$ (4). 设 $G = G_1' \supseteq G_2' \supseteq \cdots \supseteq G_s' = \{1\}$ 是 G 的次正规序列, 并且 G_i'/G_{i+1}' 为 Abel 群. 由于 G 是有限群, 故 G_i'/G_{i+1}' 也是有限群. 如果对某个 i 有

$$\left|G_i'/G_{i+1}'\right| = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

其中 $k \geqslant 1, p_1, p_2, \cdots, p_k$ 是互不相等的素数,$\sum_{j=1}^{k} a_j > 1$. 令 P_j 是 Abel 群 G_i'/G_{i+1}' 的 Sylow p_j 子群, 则 $|P_j| = p_j^{a_j}$. 由命题 1.8(1)知 P_j 是 G_i'/G_{i+1}' 的正规子群. 由命题 2.11知有内直积分解

$$G_i'/G_{i+1}' = P_1 \otimes P_2 \otimes \cdots \otimes P_k.$$

又设 P_k' 为 P_k 的 $p_k^{a_k-1}$ 阶子群, 则 P_k' 也为 Abel 群 G_i'/G_{i+1}' 的子群, 由命题 1.8(1)知 $P_k' \lhd G_i'/G_{i+1}'$. 由定理 2.30(4)知

$$H' \triangleq P_1 \otimes P_2 \otimes \cdots \otimes P_{k-1} \otimes P_k' \lhd G_i'/G_{i+1}'.$$

再利用Lagrange 定理及定理 2.30(2)可得

$$\begin{aligned} \left|H'\right| &= p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k-1}, \\ \left[G_i'/G_{i+1}' : H'\right] &= \frac{\left|G_i'/G_{i+1}'\right|}{|H'|} = \frac{p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}}{p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k-1}} = p_k. \end{aligned} \tag{2.26}$$

设 π 为 G_i' 到 G_i'/G_{i+1}' 上的自然同态, 令 $H = \pi^{-1}(H')$, 则由 $1 \in H'$ 和推论 1.4(2)知

$$G_{i+1}' = \ker \pi = \pi^{-1}(1) \subseteq \pi^{-1}(H') = H = \pi^{-1}(H') \lhd G_i'.$$

于是由定理 1.39(3)可得

$$G_{i+1}' \lhd H \lhd G_i', \quad G_i'/H \cong \left(G_i'/G_{i+1}'\right)/\pi(H) = \left(G_i'/G_{i+1}'\right)/H'.$$

将 π 限制在 H 上, 则 $\pi|_H$ 是 H 到 H' 的满同态. 再利用定理 1.39(3)可得

$$H/G_{i+1}' \cong \pi(H)/\pi\left(G_{i+1}'\right) = \pi(H)/\{1\} = H'.$$

再结合(2.26)式可得

$$[G_i' : H] = [G_i'/G_{i+1}' : H'] = p_k,$$
$$[H : G_{i+1}'] = |H'| = p_1^{a_1} p_2^{a_2} \cdots p_{k-1}^{a_{k-1}} p_k^{a_k - 1}.$$

故 G_i'/H 是素数阶群,H/G_{i+1}' 仍是 Abel 群. 同理可由 Abel 群 H/G_{i+1}' 得到 H_1, 使得 $G_{i+1}' \lhd H_1 \lhd H$,H/H_1 是素数阶群,H_1/G_{i+1}' 仍是 Abel 群且

$$\left[H_1 : G_{i+1}'\right] = p_1^{a_1} p_2^{a_2} \cdots p_{k-1}^{a_{k-1}} p_k^{a_k - 2}.$$

依次进行下去, 因为 $\left[G_i' : G_{i+1}'\right]$ 的阶有限, 所以这个操作必会在有限步后终止, 最终得到

$$G_{i+1}' \lhd H_m \lhd \cdots \lhd H_2 \lhd H_1 \lhd H, \quad m = \sum_{i=1}^{k} a_i - 2,$$

$H/H_1, H_k/H_{k+1}, k = 1, 2, \cdots m$ 都是素数阶群, 并且 $\left[H_m : G_{i+1}'\right] = p_1$, 故 H_m/G_{i+1}' 也是素数阶群. 根据 i 的任意性, 我们在每个 G_i', G_{i+1}' 之间都可以像这样插入一列群, 最终得到一个新的次正规序列, 并且这个新的次正规序列的因子都是素数阶群.

(4) $\Rightarrow$ (1). 因 $G_{t-1}'', G_{t-2}''/G_{t-1}''$ 都是素数阶群, 故由命题 1.24知 $G_{t-1}'', G_{t-2}''/G_{t-1}''$ 都是循环群, 因而由命题 2.14知它们都可解. 注意到短正合序列

$$1 \longrightarrow G_{t-1}'' \xrightarrow{\lambda} G_{t-2}'' \xrightarrow{\mu} G_{t-2}''/G_{t-1}'' \longrightarrow 1,$$

故 G_{t-2}'' 是循环群 G_{t-2}''/G_{t-1}'' 过可解群 G_{t-1}'' 的扩张, 由定理 2.31知 G_{t-2}'' 是可解群. 假设 G_{i+1}'' 为可解群, 则同理可得 G_i'' 是循环群 G_i''/G_{i+1}'' 过可解群 G_{i+1}'' 的扩张, 故由定理 2.31知 G_i'' 是可解群. 因此由数学归纳法知当 $i = 1$ 时知 G 为可解群.

□

例题 2.11 在 A_4 中有正规序列

$$A_4 \supseteq K_4 \supseteq \{\mathrm{id}\}.$$

A_4/K_4 是 3 阶群,K_4 是 Abel 群, 于是 A_4 是可解群.

证明

□

定理 2.33

(1) 设 G 是幂零群,A 是幂零群 G 的子群, 则 A 也是幂零群.

(2) 设 G 是幂零群,f 是群 G 到群 G_1 的同态, 则 $f(G)$ 也是幂零群.

(3) 设 G 是幂零群 B 过幂零群 A 的扩张, 若 G 是中心扩张或平凡扩张, 则 G 也是幂零群.

♡

证明

(1) 由 G 是幂零群知, 存在 $k_0 \in \mathbb{N}$, 使得 $\Gamma_{k_0}(G) = \{1\}$. 再由命题 2.13(2)知 $\Gamma_{k_0}(A) \subseteq \Gamma_{k_0}(G) = \{1\}$, 故 $\Gamma_{k_0}(A) = \{1\}$. 由此知 A 也为幂零群.

(2) 由 G 是幂零群知, 存在 $k_0 \in \mathbb{N}$, 使得 $\Gamma_{k_0}(G) = \{1\}$. 再由命题 2.13(2)知 $\Gamma_{k_0}(f(G)) = f(\Gamma_{k_0}(G)) = f(\{1\}) = \{1\}$, 故 $\Gamma_{k_0}(f(G)) = \{1\}$. 由此知 G_1 也是幂零群.

(3) 若 G 是中心扩张, 则由条件知 $A \subseteq C(G), G/A = B$, 又设 π 是 G 到 B 上的自然同态. 由 B 幂零知, 存在 $k_1 \in \mathbb{N}$, 使得

$$\pi(\Gamma_{k_1}(G)) = \Gamma_{k_1}(B) = \{1\},$$

因而 $\Gamma_{k_1}(G) \subseteq \ker\pi = A \subseteq C(G)$. 故 $\forall a \in \Gamma_{k_1}(G), b \in G$ 有

$$[a, b] = a^{-1}b^{-1}ab = a^{-1}a = 1.$$

于是 $\Gamma_{k_1+1}(G) = [G, \Gamma_{k_1}(G)] = \{1\}$, 这就证明了 G 是幂零群.

若 G 是平凡扩张, 则由定理 2.29知 $G \cong A \times B$ 且 A, B 都是幂零群. 由命题 2.13(4)知

$$\Gamma_k(G) = \Gamma_k(A) \times \Gamma_k(B), \ \forall k \in \mathbb{N}.$$

又由 A, B 是幂零群知, 存在 $k_1, k_2 \in \mathbb{N}$, 使得 $\Gamma_{k_1}(A) = \Gamma_{k_2}(B) = \{1\}$. 又因为

$$\Gamma_{k_1}(A) \supseteq \Gamma_k(A), \ \forall k \geqslant k_1; \quad \Gamma_{k_2}(B) \supseteq \Gamma_k(B), \ \forall k \geqslant k_2.$$

所以

$$\Gamma_k(A) = \{1\}, \ \forall k \geqslant k_1; \quad \Gamma_k(B) = \{1\}, \ \forall k \geqslant k_2.$$

于是取 $K = \max\{k_1, k_2\}$, 则

$$\Gamma_K(G) = \Gamma_K(A) \times \Gamma_K(B) = \{1\} \times \{1\} = \{1\}.$$

故 G 也为幂零群.

□

定理 2.34

设 G 是群, 则下列条件等价:

(1) G 是一个幂零群;

(2) G 中有正规序列

$$G = G_1 \supseteq G_2 \supseteq \cdots \supseteq G_r = \{1\},$$

使 $G_i/G_{i+1} \subseteq C(G/G_{i+1}), 1 \leqslant i \leqslant r-1$;

(3) 存在 $k \in \mathbb{N}$, 使得 $C_k(G) = G$.

♡

注 由这个定理的证明知: **群 G 是幂零群的充要条件是 G 的降中心列都是正规序列且 $\Gamma_i/\Gamma_{i+1} \subseteq C(G/\Gamma_{i+1})$.**

证明 (1)⇒ (2). 因 G 是幂零群, 故有 $k \in \mathbb{N}$, 使 $\Gamma_k(G) = \{1\}$. 再由命题 2.13(7)知 G 中有正规序列

$$G = \Gamma_1(G) \supseteq \Gamma_2(G) \supseteq \cdots \supseteq \Gamma_k(G) = \{1\},$$

因而由推论 1.4(2)知 $\Gamma_i(G)/\Gamma_{i+1}(G) \subseteq G/\Gamma_{i+1}(G)$. 设 π 为 G 到 $G/\Gamma_{i+1}(G)$ 的自然同态, 由命题 2.13(3)及 $[G, \Gamma_i(G)] = \Gamma_{i+1}(G)$ 知

$$[G/\Gamma_{i+1}(G), \Gamma_i(G)/\Gamma_{i+1}(G)] = [\pi(G), \pi(\Gamma_i(G))] = \pi([G, \Gamma_i(G)]) = \pi(\Gamma_{i+1}(G)) = \{1\},$$

因而由引理 2.2(1)知 $\Gamma_i(G)/\Gamma_{i+1}(G) \subseteq C(G/\Gamma_{i+1}(G))$, 故 G 的降中心列满足条件 (2) 的要求.

(2) ⇒ (3). 用反序归纳法证明 $G_i \subseteq C_{r-i}(G)$, 其中 $C_0(G) = \{1\}$. 当 $i = r$ 时,$G_r = \{1\} = C_0(G) = C_{r-r}(G)$. 设 $i+1$ 时已成立, 因而 $G_{i+1} \subseteq C_{r-(i+1)}(G)$. 又 $G_i/G_{i+1} \subseteq C(G/G_{i+1})$, 由命题 1.8(6)知

$$[G_i, G] \subseteq G_{i+1}.$$

即对 $\forall a \in G_i$, 有

$$[a, b] \in G_{i+1} \subseteq C_{r-(i+1)}(G), \forall b \in G.$$

因而由命题 2.13(6)知 $a \in C_{r-i}(G)$, 故 $G_i \subseteq C_{r-i}(G)$. 特别地, 有 $G_1 = G \subseteq C_{r-1}(G)$, 即取 $k = r-1$ 知条件 (3) 成立.

(3) ⇒ (1). 设有 $k \in \mathbb{N}$, 使 $C_k(G) = G$, 再结合命题 2.13(7)知 G 中有正规序列

$$G = C_k(G) \supseteq C_{k-1}(G) \supseteq \cdots \supseteq C_1(G) \supseteq C_0(G) = \{1\}.$$

用数学归纳法证明 $\Gamma_i(G) \subseteq C_{k-i+1}(G), i = 1, 2, \cdots$. 当 $i = 1$ 时, 显然成立. 假设结论对 i 成立, 现在考虑 $i+1$ 的情形. 由于 $C_{k-i+1}(G)/C_{k-i}(G) = C(G/C_{k-i}(G))$, 故由命题 1.8(6)有 $[G, C_{k-i+1}(G)] \subseteq C_{k-i}(G)$, 于是再结合引理 2.2(4)得

$$\Gamma_{i+1}(G) = [G, \Gamma_i(G)] \subseteq [G, C_{k-i+1}(G)] \subseteq C_{k-i}(G).$$

故由数学归纳法知 $\Gamma_i(G) \subseteq C_{k-i+1}(G), i = 1, 2, \cdots$. 特别地, 有 $\Gamma_{k+1}(G) \subseteq C_0(G) = \{1\}$, 故 $\Gamma_{k+1} = \{1\}$. 因而 G 是幂零群.

□

定理 2.35

设 p 是一个素数, 则有限 p 群都是幂零群.

♡

证明 由命题 2.14知阶数为 p 的有限 p 群都是幂零群. 假设结论对阶数小于等于 p^{n-1} 的有限 p 群都成立, 现设 $|G|=p^n$, 则由定理 2.17(3)知 $C(G)\neq\{1\}$, 从而 $|C(G)|>1$. 若 $|C(G)|=|G|$, 则 G 是 Abel 群, 由命题 2.14知 G 是幂零群. 下设 $|C(G)|=p^k(1\leqslant k<n)$, 则由Lagrange 定理得

$$|G|=[G:C(G)]\cdot|C(G)|\Longleftrightarrow[G:C(G)]=p^{n-k}<p^n.$$

于是由归纳假设知 $G/C(G),C(G)$ 都是幂零群. 又显然 G 是 $G/C(G)$ 过 $C(G)$ 的中心扩张, 故由定理 2.33(3)知 G 为幂零群. 因此由数学归纳法知任何有限 p 群都是幂零群.

□

例题 2.12 设 H 是四元数体,$G=\{\pm1,\pm i,\pm j,\pm k\}$, 其中 $1,i,j,k\in H$ 如命题 1.13所述, 则 G 是 8 阶群. 这是一个非 Abel 幂零群的例子.

证明

□

2.7 Jordan-Hölder 定理

定义 2.28

群 G 的两个次正规 (正规) 序列

$$G=G_1\supseteq G_2\supseteq\cdots\supseteq G_r=\{1\},$$

$$G=H_1\supset H_2\supseteq\cdots\supseteq H_s=\{1\}$$

称为**同构的**, 如果这两个序列的因子集 $\{G_i/G_{i+1}\mid 1\leqslant i\leqslant r-1\},\{H_j/H_{j+1}\mid 1\leqslant j\leqslant s-1\}$ 之间有一一对应关系, 并且对应的因子是同构的.

♣

注 显然, 若两个次正规 (正规) 序列同构, 则它们有相同的长度.

引理 2.3 (Zassenhaus 定理)

设 H,K 是群 G 的子群, 又 H^*,K^* 分别是 H,K 的正规子群, 则

$$H^*(H\cap K^*)\lhd H^*(H\cap K),\quad K^*(H^*\cap K)\lhd K^*(H\cap K),$$

$$H^*(H\cap K)/H^*(H\cap K^*)\cong(H\cap K)/(H\cap K^*)(H^*\cap K)\cong K^*(H\cap K)/K^*(H^*\cap K).$$

$$(H\cap K^*)H^*\lhd(H\cap K)H^*,\quad (H^*\cap K)K^*\lhd(H\cap K)K^*,$$

$$(H\cap K)H^*/(H\cap K^*)H^*\cong(H\cap K)/(H\cap K^*)(H^*\cap K)\cong(H\cap K)K^*/(H^*\cap K)K^*.$$

♡

证明 因为 H^* 是 H 的正规子群, $H\cap K,H\cap K^*$ 都是 H 的子群, 故由定理 1.40(2)知 $H^*(H\cap K),H^*(H\cap K^*)$ 都是 H 的子群. 同样 $K^*(H\cap K),K^*(H^*\cap K)$ 都是 K 的子群, 而且 $H^*(H\cap K^*)\subseteq H^*(H\cap K),K^*(H^*\cap K)\subseteq K^*(H\cap K)$. 对 $\forall a\in H^*\cap K,b\in H\cap K^*,x\in H\cap K$, 有

$$xax^{-1}\in H^*\cap K,\quad xbx^{-1}\in H\cap K^*.$$

故 $H^*\cap K,H\cap K^*\lhd H\cap K$. 再由推论 1.4(2)知 $(H\cap K^*)(H^*\cap K)=L$ 也是 $H\cap K$ 的正规子群.

作 $H^*(H\cap K)$ 到 $(H\cap K)/L$ 上的映射 ϕ,

$$\phi(hx)=xL,\quad \forall h\in H^*,x\in H\cap K.$$

若 $h_1x_1 = h_2x_2(h_i \in H^*, x_i \in H \cap K, i = 1, 2)$, 则

$$h_2^{-1}h_1 = x_2x_1^{-1} \in H^* \cap (H \cap K) = H^* \cap K \subseteq L \Longrightarrow x_2L = x_1L,$$

因而 $\phi(h_1x_1) = \phi(h_2x_2)$, 故 ϕ 是良定义的.

再证明 ϕ 是同态, 由于 $H^* \lhd H, x_1h_2x_1^{-1} \in H^*$, 故

$$\phi((h_1x_1)(h_2x_2)) = \phi(h_1(x_1h_2x_1^{-1})x_1x_2) = x_1x_2L = (x_1L)\cdot(x_2L) = \phi(h_1x_1)\cdot\phi(h_2x_2),$$

故 ϕ 是 $H^*(H \cap K)$ 到 $H \cap K/L$ 上的同态, 显然 ϕ 还是满同态. 注意到

$$hx \in \ker\phi \iff \phi(hx) = xL = L \iff x \in L \iff hx \in H^*L = H^*(H^* \cap K)(H \cap K^*) = H^*(H \cap K^*),$$

故 $\ker\phi = H^*(H \cap K^*)$. 因而由群的同态基本定理得

$$H^*(H \cap K^*) \lhd H^*(H \cap K),$$
$$H^*(H \cap K)/H^*(H \cap K^*) \cong (H \cap K)/(H \cap K^*)(H^* \cap K).$$

同理可得

$$K^*(H^* \cap K) \lhd K^*(H \cap K),$$
$$K^*(H \cap K)/K^*(H^* \cap K) \cong (H \cap K)/(H \cap K^*)(H^* \cap K).$$

故

$$H^*(H \cap K)/H^*(H \cap K^*) \cong (H \cap K)/(H \cap K^*)(H^* \cap K) \cong K^*(H \cap K)/K^*(H^* \cap K).$$

综上, 同理可得

$$(H \cap K^*)H^* \lhd (H \cap K)H^*, \quad (H^* \cap K)K^* \lhd (H \cap K)K^*,$$
$$(H \cap K)H^*/(H \cap K^*)H^* \cong (H \cap K)/(H \cap K^*)(H^* \cap K) \cong (H \cap K)K^*/(H^* \cap K)K^*.$$

□

定理 2.36 (Schreier 定理)

群 G 的两个次正规 (正规) 序列有同构的加细.

♡

证明 设群 G 有次正规 (正规) 序列

$$G = G_1 \supseteq G_2 \supseteq \cdots \supseteq G_r = \{1\}, \tag{2.27}$$
$$G = H_1 \supseteq H_2 \supseteq \cdots \supseteq H_s = \{1\}. \tag{2.28}$$

令

$$G_{i,k} = (G_i \cap H_k)G_{i+1}, \quad 1 \leqslant i \leqslant r-1, 1 \leqslant k \leqslant s,$$
$$G_{r,s} = \{1\},$$
$$H_{i,k} = (H_i \cap G_k)H_{i+1}, \quad 1 \leqslant i \leqslant s-1, 1 \leqslant k \leqslant r,$$
$$H_{s,r} = \{1\}.$$

由 $G_{k+1} \lhd G_k(1 \leqslant k \leqslant r-1), H_{k+1} \lhd H_k(1 \leqslant k \leqslant s-1)$ 及Zassenhaus 定理可得

$$G_{i,k+1} \lhd G_{i,k}, \quad 1 \leqslant i \leqslant r-1, 1 \leqslant k \leqslant s-1,$$
$$H_{i,k+1} \lhd H_{i,k}, \quad 1 \leqslant i \leqslant s-1, 1 \leqslant k \leqslant r-1.$$

从而

$$G_{i+1,1} = (G_{i+1} \cap G)G_{i+2} = G_{i+1} = (G_i \cap H_s)G_{i+1} = G_{i,s} \lhd G_{i,s-1}, \ 1 \leqslant i \leqslant r-1,$$
$$H_{i+1,1} = (H_{i+1} \cap G)H_{i+2} = H_{i+1} = (H_i \cap G_r)H_{i+1} = H_{i,r} \lhd H_{i,r-1}, \ 1 \leqslant i \leqslant s-1.$$

又若序列(2.27), 序列(2.28)都是正规序列, 即 $G_i, H_j(1 \leqslant i \leqslant s, 1 \leqslant j \leqslant r)$ 均为 G 的正规子群, 则由命题 (4)(5)知

$G_{i,k}, H_{j,k}$ 也是 G 的正规子群. 这样, 即得序列(2.27), 序列(2.28)的加细的次正规 (正规) 序列

$$\begin{aligned} G = G_{1,1} &\supseteq G_{1,2} \supseteq \cdots \supseteq G_{1,s-1} \\ &\supseteq G_{2,1} \supseteq G_{2,2} \supseteq \cdots \supseteq G_{2,s-1} \\ &\supseteq \cdots \\ &\supseteq G_{r-1,1} \supseteq G_{r-1,2} \supseteq \cdots \supseteq G_{r-1,s-1} \supseteq G_{r,s} = \{1\}, \end{aligned} \tag{2.29}$$

$$\begin{aligned} G = H_{1,1} &\supseteq H_{1,2} \supseteq \cdots \supseteq H_{1,r-1} \\ &\supseteq H_{2,1} \supseteq H_{2,2} \supseteq \cdots \supseteq H_{2,r-1} \\ &\supseteq \cdots \\ &\supseteq H_{s-1,1} \supseteq H_{s-1,2} \supseteq \cdots \supseteq H_{s-1,r-1} \supseteq H_{s,r} = \{1\}. \end{aligned} \tag{2.30}$$

由Zassenhaus 定理有

$$\frac{G_{i,k}}{G_{i,k+1}} = \frac{(G_i \cap H_k)G_{i+1}}{(G_i \cap H_{k+1})G_{i+1}} \cong \frac{(G_i \cap H_k)H_{k+1}}{(G_{i+1} \cap H_k)H_{k+1}} = \frac{H_{k,i}}{H_{k,i+1}},$$

$$H_{s-1,r-1} = H_{s-1} \cap G_{r-1} = G_{r-1,s-1}$$

故序列(2.29), (2.30)是 G 的同构的次正规 (正规) 序列.

□

定义 2.29

1. 群 G 的次正规序列
$$G = G_1 \supseteq G_2 \supseteq \cdots \supseteq G_r = \{1\}$$
的因子 $G_i/G_{i+1}(1 \leqslant i \leqslant r-1)$ 如果都是单群, 那么称此序列为 G 的**合成序列**.
2. 群 G 的正规序列
$$G = G_1 \supseteq G_2 \supseteq \cdots \supseteq G_r = \{1\}$$
的因子 $G_i/G_{i+1}(1 \leqslant i \leqslant r-1)$ 如果都是单群, 那么称此序列为 G 的**主序列**.

♣

注 显然群 G 的主序列必是合成序列.

命题 2.15

若 $G = G_1 \supseteq G_2 \supseteq \cdots \supseteq G_r = \{1\}$ 为 G 的合成序列, 则 G_{i+1} 是 G_i 的极大正规子群.

♠

证明

□

例题 2.13 设 $G = \langle a \rangle$ 为 15 阶循环群, 则

$$G \supseteq \langle a^3 \rangle \supseteq \{1\},$$
$$G \supseteq \langle a^5 \rangle \supseteq \{1\}$$

是两个同构的正规序列. 并且这两个序列都是 G 的主序列, 也是合成序列.

证明

□

例题 2.14 设 $n \geqslant 5$, 则 $S_n \supseteq A_n \supseteq \{1\}$ 是 S_n 的主序列, 也是 S_n 的合成序列.

例题 2.15 序列 $S_4 \supseteq A_4 \supseteq K_4 \supseteq \langle (12)(34) \rangle \supseteq \{1\}$ 是 S_4 的合成序列, 但不是 S_4 的主序列.

证明

□

例题 2.16 无限循环群 $G = \langle a \rangle$ 无合成序列.

证明 事实上, 若 G 有合成序列

$$G = G_1 \supseteq G_2 \supseteq \cdots \supseteq G_{r-1} \supseteq G_r = \{1\},$$

则 $G_{r-1}/G_r = G_{r-1} = \langle a^k \rangle$ 为单群, 但 $\langle a^k \rangle$ 是无限循环群, 而由命题 2.6知无限循环群非单群, 矛盾!

□

定理 2.37 (Jordan-Hölder 定理)

若群 G 有合成 (主) 序列, 则 G 的任两个合成 (主) 序列是同构的.

♡

注 这个定理表明: **任意群的合成 (主) 序列的因子在同构意义下唯一.**

证明 设 G 有两合成 (主) 序列

$$G = G_1 \supseteq G_2 \supseteq \cdots \supseteq G_r = \{1\}, \tag{2.31}$$

$$G = H_1 \supseteq H_2 \supseteq \cdots \supseteq H_s = \{1\}. \tag{2.32}$$

由于 $G_i/G_{i+1}(1 \leqslant i \leqslant r-1), H_j/H_{j+1}(1 \leqslant i \leqslant s-1)$ 都是单群, 因而序列(2.31)和序列(2.32)都不可能再加细. 否则, 存在 $k_1 \in \{1, 2, \cdots, r\}, k_2 \in \{1, 2, \cdots, s\}$ 以及群 K_1, K_2, 使得

$$G_{k_1+1} \subset K_1 \subset G_{k_1}, \quad H_{k_2+1} \subset K_2 \subset H_{k_2}; \tag{2.33}$$

$$G_{k_1+1} \lhd K_1 \lhd G_{k_1}, \quad H_{k_2+1} \lhd K_2 \lhd H_{k_2}.$$

由推论 1.4(2)知

$$K_1/G_{k_1+1} \lhd G_{k_1}/G_{k_1+1}, \quad K_2/G_{k_2+1} \lhd H_{k_2}/H_{k_2+1}.$$

又因为 $G_{k_1}/G_{k_1+1}, H_{k_2}/H_{k_2+1}$ 都是单群, 所以

$$K_1/G_{k_1+1} = G_{k_1+1}\text{或}G_{k_1}/G_{k_1+1}, \quad K_2/H_{k_2+1} = H_{k_2+1}\text{或}H_{k_2}/H_{k_2+1}.$$

即

$$K_1 = G_{k_1+1}\text{或}G_{k_1}, \quad K_2 = H_{k_2+1}\text{或}H_{k_2}.$$

这与(2.33)式矛盾!

另外, 由Schreier 定理知序列(2.31)和序列(2.32)可加细为同构的次正规 (正规) 序列, 分别记为序列 S 和序列 T, 则序列 S 与序列 T 同构. 而已经证明序列(2.31)和序列(2.32)不可加细, 故序列 S 等于序列(2.31), 序列 T 等于序列(2.32). 因而序列(2.31)和序列(2.32)必然同构.

□

定义 2.30

设 G 是群, Ω 为一集合, 如果有 $\Omega \times G$ 到 G 的映射 $(\sigma, a) \to \sigma(a)(\forall \sigma \in \Omega, a \in G)$ 满足

$$\sigma(ab) = \sigma(a)\sigma(b), \ \forall \sigma \in \Omega, \ a, b \in G,$$

那么称 G 为**带算子集 Ω 的群**, 简称 **Ω 群**. Ω 的元素称为 G 的**算子**.

♣

注 事实上, 由 Ω 群的定义又知 Ω 中每个元素 σ 都是群 G 的自同态.

例题 2.17 设 G 是 Abel 群, 运算为加法, 则 G 是一个 $\mathbb{Z}$ 群.

证明 事实上, $(n, a) \to na(n \in \mathbb{Z}, a \in G)$ 为 $\mathbb{Z} \times G$ 到 G 的映射. 并且

$$n(a+b) = n \cdot (a+b) = na + nb = n(a) + n(b), \ \forall n \in \mathbb{Z}, a, b \in G.$$

□

例题 2.18 设 M 是环 R 上的左模, 则 M 是 R 群. 特别地, 域 F 上的线性空间可看成 F 群.

证明 事实上, $R \times M$ 到 M 的映射为 $(a, x) \to ax(a \in R, \ x \in M)$.

□

定义 2.31

设 G 为 Ω 群, H 是 G 的子群, 且满足

$$\sigma(H) \subseteq H,\ \forall \sigma \in \Omega,$$

则称为 H 为 G 的 **Ω 子群**. 又若 $H \lhd G$, 即 $H \subseteq G$ 且 $H \lhd G$, 则称 H 为 G 的 **Ω 正规子群**.

命题 2.16

左 R 模 M 可看成 R 群, 其 R 子群 M_1 就是 M 的子模, 特别是一个环 R, 即可看成左 R 模, 因而也可看成 R 模. 这时, R 子群为 R 的左理想, 环 R 也可看成右 R 模、R 群, 这时 R 子群为右理想, 环 R 也可看成 R 双模, 相应的 R 子群为 R 的理想.

注 这个命题表明: 环与模都是特殊的 Ω 群.

证明

□

例题 2.19 设 G 是群, 若 $\Omega = \mathrm{Int}G(G$ 的内自同构的集合), 则 G 的 Ω 子群就是 G 的正规子群.

证明

□

定义 2.32

设 G 是群.

1. 若 $\Omega = \mathrm{Aut}G(G$ 的自同构的集合), 则 G 的 Ω 子群称为 G 的**特征子群**;
2. 若 $\Omega = \mathrm{End}G(G$ 的自同态的集合), 则 G 的 Ω 子群称为 G 的**完全不变子群**.

定理 2.38

设 H 是 Ω 群 G 的 Ω 正规子群, π 为 G 到 G/H 的自然同态, 则 $\Omega \times G/H$ 到 G/H 上的映射 $(\sigma, \pi(a)) \to \pi(\sigma(a))(\sigma \in \Omega, \pi(a) \in G/H)$ 使得 G/H 也是 Ω 群, 称为 G 对 H 的 **Ω 商群**.

证明 若 $(\sigma, \pi(a)) = (\sigma', \pi(b)) \in \Omega \times G/H$, 则 $\sigma = \sigma', \pi(a) = \pi(b)(a, b \in G)$, 于是 $ab^{-1} \in H$, 从而有 $\sigma(a)\sigma'(b)^{-1} = \sigma(a)\sigma(b)^{-1} = \sigma(ab^{-1}) \in H$, 故 $\pi(\sigma(a)) = \pi(\sigma'(b))$. 故 $\Omega \times G/H$ 到 G/H 的映射 $(\sigma, \pi(a)) \to \pi(\sigma(a))$ 是良定义的.

又 $\forall a, b \in G, \sigma \in \Omega$ 有

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

于是 G/H 是 Ω 群.

□

定义 2.33

设 G, G_1 都是 Ω 群, ϕ 是群 G 到群 G_1 的同态且满足 $\phi\sigma = \sigma\phi(\forall \sigma \in \Omega)$, 则称 ϕ 是 **Ω 同态**. 若 ϕ 还是群的同构, 则称 ϕ 是 **Ω 同构**.

注 与通常的群的同态基本定理一样, 可证 Ω 群的同态基本定理及其他一些定理, 如 Zassenhaus 引理. 同样, 也可以引入 Ω 群的次正规 (正规) 序列、合成序列和主序列等概念, 并能证明 Schreier 定理与 Jordan-Hölder 定理. 由于环与模均可看成特殊的 Ω 群, 因而就可将 Jordan-Hölder 定理用于环与模的研究.

命题 2.17

若 H 为 Ω 群 G 的 Ω 正规子群, 则 G 到 G/H 的自然同态 π 是 Ω 同态.

证明

□

定义 2.34

R 模 M 的有限子模序列

$$M = M_1 \supseteq M_2 \supseteq \cdots \supseteq M_r = 0$$

满足 $M_i/M_{i+1}(i = 1, 2, \cdots, r-1)$ 为单模, 则该序列称为 M 的一个**合成序列**, M_i/M_{i+1} 称为**合成因子**.

♣

定理 2.39 (模的 Jordan-Hölder 定理)

若 R 模 M 有合成序列, 则 M 的任两合成序列是同构的, 即它们的合成因子在同构意义下唯一.

♡

注 若将 M 看成带算子集 R 的 R 群, 则这个定理就是群的 Jordan-Hölder 定理的特殊情形. 与群的 Jordan-Hölder 定理同样证明.

证明

□

2.8 自由幺半群与自由群

定义 2.35 (自由幺半群)

设 X 是一个非空集合, 称 X 中任一有限长的序列

$$x_1x_2\cdots x_i, \quad x_1, x_2, \cdots, x_i \in X$$

为一个**字**. 当 $i = 0$ 时, 称为**空字**, 记为 $\wedge$. 记所有字的集合为 $\widetilde{X}$. 在 $\widetilde{X}$ 上定义乘法为

$$(x_1x_2\cdots x_i)(y_1y_2\cdots y_j) = x_1x_2\cdots x_iy_1y_2\cdots y_j.$$

显然 $\widetilde{X}$ 对此乘法是以 $\wedge$ 为幺元的幺半群, 称为**由 X 生成的自由幺半群**.

♣

定理 2.40

设集合 X 非空,S 是幺半群,f 是 X 到 S 的映射, 则存在唯一的 $\widetilde{X}$ 到 S 的同态 ϕ, 使

$$\phi(x) = f(x), \quad \forall x \in X.$$

♡

注 由这个定理知任何幺半群均可视为自由半群的同态像.

证明 记 e 为 S 的幺元, 定义 $\widetilde{X}$ 到 S 的映射 ϕ:

$$\phi(\wedge) = e, \quad \phi(x_1x_2\cdots x_i) = f(x_1)f(x_2)\cdots f(x_i), \ \forall x_1x_2\cdots x_i \in \widetilde{X}.$$

则 ϕ 显然为同态且 $\phi(x) = f(x), \forall x \in X$.

若 ψ 为 $\widetilde{X}$ 到 S 的同态且 $\psi(x) = f(x)$, 则对 $\forall x_1x_2\cdots x_i \in \widetilde{X}$, 有

$$\psi(x_1x_2\cdots x_i) = \psi(x_1)\psi(x_2)\cdots\psi(x_i) = f(x_1)f(x_2)\cdots f(x_i) = \phi(x_1x_2\cdots x_i),$$

即 ϕ 唯一.

□

定义 2.36

设非空集合 X, 令非空集合 X' 满足 $X \cap X' = \varnothing$, 并且存在 X 到 X' 上的一一对应 φ, 记 $\varphi(a) = a', \forall a \in X$.

令 $X^* = X \cup X'$, 设 $x \in X^*$, 定义 x',

$$x' = \begin{cases} \varphi^{-1}(x) = a, & x = a' \in X', \\ \varphi(x) = a', & x = a \in X, \end{cases} \tag{2.34}$$

并且记 X^* 生成的自由幺半群为 $\widetilde{X^*}$. 设 $w_1, w_2 \in \widetilde{X^*}$, 若 $\exists g, h \in \widetilde{X^*}, x \in X^*$, 使得

$$\begin{cases} w_1 = gh, \\ w_2 = gxx'h \end{cases} \text{或} \begin{cases} w_1 = gxx'h, \\ w_2 = gh, \end{cases}$$

则称 w_1 与 w_2 是**相邻的**.

♣

定理 2.41

设非空集合 X, 令非空集合 X' 满足 $X \cap X' = \varnothing$, 并且存在 X 到 X' 上的一一对应 φ, 记 $\varphi(a) = a', \forall a \in X$. 再设 $X^* = X \cup X'$,$\widetilde{X^*}$ 为集合 X^* 生成的自由幺半群. 在 $\widetilde{X^*}$ 中定义关系 $\sim$ 如下: $w_1, w_2 \in \widetilde{X^*}$, 称 $w_1 \sim w_2$, 如果存在 $\widetilde{X^*}$ 中序列

$$w_1 = v_1, v_2, \cdots, v_l = w_2$$

满足 v_i 与 v_{i+1} 相邻. 则 “$\sim$” 是 $\widetilde{X^*}$ 中同余关系, 并且 $\widetilde{X^*}$ 对于 $\sim$ 的商幺半群 $\widetilde{X^*}/\sim = F(X)$ 是群, 称 $F(X)$ 为**由 X 生成的自由群**. 用 $\overline{x}$ 表示 x 在 $F(X)$ 中的同余类, 则 $\overline{\wedge}$ 是 $F(X)$ 的幺元. 并且

$$(\overline{x_1 x_2 \cdots x_m})^{-1} = \overline{x'_m x'_{m-1} \cdots x'_1}, \ \forall \overline{x_1 x_2 \cdots x_m} \in F(X).$$

特别地,$(\overline{x})^{-1} = \overline{x'}$, $\forall x \in X$. 因此也记 $x' = x^{-1}$,$X' = X^{-1}$.

♡

注 X' 是根据 X 随便取一个形式逆集合, 只是为了满足群中每个元素都有逆元而引入的符号.

证明 首先证 $\sim$ 是等价关系.

$\forall w \in \widetilde{X^*}$, 取 $v_1 = w = w\wedge$, $v_2 = wa_1a'_1\wedge$, $v_3 = w\wedge = w$. 于是 v_1 与 v_2 相邻,v_2 与 v_3 相邻, 故有 $w \sim w$.

又设 $w_1 \sim w_2$, 即有 $w_1 = v_1, v_2, \cdots, v_l = w_2$ 且 v_i 与 v_{i+1} 相邻. 令 $u_i = v_{l-i+1}$, 则 $u_1 = w_2, u_2, \cdots, u_l = w_1$ 且 u_i 与 u_{i+1} 相邻. 于是 $w_2 \sim w_1$.

再设 $w_1 \sim w_2, w_2 \sim w_3$, 于是存在以下序列:

$$w_1 = v_1, v_2, \cdots, v_l = w_2, \quad v_i \text{与} v_{i+1} \text{相邻},$$
$$w_2 = u_1, u_2, \cdots, u_m = w_3, \quad u_j \text{与} u_{j+1} \text{相邻},$$

因而序列 $w_1 = v_1, v_2, \cdots, v_l = u_1, u_2, \cdots, u_m = w_3$ 的任意相邻两项是相邻的, 故 $w_1 \sim w_3$.

其次证 $\sim$ 为同余关系. 设 $w_1 \sim w_2, u_1 \sim u_2$, 则于是存在以下序列:

$$w_1 = v_1, v_2, \cdots, v_l = w_2, \quad v_i \text{与} v_{i+1} \text{相邻},$$
$$u_1 = u_1, u_2, \cdots, u_m = u_2, \quad u_j \text{与} u_{j+1} \text{相邻}.$$

注意到若 u_1 与 u_2 相邻, 即有 $u_1 = gh, u_2 = gxx'h$, 因而对 $\forall v \in \tilde{X^*}$, 有 $u_1 v = ghv, u_2 v = gxx'hv$, 于是 $u_1 v$ 与 $u_2 v$ 相邻, 同样 vu_1 与 vu_2 相邻. 于是有

$$w_1 u_1 = v_1 u_1, v_2 u_1, \cdots, v_l u_1 = w_2 u_1 \quad v_i u_1 \text{与} v_{i+1} u_1 \text{相邻},$$
$$w_2 u_1 = v_l u_1, v_l u_2, \cdots, v_l u_m = w_2 u_2 \quad v_l u_i \text{与} v_l u_{i+1} \text{相邻}.$$

这说明 $w_1 u_1 \sim w_2 u_1$,$w_2 u_1 \sim w_2 u_2$, 故 $w_1 u_1 \sim w_2 u_2$, 即 $\sim$ 为同余关系.

最后, 由定理**??**知 $F(X) = \widetilde{X^*}/\sim$ 是商幺半群. 再证明商幺半群 $F(X) = \widetilde{X^*}/\sim$ 是群, 只需证明 $F(X)$ 中任一元素可逆. 对 $\forall x \in \widetilde{X^*}$,$\wedge$ 为空字,x' 如式(2.34), 则有 $\wedge xx'\wedge = xx', \wedge = \wedge\wedge$, 即 xx' 与 $\wedge$ 相邻, 因而

$$\wedge \sim xx', \ \forall x \in \widetilde{X^*}. \tag{2.35}$$

用 $\overline{x}$ 表示 x 在 $F(X)$ 中的同余类, 则 $\overline{\wedge}$ 是 $F(X)$ 的幺元. 对任意 $\overline{x_1 x_2 \cdots x_m} \in F(X)$, 有 $x_1 x_2 \cdots x_m \in \widetilde{X^*}$, 从而

$x'_m x'_{m-1}\cdots x'_1 \in \widetilde{X^*}$, 再结合 “$\sim$” 是同余关系和(2.35)式可得

$$\begin{aligned}(x_1x_2\cdots x_m)(x'_m x'_{m-1}\cdots x'_1) &= x_1x_2\cdots x_m x'_m\cdots x'_1 \sim x_1x_2\cdots x_{m-1}\wedge x'_{m-1}\cdots x'_1\\ &= x_1x_2\cdots x_{m-1}x'_{m-1}\cdots x'_1 \sim \cdots \sim x_1\wedge x'_1 = x_1x'_1 \sim \wedge.\end{aligned}$$

于是

$$\begin{aligned}&\left(\overline{x_1x_2\cdots x_m}\right)\left(\overline{x'_m x'_{m-1}\cdots x'_1}\right) = \overline{(x_1x_2\cdots x_m)\left(x'_m x'_{m-1}\cdots x'_1\right)}\\ &= \left\{x\in\widetilde{X^*}\mid x\sim (x_1x_2\cdots x_m)\left(x'_m x'_{m-1}\cdots x'_1\right)\right\}\\ &= \left\{x\in\widetilde{X^*}\mid x\sim\wedge\right\} = \overline{\wedge}.\end{aligned}$$

故 $\overline{x'_m x'_{m-1}\cdots x'_1}$ 就是 $\overline{x_1x_2\cdots x_m}$ 的逆. 这就证明了 $F(X)$ 中元素均可逆, 故为群.

□

命题 2.18

设 $X=\{a\}$, 则 $F(X)$ 为无限循环群. ♠

证明

□

定理 2.42

设非空集合 X, 令非空集合 X' 满足 $X\cap X'=\varnothing$, 并且存在 X 到 X' 上的一一对应 φ, 记 $\varphi(a)=a', \forall a\in X$. 再设 $X^*=X\cup X', \widetilde{X^*}$ 为集合 X^* 生成的自由幺半群. 在 $\widetilde{X^*}$ 中定义关系 $\sim$ 如下: $w_1,w_2\in\widetilde{X^*}$, 称 $w_1\sim w_2$, 如果存在 $\widetilde{X^*}$ 中序列

$$w_1=v_1,v_2,\cdots,v_l=w_2$$

满足 v_i 与 v_{i+1} 相邻. 又 f 是 X 到 G 的映射, 则存在唯一的自由群 $F(X)$ 到群 G 的同态 ψ, 使得

$$\psi(\overline{x})=f(x)(\forall x\in X),$$

其中 $\overline{x}$ 表示 x 在 $F(X)=\widetilde{X^*}/\sim$ 中的同余类. ♡

证明 首先将 f 扩充为 X^* 到 G 的映射, 仍以 f 表示, 满足 $f(x')=f(x)^{-1}(\forall x'\in X')$.

由定理 2.40知有唯一的幺半群 $\widetilde{X^*}$ 到 G 的同态 ϕ, 使得 $\phi(x)=f(x)(\forall x\in X^*)$. 若 $\widetilde{X^*}$ 中元素 w_1 与 w_2 相邻, 不妨设

$$w_1=gh,\ w_2=gxx'h,\quad g,h\in\widetilde{X^*},\ x,x'\in X^*.$$

其中 x' 的定义如式(2.34), 则有

$$\phi(w_2)=\phi(g)\phi(x)\phi(x')\phi(h)=\phi(g)f(x)f(x)^{-1}\phi(h)=\phi(g)\phi(h)=\phi(w_1),$$

即对 $\forall w_1,w_2\in\widetilde{X^*}$, 都有

$$w_1\sim w_2\Longrightarrow\phi(w_1)=\phi(w_2). \tag{2.36}$$

定义 $F(X)$ 到 G 的映射 ψ, 满足

$$\psi(\overline{w})=\phi(w),\forall\,\overline{w}\in F(X).$$

若 $\overline{w_1}=\overline{w_2}$, 则 $w_1\sim w_2$, 由(2.36)式知

$$\psi\left(\overline{w_1}\right)=\phi\left(w_1\right)=\phi\left(w_2\right)=\psi\left(\overline{w_2}\right).$$

故 ψ 是良定义的. 对 $\overline{w_1},\overline{w_2}\in F(x)$, 有

$$\psi\left(\overline{w_1}\,\overline{w_2}\right)=\psi\left(\overline{w_1w_2}\right)=\phi\left(w_1w_2\right)=\phi\left(w_1\right)\phi\left(w_2\right)=\psi\left(\overline{w_1}\right)\psi\left(\overline{w_2}\right).$$

故 ψ 为同态. 显然 $\psi(\overline{x})=\phi(x)=f(x)(\forall x\in X)$.

最后证明 ψ 的唯一性. 若 ψ' 为 $F(X)$ 到 G 的同态且 $\psi(\overline{x})=f(x)(\forall x\in X)$, 则对 $\forall x\in X$, 有

$$\psi'(\overline{x})=f(x)=\psi(\overline{x}).$$

对 $\forall x'\in X'$, 由定理 2.41知 $(\overline{x})^{-1}=\overline{x'}$. 从而

$$\psi'\left(\overline{x'}\right)=\psi'\left((\overline{x})^{-1}\right)=\psi'(\overline{x})^{-1}=f(x)^{-1}=f\left(x'\right)=\psi\left(\overline{x'}\right).$$

因此

$$\psi'(\overline{x})=\psi(\overline{x}),\quad \forall x\in X\cup X'=X^{*}.$$

对 $\forall\overline{x_1x_2\cdots x_m}\in F(X)$, 则 $x_1,x_2,\cdots,x_m\in X^{*}$. 于是

$$\begin{aligned}\psi'(\overline{x_1x_2\cdots x_m})&=\psi'(\overline{x_1x_2}\cdots\overline{x_m})=\psi'(\overline{x_1})\psi'(\overline{x_2})\cdots\psi'(\overline{x_m})\\&=\psi(\overline{x_1})\psi(\overline{x_2})\cdots\psi(\overline{x_m})=\psi(\overline{x_1x_2}\cdots\overline{x_m})=\psi(\overline{x_1x_2\cdots x_m}).\end{aligned}$$

因此 ψ 唯一.

□

推论 2.5

设非空集合 $X=\{a_1,a_2,\cdots,a_n\}$, 则 $\alpha:x\longrightarrow\overline{x}$, $\forall x\in X$ 是 X 到 $F(X)$ 中的单射.

♡

注 由这个推论知, 当 X 为非空有限集时,$X\cong\alpha(X)\subseteq F(X)$, 从而 X 可视为 $F(X)$ 的子集, 此时,定理 2.42中 ψ 的条件可改为

$$\psi(x)=f(x),\quad \forall x\in X.$$

证明 在 $\mathbb{Z}^n=\{(m_1,m_2,\cdots,m_n)\mid m_i\in\mathbb{Z},1\leqslant i\leqslant n\}$ 中定义加法运算为

$$(m_1,m_2,\cdots,m_n)+(l_1,l_2,\cdots,l_n)=(m_1+l_1,m_2+l_2,\cdots,m_n+l_n),$$

则 $\mathbb{Z}^n$ 是交换群, 而 X 到 $\mathbb{Z}^n$ 中映射

$$f:a_i\longrightarrow(m_1,m_2,\cdots,m_n),\quad m_j=\delta_{ij}=\begin{cases}1, & i=j\\ 0, & i\neq j\end{cases},\ 1\leqslant i,j\leqslant n$$

是单射. 如图 2.3所示, 由定理 2.42知有 $F(X)$ 到 $\mathbb{Z}^n$ 的同态 ψ, 使得

$$\psi(\overline{x})=f(x),\quad \forall x\in X,$$

即有 $\psi\alpha=f$. 若 $\alpha(a_i)=\alpha\left(a_j\right)\left(a_i,a_j\in X\right)$, 即 $\overline{a_i}=\overline{a_j}$, 则两边同时作用 ψ 得

$$f(a_i)=\psi(\overline{a_i})=\psi\left(\overline{a_j}\right)=f\left(a_j\right).$$

因为 f 是单射, 所以 $a_i=a_j$. 故 α 也是单射.

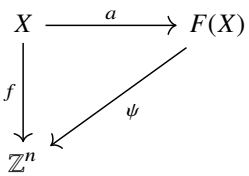

图 2.3

□

推论 2.6

设是有限生成群 $G=\langle g_1,g_2,\cdots,g_n\rangle$, 非空集合 $X=\{a_1,a_2,\cdots,a_n\}$,$F(X)$ 是集合 X 的自由群. 定义 X 到 G

的映射 f,

$$f(a_i)=g_i,\quad 1\leqslant i\leqslant n.$$

由定理 2.42和推论 2.5知, 存在 $F(X)$ 到 G 的满同态 ψ 满足

$$\psi(\overline{a_i})=\psi(a_i)=f(a_i)=g_i,\quad 1\leqslant i\leqslant n,$$

则

$$G\cong F(X)/\ker\psi.$$

称 $\ker\psi$ 为 G 的生成元 $g_1,g_2,\cdots,g_n$ 间的**关系集**. 若 $\ker\psi$ 也是由有限个元素 $w_1,w_2,\cdots,w_r$ 生成, 即 $\ker\psi=\langle w_1,w_2,\cdots,w_r\rangle$, 则称 G 是**可有限表现的**, 而且

$$\psi(w_i)=e,\quad 1\leqslant i\leqslant r.$$

称 $w_1,w_2,\cdots,w_r$ 为 G 的生成元 $g_1,g_2,\cdots,g_n$ 的一组**生成关系**.

♡

证明 由定理 2.1知

$$\langle G\rangle=\left\{x_1x_2\cdots x_m\mid x_i\in G\cup G^{-1},1\leqslant i\leqslant m,m\in\mathbb{N}\right\}.$$

于是对 $\forall\overline{a_1a_2\cdots a_m}\in F(X)(1\leqslant m\leqslant n)$, 有

$$\psi\left(\overline{a_1a_2\cdots a_m}\right)=\psi\left(\overline{a_1a_2}\cdots\overline{a_m}\right)=\psi\left(\overline{a_1}\right)\psi\left(\overline{a_2}\right)\cdots\psi\left(\overline{a_m}\right)=g_1g_2\cdots g_m\in\langle G\rangle.$$

因此 $\psi(F(X))\subseteq\langle G\rangle$. 对 $\forall x_1x_2\cdots x_m\in\langle G\rangle(1\leqslant m\leqslant n)$, 不妨设

$$x_1x_2\cdots x_m=\left(g_{i_1}g_{i_2}\cdots g_{i_k}\right)\left(g_{i_{k+1}}^{-1}g_{i_{k+2}}^{-1}\cdots g_{i_m}^{-1}\right),\quad i_1,i_2,\cdots,i_m\in\{1,2,\cdots,m\}.$$

从而

$$\begin{aligned}x_1x_2\cdots x_m&=\left(g_{i_1}g_{i_2}\cdots g_{i_k}\right)\left(g_{i_{k+1}}^{-1}g_{i_{k+2}}^{-1}\cdots g_{i_m}^{-1}\right)\\&=\left(\psi\left(\overline{a_{i_1}}\right)\psi\left(\overline{a_{i_2}}\right)\cdots\psi\left(\overline{a_{i_k}}\right)\right)\left(\psi\left(\overline{a_{i_{k+1}}}\right)^{-1}\psi\left(\overline{a_{i_{k+2}}}\right)^{-1}\cdots\psi\left(\overline{a_{i_m}}\right)^{-1}\right)\\&=\psi\left(\overline{a_{i_1}a_{i_2}\cdots a_{i_k}}\right)\left(\psi\left(\left(\overline{a_{i_{k+1}}}\right)^{-1}\right)\psi\left(\left(\overline{a_{i_{k+2}}}\right)^{-1}\right)\cdots\psi\left(\left(\overline{a_{i_m}}\right)^{-1}\right)\right)\\&=\psi\left(\overline{a_{i_1}a_{i_2}\cdots a_{i_k}}\right)\left(\psi\left(\overline{a'_{i_{k+1}}}\right)\psi\left(\overline{a'_{i_{k+2}}}\right)\cdots\psi\left(\overline{a_{i_m}}'\right)\right)\\&=\psi\left(\overline{a_{i_1}a_{i_2}\cdots a_{i_k}}\right)\psi\left(\overline{a'_{i_{k+1}}a'_{i_{k+2}}\cdots a'_{i_m}}\right)\\&=\psi\left(\overline{a_{i_1}a_{i_2}\cdots a_{i_k}a'_{i_{k+1}}a'_{i_{k+2}}\cdots a'_{i_m}}\right)\in\psi(F(X)).\end{aligned}$$

因此 $\psi(F(X))\supseteq\langle G\rangle$. 故 $\psi(F(X))=\langle G\rangle$, 即 ψ 是 $F(X)$ 到 G 的满同态. 故由群的同态基本定理知 $G\cong F(X)/\ker\psi$.

□

命题 2.19

设 D_n 是保持正 n 边形不动的转动与反射 (也叫对称) 生成的群, 通常称为**二面体群**. 以正 n 边形的中心为原点, 并设 x 轴的正方向通过一个顶点. 设 a 是转动 $\dfrac{2\pi}{n}$, 而 b 是对 x 轴的反射. 容易看出 D_n 由 a 与 b 生成, 即 $D_n=\langle a,b\rangle$.

令 $X=\{x_1,x_2\}$, 于是由推论 2.6知有 $F(X)$ 到 D_n 的满同态 ψ, 使 $\psi(x_1)=a,\psi(x_2)=b$. 则 $x_1^n,x_2^2,x_1x_2x_1x_2$ 就是 D_n 的生成元 a,b 的一组生成关系.

♠

证明 不难发现 D_n 中只有 n 个不同的转动和 n 个不同的反射对称, 即

$$\mathrm{id},a,\cdots,a^{n-1};\quad b,ab,\cdots,a^{n-1}b.$$

故 $|D_n|=2n$ 且有

$$a^n=\mathrm{id},\quad b^2=\mathrm{id},\quad abab=\mathrm{id}.$$

由上式知

$$\psi\left(x_1^n\right)=a^n=\mathrm{id},\quad \psi\left(x_2^2\right)=b^2=\mathrm{id},\quad \psi\left(x_1x_2x_1x_2\right)=abab=\mathrm{id}.$$

故 $x_1^n,x_2^2,x_1x_2x_1x_2\in\ker\psi$. 由推论 2.5知可将 X 视为 $F(X)$ 的子集, 于是由 $x_1^n,x_2^2,x_1x_2x_1x_2$ 生成的 $F(X)$ 的子群 K 在 $\ker\psi$ 中, 故 $|K|\leqslant|\ker\psi|$.

对 $\forall x\in X^*$, 用 $\widetilde{x}$表示x在$F(X)$ 中的同余类. 对 $\forall\widetilde{x_{k_1}^{\varepsilon_1}x_{k_2}^{\varepsilon_2}\cdots x_{k_m}^{\varepsilon_m}}\in F(X)\left(k_i\in\{1,2\},\varepsilon_i\in\{-1,1\},1\leqslant i\leqslant m\right)$, 有

$$\begin{aligned}\left(\widetilde{x_{k_1}^{\varepsilon_1}x_{k_2}^{\varepsilon_2}\cdots x_{k_m}^{\varepsilon_m}}\right)x_1^n\left(\widetilde{x_{k_1}^{\varepsilon_1}x_{k_2}^{\varepsilon_2}\cdots x_{k_m}^{\varepsilon_m}}\right)^{-1}&=\left(\widetilde{x_{k_1}^{\varepsilon_1}x_{k_2}^{\varepsilon_2}\cdots x_{k_m}^{\varepsilon_m}}\right)\widetilde{x_1^n}\left(\widetilde{x_{k_m}^{-\varepsilon_m}x_{k_{m-1}}^{-\varepsilon_{m-1}}\cdots x_{k_1}^{-\varepsilon_1}}\right)\\&=\widetilde{x_{k_1}^{\varepsilon_1}}\widetilde{x_{k_2}^{\varepsilon_2}}\cdots\widetilde{x_{k_m}^{\varepsilon_m}}\widetilde{x_1^n}\widetilde{x_{k_m}^{-\varepsilon_m}}\widetilde{x_{k_{m-1}}^{-\varepsilon_{m-1}}}\cdots\widetilde{x_{k_1}^{-\varepsilon_1}}\in F(X),\\\left(\widetilde{x_{k_1}^{\varepsilon_1}x_{k_2}^{\varepsilon_2}\cdots x_{k_m}^{\varepsilon_m}}\right)x_2^2\left(\widetilde{x_{k_1}^{\varepsilon_1}x_{k_2}^{\varepsilon_2}\cdots x_{k_m}^{\varepsilon_m}}\right)^{-1}&=\left(\widetilde{x_{k_1}^{\varepsilon_1}x_{k_2}^{\varepsilon_2}\cdots x_{k_m}^{\varepsilon_m}}\right)\widetilde{x_2^2}\left(\widetilde{x_{k_m}^{-\varepsilon_m}x_{k_{m-1}}^{-\varepsilon_{m-1}}\cdots x_{k_1}^{-\varepsilon_1}}\right)\\&=\widetilde{x_{k_1}^{\varepsilon_1}}\widetilde{x_{k_2}^{\varepsilon_2}}\cdots\widetilde{x_{k_m}^{\varepsilon_m}}\widetilde{x_2^2}\widetilde{x_{k_m}^{-\varepsilon_m}}\widetilde{x_{k_{m-1}}^{-\varepsilon_{m-1}}}\cdots\widetilde{x_{k_1}^{-\varepsilon_1}}\in F(X),\\\left(\widetilde{x_{k_1}^{\varepsilon_1}x_{k_2}^{\varepsilon_2}\cdots x_{k_m}^{\varepsilon_m}}\right)(x_1x_2x_1x_2)\left(\widetilde{x_{k_1}^{\varepsilon_1}x_{k_2}^{\varepsilon_2}\cdots x_{k_m}^{\varepsilon_m}}\right)^{-1}&=\left(\widetilde{x_{k_1}^{\varepsilon_1}x_{k_2}^{\varepsilon_2}\cdots x_{k_m}^{\varepsilon_m}}\right)\left(\widetilde{x_1x_2x_1x_2}\right)\left(\widetilde{x_{k_m}^{-\varepsilon_m}x_{k_{m-1}}^{-\varepsilon_{m-1}}\cdots x_{k_1}^{-\varepsilon_1}}\right)\\&=\widetilde{x_{k_1}^{\varepsilon_1}}\widetilde{x_{k_2}^{\varepsilon_2}}\cdots\widetilde{x_{k_m}^{\varepsilon_m}}\widetilde{x_1}\widetilde{x_2}\widetilde{x_1}\widetilde{x_2}\widetilde{x_{k_m}^{-\varepsilon_m}}\widetilde{x_{k_{m-1}}^{-\varepsilon_{m-1}}}\cdots\widetilde{x_{k_1}^{-\varepsilon_1}}\in F(X).\end{aligned}$$

因而 K 是 $F(X)$ 的正规子群.

又 $F(X)/\ker\psi$ 与 D_n 同构, 从而 $[F(X):\ker\psi]=|D_n|=2n$. 因而只需证明 $[F(X):K]\leqslant|D_n|=2n$, 则由推论 1.1可得

$$[F(X):K]=\frac{|F(X)|}{|K|}\leqslant 2n\Longrightarrow|K|\geqslant\frac{|F(X)|}{2n}=\frac{|F(X)|}{[F(X):\ker\psi]}=\frac{|F(X)|}{|F(X)|}\cdot|\ker\psi|=|\ker\psi|.$$

因此 $|K|=|\ker\psi|$, 故 $\ker\psi=K$, 即 $x_1^n,x_2^2,x_1x_2x_1x_2$ 就是 D_n 的生成元 a,b 的一组生成关系.

注意到

$$F(X)=\left\{\widetilde{y_1y_2\cdots y_m}\mid y_i\in X^*=\left\{x_1,x_2,x_1^{-1},x_2^{-1}\right\},1\leqslant i\leqslant m,m\in\mathbb{N}\right\},$$

故 $\overline{x_1}=x_1K,\overline{x_2}=x_2K$ 为 $F(X)/K$ 的生成元, 即 $F(X)/K=\langle\overline{x_1},\overline{x_2}\rangle$. 由 $x_1^n,x_2^2,x_1x_2x_1x_2\in K$ 有

$$\overline{x_1^n}=\overline{x_2^2}=\overline{x_1x_2x_1x_2}=\overline{e},$$

故

$$\overline{x_1x_2x_1x_2}=\overline{e}\Longrightarrow\overline{x_1^{-1}}\left(\overline{x_1x_2x_1x_2}\right)\overline{x_2}=\overline{x_1^{-1}}\overline{x_2}\Longleftrightarrow\overline{x_2x_1}=\overline{x_1^{-1}}\overline{x_2}.$$

假设 $\overline{x_2}\overline{x_1^k}=\overline{x_1^{-k}}\overline{x_2}$, 则

$$\overline{x_2}\overline{x_1^{k+1}}=\left(\overline{x_2}\overline{x_1^k}\right)\overline{x_1}=\left(\overline{x_1^{-k}}\overline{x_2}\right)\overline{x_1}=\overline{x_1^{-k}}\left(\overline{x_2x_1}\right)=\overline{x_1^{-k}}\left(\overline{x_1^{-1}}\overline{x_2}\right)=\overline{x_1^{-(k+1)}}\overline{x_2}.$$

故由数学归纳法知

$$\overline{x_2}\overline{x_1^k}=\overline{x_1^{-k}}\overline{x_2},\quad 1\leqslant k\leqslant n.$$

再结合 $\left(\overline{x_2^2}\right)=\overline{x_2}$ 可得

$$\overline{x_1^k}\overline{x_2}=\overline{x_2}\overline{x_1^{-k}},\quad 1\leqslant k\leqslant n.\tag{2.37}$$

令 $G_1=\{\overline{x_1^k},\overline{x_1^k}\overline{x_2}\mid 1\leqslant k\leqslant n\}$, 则对 $\forall k,l\in\{1,2,\cdots,n\}$, 由 $\overline{x_1^n}=\overline{e}$ 知

$$\overline{x_1^{k+l}}=\begin{cases}\overline{x_1^{k+l-n}}\in G_1, & n<k+l\leqslant 2n,\\ \overline{x_1^{k+l}}\in G_1, & 1\leqslant k+l\leqslant n.\end{cases}$$

于是再利用(2.37)式可得

(i) $\overline{x_1^k}\cdot\overline{x_1^{-l}}=\overline{x_1^{k-l}}\in G_1$;

(ii) $\left(\overline{x_1^k}\overline{x_2}\right)\cdot\left(\overline{x_1^l}\overline{x_2}\right)^{-1}=\left(\overline{x_1^k}\overline{x_2}\right)\cdot\left(\overline{x_2^{-1}}\overline{x_1^{-l}}\right)=\left(\overline{x_1^k}\overline{x_2}\right)\cdot\left(\overline{x_2}\overline{x_1^{-l}}\right)=\overline{x_1^{k-l}}\in G_1$;

(iii) $\left(\overline{x_1^l}\overline{x_2}\right)\cdot\overline{x_1^{-k}}\overset{(2.37)式}{=\!=}\left(\overline{x_2}\overline{x_1^{-l}}\right)\cdot\overline{x_1^{-k}}=\overline{x_2}\overline{x_1^{-k-l}}\overset{(2.37)式}{=\!=}\overline{x_1^{k+l}}\overline{x_2}\in G_1$;

(iv) $\overline{x_1^k}\cdot\left(\overline{x_1^l}\overline{x_2}\right)^{-1}=\overline{x_1^k}\cdot\left(\overline{x_2^{-1}x_1^{-l}}\right)=\overline{x_1^k}\cdot\left(\overline{x_2}\overline{x_1^{-l}}\right)\overset{(2.37)式}{=\!=\!=}\overline{x_1^k}\cdot\left(\overline{x_1^l}\overline{x_2}\right)=\overline{x_1^{k+l}}\overline{x_2}\in G_1$.

因而由定理 1.6(4)知 $F(X)/K=\langle\overline{x_1},\overline{x_2}\rangle\subseteq G_1$. 故 $G_1=\{\overline{x_1^k},\overline{x_1^k}\overline{x_2}\mid 1\leqslant k\leqslant n\}$ 为 $F(X)/K$ 的子群, 显然 $|G_1|\leqslant 2n$. 但由 $\overline{x_1},\overline{x_2}\in G_1$ 知 $G_1=F(X)/K$, 因而 $[F(X):K]\leqslant 2n$.

□

2.9 点群

定义 2.37

以 $O(3)$ 表示三维 Euclid 空间的正交变换群.

而以 $SO(3)$ 表示三维 Euclid 空间的特殊正交变换群, 即行列式为 1 的正交变换构成的群.

♣

注 显然 $SO(3)$ 中元素都是绕原点的转动, 而 $O(3)$ 除转动外, 还有镜面反射.

命题 2.20

$SO(3)\lhd O(3),\quad [O(3):SO(3)]=2.$

♠

证明 由线性代数理论易知.

□

定义 2.38

$O(3)$ 的有限子群 G 称为**点群**.

如果点群 G 满足 $G\subseteq SO(3)$, 则称为**第一类点群**, 否则称为**第二类点群**.

♣

定理 2.43

设 G 是一个第二类点群. 令 $I=-I_3$, 其中 I_3 为三阶单位阵, 则有以下结果:

(1) $G\cap SO(3)=K$ 是 G 的正规子群且 $[G:K]=2$;

(2) 若 $I\in G$, 则有 G 内直积分解 $G=K\otimes\langle I\rangle$;

(3) 若 $I\notin G$, 令 $K^+=\{Ig\mid g\in G\setminus K\}$, 则 $G^+=K\cup K^+$ 是第一类点群且 $G\cong G^+$.

♡

证明

(1) 由命题 2.20知 $SO(3)\lhd O(3)$, 故 $\forall g\in K,h\in G$ 有 $hgh^{-1}\in SO(3)$, 即有

$$hgh^{-1}\in G\cap SO(3)=K.$$

这说明 $K\lhd G$, 又 $g_1,g_2\in G\setminus K$, 则由

$$\det(g_1g_2^{-1})=\det(g_1)\det(g_2^{-1})=(-1)\cdot(-1)=1\Longrightarrow g_1g_2^{-1}\in K$$

知 $g_1K=g_2K$, 因此任取 $g'\in G\setminus K$, 则 $g'K=g''K,\forall g''\in G\setminus K$. 而 $gK=K,\forall g\in K$.

$$G/K=\{gK\mid g\in G=K\cup(G\setminus K)\}=\{K,g'K\}.$$

故 $[G:K]=2$.

(2) 若 $I\in G$, 则对 $\forall A\in G\setminus K$, 有 $\det A=-1$, 从而 $\det(IA)=1$ 且 $IA\in G$, 故 $IA\in K$, 因此存在 $A'\in K$, 使得

$$IA=A'\Longrightarrow A=IA'\in IK.$$

故 $G\setminus K\subseteq IK$. 对 $\forall IB\in IK$, 有 $\det(IB)=-1$, 故 $IB\notin K$, 但 $IB\in G$, 故 $IB\in G\setminus K$, 因此 $IK\subseteq G\setminus K$. 综上 $IK=G\setminus K$. 于是

$$G=K\cup(G\backslash K)=K\cup IK=(-IK)\cup(IK)=\{-Ik,Ik\mid k\in K\}=K\{I,-I\}.$$

又 $\langle I\rangle=\{I,-I\}$ 为二阶群且 $K\cap\langle I\rangle=\{-I\}$. 由 $(\pm I)g=g(\pm I)(\forall g\in G)$ 知 $\langle I\rangle\lhd G$. 故

$$G=K\otimes\langle I\rangle.$$

(3) 若 $I\notin G$, 由于 $g\in G\setminus K$, 故 $Ig\in SO(3)$, 即

$$G^+=K\cup K^+\subseteq SO(3).$$

令

$$\varepsilon(g)=\frac{1}{2}(1-\det g)=\begin{cases}0, & g\in K,\\ 1, & g\in G\setminus K.\end{cases}$$

再作 G 到 G^+ 的映射 σ 如下:

$$\sigma(g)=I^{\varepsilon(g)}g,\ g\in G.$$

显然 σ 是 G 到 G^+ 上的双射, 而且对 $\forall g_1,g_2\in G$, 注意到 $I^2=I^0$, 故

$$\varepsilon(g_1)+\varepsilon(g_2)=1-\frac{\det g_1+\det g_2}{2}=\begin{cases}0, & g_1g_2\in K,\\ 1, & g_1g_2\in G\setminus K\end{cases}=\varepsilon(g_1g_2).$$

从而

$$\begin{aligned}\sigma(g_1)\sigma(g_2)&=I^{\varepsilon(g_1)}g_1I^{\varepsilon(g_2)}g_2=I^{\varepsilon(g_1)+\varepsilon(g_2)}g_1g_2\\&=I^{\varepsilon(g_1g_2)}g_1g_2=\sigma(g_1g_2)\in G^+,\end{aligned}$$

即 σ 保持乘法且 G^+ 对乘法封闭. 又因为

$$\sigma(g_1)^{-1}=\left(I^{\varepsilon(g_1)}g_1\right)^{-1}=I^{\varepsilon(g_1)}g_1^{-1}=\sigma\left(g_1^{-1}\right)\in G^+.$$

所以 G^+ 对逆元封闭. 因此 G^+ 为群. 故 σ 是 G 到 G^+ 上的群同构, 即 $G\cong G^+$.

□

定义 2.39

三维 Euclid 空间可视为 $\mathbf{R}^3$, $x=(x_1,x_2,x_3)\in\mathbf{R}^3$, x 的长度为

$$|x|=\sqrt{x_1^2+x_2^2+x_3^2}.$$

设 $r\in\mathbf{R}$ 且 $r>0$, 则 $S_r=\{x\in\mathbf{R}^3\mid|x|=r\}$ 为半径为 r 的球面.

♣

注 显然 $\forall g\in O(3),x\in S_r$ 有 $gx\in S_r$.

定义 2.40

设 G 为第一类点群, 若 $x\in S_r$ 有 $g\in G,g\neq\mathrm{id}$, 使得

$$gx=x,$$

称 x 为 g 的**极点**, 也称为 G 的**极点**.

♣

引理 2.4

设 P 是第一类点群 G 的所有极点的集合, 则有以下结果:

(1) P 是有限集, $g\in G,g\neq\mathrm{id}$, g 有且仅有两个极点;

(2) $\forall g\in G,x\in P$ 有 $gx\in P$, 即 G 把极点映为极点.

♡

证明

(1) 若 x 为 g 的极点, 即 $gx=x$. 于是 $-x\in S_r,g(-x)=-x$. 因此,$-x$ 亦为 g 的极点. 此时 $x,-x$ 是 g 的转动轴与 S_r 的交点, 因而对 $\forall g\in G,g\neq\mathrm{id}$,$g$ 有且仅有两点极点, 故 P 是有限集.

(2) 设 x 是 g_1 的极点, $g \in G$, 由

$$(gg_1g^{-1})(gx) = gx$$

知 gx 是 gg_1g^{-1} 的极点.

□

推论 2.7

由引理 2.4(2)知 G 把极点映为极点, 故可视 G 作用于极点集 P 上, 因而由定理 2.7(2)知 P 在 G 作用下分成一些 G 的轨道,

$$P = P_1 \cup P_2 \cup \cdots \cup P_k,\ i \neq j,\ P_i \cap P_j = \varnothing.$$

设 x 是一个极点,$G_x = \{g \in G \mid gx = x\}$ 是 x 的迷向子群, 则 $|G_x| \geqslant 2$, 并且

$$G_{gx} = gG_xg^{-1},\ g \in G.$$

若 $x \in P_i$,$P_i = \{gx \mid g \in G\}$, 则由推论 2.3知 $|P_i| = [G : G_x]$.

♡

证明 由极点定义知, 必存在 $g_x \in G \setminus \{\mathrm{id}\}$, 使 $g_xx = x$. 从而 $G_x \supseteq \{\mathrm{id}, g_x\}$, 故 $|G_x| \geqslant 2$.

又由定理 2.10**??**知

$$G_{gx} = gG_xg^{-1},\ g \in G.$$

□

定理 2.44

第一类点群 G 的极点集 P 只能分成两个或三个轨道.

♡

证明 根据推论 2.7, 可设极点集可分解成 k 个轨道,

$$P = P_1 \cup P_2 \cup \cdots \cup P_k,\ x_i \in P_i.$$

又设 $|G| = n$, $n_i = |G_{x_i}|, p_i = |P_i|$, 其中 G_{x_i} 是 x_i 的迷向子群. 于是由推论 2.7和推论 1.1知

$$p_i = |P_i| = [G : G_{x_i}] = \frac{n}{n_i},\quad n_i \geqslant 2.$$

于是 G_{x_i} 中非恒等元数为 $n_i - 1 = \dfrac{n}{p_i} - 1$. 于是对于第 i 个轨道,G 中以 P_i 中某点为极点的非恒等元的变换数目为

$$\sum_{x \in P_i} |G_x \setminus \{\mathrm{id}\}| = p_i(n_i - 1) = n - p_i.$$

将每个轨道并起来得到

$$\sum_{x \in P} |G_x \setminus \{\mathrm{id}\}| = \sum_{i=1}^{k} p_i(n_i - 1) = \sum_{i=1}^{k}(n - p_i).$$

但注意 G 中除恒等变换外有 $n-1$ 个变换, 并且除恒等变换外的每个变换 g 都有两个极点, 即若 $gx = x$, 则 $g \in G_x \cap G_{-x}$, 故上述计数中每个 g 都重复计数了一次. 因而有

$$\sum_{i=1}^{k} p_i(n_i - 1) = 2(n-1).$$

以 n 除两边, 则有

$$\sum_{i=1}^{k}\left(1 - \frac{1}{n_i}\right) = 2\left(1 - \frac{1}{n}\right), \tag{2.38}$$

其中

$$n \geqslant n_i \geqslant 2.$$

若 $k = 1$, 则由式(2.38)知 $n_1 = n$, 于是 $1 - \dfrac{1}{n} = 2\left(1 - \dfrac{1}{n}\right)$, 矛盾.

若 $k \geqslant 4$, 则由式(2.38)知

$$\sum_{i=1}^{k}\left(1-\frac{1}{n_i}\right)=k-\sum_{i=1}^{k}\frac{1}{n_i}\geqslant k-\frac{k}{2}=\frac{k}{2}\geqslant 2,$$

但是 $2\left(1-\frac{1}{n}\right)<2$, 这就导出矛盾, 故 $k=2$ 或 $k=3$.

□

定理 2.45

如果第一类点群 G 的极点分成两个轨道, 则 G 只有两个极点 $x,-x$. 此时 $G_x=G_{-x}=G$ 为 n 阶循环群.

♡

注 对于群 G, 有一个简单的几何解释. 可以把 g 看成在平面直角坐标系中绕原点旋转 $2\pi/n$ 角, 即有

$$g=\begin{pmatrix}\cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n}\\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n}\end{pmatrix}.$$

证明 设 G 的极点集 P 可分解为如下两个轨道:

$$P=P_1\cup P_2,\ x_i\in P_i.$$

其中 $p_1=|P_1|\geqslant 1, p_2=|P_2|\geqslant 1$. 又设 $|G|=n$, $n_i=|G_{x_i}|$,G_{x_i} 是 x_i 的迷向子群. 由式(2.38)有

$$2(1-n^{-1})=1-n_1^{-1}+1-n_2^{-1},$$
$$\frac{2}{n}=\frac{1}{n_1}+\frac{1}{n_2}=\frac{p_1}{n}+\frac{p_2}{n},$$

因此

$$p_1=p_2=1,\ n_1=n_2=n,$$

故 G 只有两个极点 $x,-x$, 因而 G 中每个元素转动轴都是通过 x 与 $-x$ 的直线. 设 G 中 n 个元素 $\mathrm{id}, g_1,\cdots,g_{n-1}$ 的旋转角分别为

$$0<\theta_1<\theta_2<\cdots<\theta_{n-1}(<2\pi).$$

由带余除法, 对 $i\geqslant 2$ 有 $m_i\in\mathbb{N}$, 使得

$$\theta_i=m_i\theta_1+\phi_i,\ 0\leqslant\phi_i<\theta_1.$$

于是 $g_ig_1^{-m_i}\in G$ 的旋转角为 $\theta_i-m_i\theta_i=\phi_i$. 若 $\phi_i\neq 0$, 则 $g_ig_1^{-m_i}$ 的旋转角与 G 中所有元素都不同, 即 $g_ig_1^{-m_i}\notin G$ 矛盾! 故 $\phi_i=0$, 即 $g_i=g_1^{m_i}$, 从而 G 为循环群且 $\theta_1=\frac{2\pi}{n}$.

□

定理 2.46

如果第一类点群 G 的极点分成三个轨道, 在方程(2.38)中, 设 $n_1\leqslant n_2\leqslant n_3$, 则有以下情形:

(1) $n_1=n_2=2$, $n_3=\frac{n}{2}$, n 为偶数,$n\geqslant 4$;

(2) $n_1=2$, $n_2=n_3=3$, $n=12$;

(3) $n_1=2$, $n_2=3$, $n_3=4$, $n=24$;

(4) $n_1=2$, $n_2=3$, $n_3=5$, $n=60$.

♡

证明 设 G 的极点集 P 可分解为如下三个轨道:

$$P=P_1\cup P_2\cup P_3,\ x_i\in P_i,\ i=1,2,3.$$

其中 $p_i=|P_i|\geqslant 1$. 又设 $|G|=n$, $n_i=|G_{x_i}|$,G_{x_i} 是 x_i 的迷向子群. 方程(2.38)可化简为

$$1+\frac{2}{n}=\frac{1}{n_1}+\frac{1}{n_2}+\frac{1}{n_3},\ n\geqslant n_i\geqslant 2.$$

由 $n_1 \leqslant n_2 \leqslant n_3$, 故 $n_1 \geqslant 3$ 时无解. 于是有

$$n_1 = 2,$$

此时有

$$1 + \frac{2}{n} = \frac{1}{2} + \frac{1}{n_2} + \frac{1}{n_3}.$$

若 $n_2 \geqslant 4$, 此时有

$$\frac{1}{2} + \frac{1}{n_2} + \frac{1}{n_3} \leqslant \frac{1}{2} + \frac{1}{4} + \frac{1}{4} = 1 < 1 + \frac{2}{n},$$

矛盾. 故 $n_2 \geqslant 4$ 方程时无解. 因此 $2 \leqslant n_2 \leqslant 3$, 即 $n_2 = 2$或3.

(1) 当 $n_1 = n_2 = 2$ 时, 此时有

$$\frac{1}{n_3} = \frac{2}{n},$$

即 $n = 2n_3$ 为偶数. 由 $n_3 \geqslant 2$, 故 $n \geqslant 4$.

(2) 当 $n_1 = 2$, $n_2 = 3$ 时有

$$1 + \frac{2}{n} = \frac{1}{2} + \frac{1}{3} + \frac{1}{n_3},$$

再结合 $n > n_1 + n_2 = 5$ 可得

$$\frac{1}{6} + \frac{2}{n} = \frac{1}{n_3} \Longrightarrow n_3 = 6 - \frac{72}{n+12} \in (6 - \frac{72}{5+12}, 6),$$

再结合 $n_3 \geqslant n_2 = 3$ 可得

$$3 \leqslant n_3 \leqslant 5.$$

(i) 当 $n_1 = 2$, $n_2 = 3$, $n_3 = 3$ 时有 $n = 12$.

(ii) 当 $n_1 = 2$, $n_2 = 3$, $n_3 = 4$ 时有 $n = 24$.

(iii) 当 $n_1 = 2$, $n_2 = 3$, $n_3 = 5$ 时有 $n = 60$.

□

设第一类点群 G 的极点集 P 分解为如下三个轨道:

$$P = P_1 \cup P_2 \cup P_3,\ x_i \in P_i,\ i = 1, 2, 3.$$

其中 $p_i = |P_i| \geqslant 1$. 又设 $|G| = n$, $n_i = |G_{x_i}|$,G_{x_i} 是 x_i 的迷向子群. 由定理 2.46知 n_1, n_2, n_3 的取值只有四种情况.

(1) 当 $n_1 = n_2$, $n = 2n_3$ 时,G 称为**二面体群**, 记为 D_{n_3}. 设 T 是平面上一个正 n_3 边形, 以 T 的中心 O 为原点, 通过 O 垂直 T 的平面的直线为 Oz 轴.r 为绕 Oz 旋转 $\frac{2\pi}{n}$ 角. 显然 r 使正 n_3 边形不变,$r^k (k = 0, 1, \cdots, n_3 - 1)$ 也使正 n_3 边形不变.T 有 n_3 条对称轴, 绕对称轴旋转 $180°$ 也保持 T 不变. 所有保持 T 不变的空间转动构成的群就是 G, 极点集 P 为这些转动轴与 S_r 的交点, 在 G 的作用下分为三个轨道.

(2) 当 $n_1 = 2$, $n_2 = 3$, $n_3 = 3$, $n = 12$ 时, 群 G 称为**正四面体群** (tetrahedral group), 记为 T. 设 T 为正四面体, 以一个顶点与中心的连线为轴旋转 $120°, 240°$ 都使 T 不变. 以中心与一边的中点的连线为轴旋转 $180°$ 也使 T 不变. 所有保持 T 不变的空间转动构成的群就是 G, 极点集 P 为这些转动轴与 S_r 的交点, 在 G 的作用下分为三个轨道.

一个正四面体是由 4 个正三角形围成的多面体. 取它的中心为坐标原点, 并使其 4 个顶点的坐标为

$$A_1(-1, -1, 1),\ A_2(1, 1, 1),\ A_3(1, -1, -1),\ A_4(-1, 1, -1),$$

如图 2.4所示.

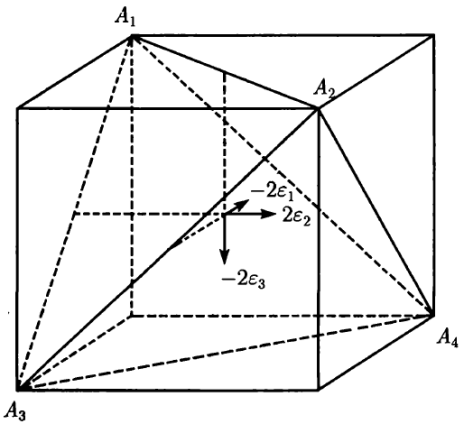

图 2.4

以 T 表示空间正四面体群, 这是使正四面体不变的旋转构成的群.

现在来看看 T 的元素. 首先, 保持 A_1 不动的变换, 除单位变换外, 还有绕过 A_1 与 $\triangle A_2A_3A_4$ 中心的直线旋转 120° 与 240°. 这两个变换有对称群的表示法:(A_2, A_3, A_4) 与 (A_2, A_4, A_3).

同样, 可以求出保持 A_2, A_3, A_4 的变换的对称群的表示法

$$(A_1, A_3, A_4),\ (A_1, A_4, A_3),\ (A_1, A_2, A_4),\ (A_1, A_4, A_2),\ (A_1, A_2, A_3),\ (A_1, A_3, A_2).$$

此外, 绕三个坐标轴旋转 180° 也使正四面体不变, 这样又有三个元素, 它们的对称群的表示法为

$$(A_2, A_3)(A_1, A_4),\ (A_1, A_3)(A_2, A_4),\ (A_1, A_2)(A_3, A_4).$$

不难看出 $|T| = 12$, 而且与 4 个文字的交错群 A_4 同构.

(3) 当 $n_1 = 2$, $n_2 = 3$, $n_3 = 4$, $n = 24$ 时, 群 G 称为**正八面体群** (octahedral group), 记为 O. 设 T 为正八面体, 以一个顶点与中心的连线为轴旋转 $90^\circ, 180^\circ, 270^\circ$ 都使 T 不变. 以中心与一边的中点的连线为轴旋转 180° 也使 T 不变. 以中心与一个面的中心的连线为轴旋转 $120^\circ, 240^\circ$ 也使 T 不变. 所有保持 T 不变的空间转动构成的群就是 G, 极点集 P 为这些转动轴与 S_r 的交点, 在 G 的作用下分为三个轨道.

一个正八面体是由 8 个正三角形围成的多面体. 取正八面体的中心为坐标原点, 并使正八面体的 6 个顶点坐标为

$$(\pm 1, 0, 0),\ (0, \pm 1, 0),\ (0, 0, \pm 1),$$

如图 2.5所示.

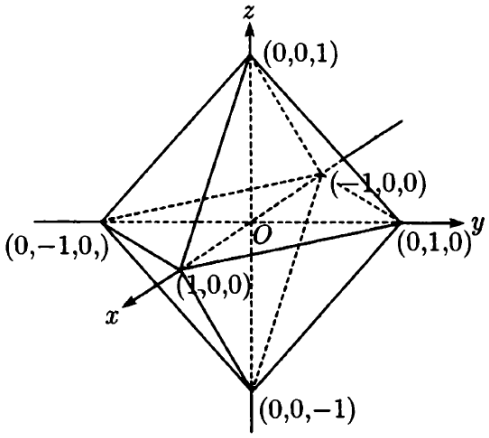

图 2.5

显然

$$x = \pm 1,\ y = \pm 1,\ z = \pm 1$$

这 6 个平面围成一个立方体. 此立方体 6 个面的中心恰为正八面体的 6 个顶点, 称为正八面体的外接立方体, 而

$$x = \pm\frac{1}{2},\ y = \pm\frac{1}{2},\ z = \pm\frac{1}{2}$$

这 6 个面围成一个立方体, 它的 8 个顶点恰好是正八面体 8 条棱的中点, 称为正八面体的内接立方体.

所谓正八面体群 O 即保持正八面体不变的旋转构成的群. 由于正八面体与立方体的关系, 因而 O 也是使立方体不变的旋转构成的群.

上面正八面体外接立方体的 8 个顶点的坐标为 $(\pm 1, \pm 1, \pm 1)$. 记通过点 $(1,1,1), (-1,1,1), (-1,-1,1)$ 与 $(1,-1,1)$ 的 4 条对角线为 $\alpha_1, \alpha_2, \alpha_3$ 与 α_4.

显然,O 中任一元素引起 $\alpha_1, \alpha_2, \alpha_3$ 与 α_4 的一个置换. 由于立方体的位置完全由这 4 条对角线决定, 故 O 中不同元素引起 $\alpha_1, \alpha_2, \alpha_3$ 与 α_4 的不同置换. 因此, 可视 $O \subseteq S_4$. 另一方面,S_4 可由 (12), (143) 两个元素生成. 事实上记 $x = (12), y = (143)$. 于是

$$xyx^{-1} = (243),\ yxy^{-1} = (24),$$
$$(243)x(243)^{-1} = (14),\ (243)^2x(243)^{-2} = (13).$$

由此可知 (12), (143) 生成 S_4.

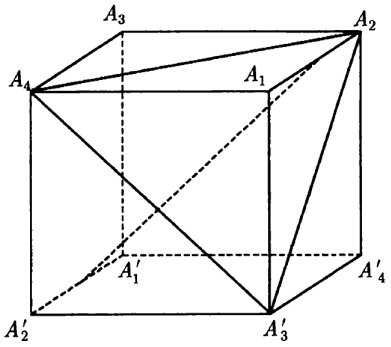

图 2.6

如图 2.6所示. 通过 A_1A_2 的中点与 $S_1'A_2'$ 的中点的轴在 $\square A_1A_2A_1'A_2'$ 所在的平面内, 与 $\square A_4A_3A_4'A_3'$ 垂直且过其中心. 绕此轴旋转 180°, 则有 $A_3 \to A_3', A_4 \to A_4', A_1 \to A_2, A_1' \to A_2'$, 因而恰好对应变换 $(\alpha_1\alpha_2)$. 同样能求出其他变换, 因而 $O \cong S_4$, 故以 S_4 代替 O.

又对角线 $\alpha_1 = A_1A_1'$ 垂直于 $\triangle A_2A_4A_3'$, 于是绕 α_1 旋转 $120°, 240°$ 也使立方体不变, 而 120° 的旋转恰为 $(\alpha_2\ \alpha_3\ \alpha_4)$.

O 也是使立方体保持不变的群.

(4) 当 $n_1 = 2,\ n_2 = 3,\ n_3 = 5,\ n = 60$ 时, 群 G 称为**正二十面体群** (icoshedral group), 记为 I. 设 T 是正二十面体, 是由 20 个正三角形组成. 通过 T 的中心与棱的中点的连线有 15 条直线, 绕这些直线的每一条线旋转 180° 都保持 T 不变. 因此,I 有 15 个二阶元. 这些直线与 S_r 的交点为 I 的极点, 并构成一个轨道 $P_1, |P_1| = 30$, 其中一点的迷向子群的阶 $n_1 = 2$.

通过 T 的中心与各面中心的连线有 10 条, 正好是长对角线所在直线. 绕这些直线的每一条线旋转 $120°, 240°$ 都保持 T 不变. 因此,I 有 20 个三阶元. 这些直线与 S_r 的交点为 I 的极点, 并构成一个轨道 $P_2, |P_2| = 20$, 其中一点的迷向子群的阶 $n_2 = 3$.

通过 T 的中心与各顶点的连线有 6 条, 正好是长对角线所在直线. 绕这些直线的每一条线旋转 72°,144°,216°, 288° 都保持 T 不变. 因此,I 有 24 个 5 阶元. 这些直线与 S_r 的交点为 I 的极点, 并构成一个轨道 $P_3, |P_3| = 12$, 其中一点的迷向子群的阶 $n_3 = 5$.

因此,I 是 60 阶群,I 的极点集 P 分成三个轨道,$P = P_1 \cup P_2 \cup P_3$. 保持 T 不变的转动群称为正二十面体群, 记为 I.

以正二十面体的各面的中心为顶点, 相邻两面的中心的连线为棱, 于是构成一个以 12 个正五边形为面的正十二面体, 称为 T 的内接正十二面体 (图 2.7),I 也保持内接正十二面体不变.

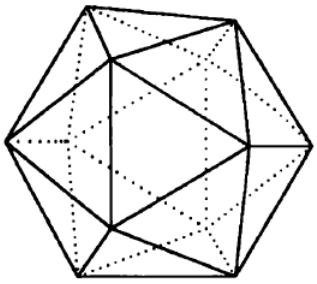

图 2.7

定理 2.47

$\cos 72^\circ = \frac{1}{4}(-1+\sqrt{5}), \sin 72^\circ = \frac{1}{4}\sqrt{10+2\sqrt{5}}$.

$\omega = \frac{1}{2}(-1+\sqrt{5})$ 称为**黄金分割数**.

♡

证明 设在 $\triangle ABC$ 中,

$$AB = AC = 1,\ \angle A = 36^\circ,\ \angle B = \angle C = 72^\circ.$$

作 $\angle B$ 的平分线交 AC 于 E. 于是

(1) $\triangle EAB$ 为等腰三角形且 $AE = EB$.

(2) $\triangle BCE$ 为顶角为 36° 的等腰三角形,$EB = BC$, 因此 $\triangle ABC \sim \triangle BCE$,

从而

$$AC : AE = AC : BC = BC : EC = AE : (AC - AE).$$

由 $AC = 1$ 有 $BC = AE = \frac{1}{2}(-1+\sqrt{5})$, 再由正弦定理即得结论.

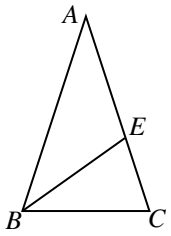

图 2.8

□

定理 2.48

I 是单群, 与 A_5 同构.

♡

证明 因为 I 的二阶元彼此共轭, 构成一个共轭类 C_2, $c_2 = 15$; 三阶元彼此共轭, 构成一个共轭类 C_3, $c_3 = 20$; 旋转 $72^\circ, 288^\circ$ 的元素彼此共轭, 构成一个共轭类 C_4, $c_4 = 12$; 旋转 $144^\circ, 216^\circ$ 的元素彼此共轭, 构成一个共轭类 C_5, $c_5 = 12$. 又 $C_1 = \{\mathrm{id}\}$, $c_1 = 1$. 由此可知 I 是 60 阶单群.

I 的 Sylow 2 子群的个数 $2t+1 \mid 15$,I 中无 4 阶元,2 的个数为 20, 因此 $2t+1 = 5$.

设 I 的 5 个 Sylow 2 子群为 Y_1, Y_2, Y_3, Y_4 和 Y_5. $\forall g \in C$, 定义 g 在 $X = \{Y_1, Y_2, Y_3, Y_4, Y_5\}$ 上的作用 $\Phi(g)$,

$$\Phi(g)Y_i = gY_iG^{-1},\ Y_i \in X.$$

于是 $\Phi(g) \in S_X \cong S_5$ 且

$$\Phi(gh) = \Phi(g)\Phi(h),\ \forall g, h \in I.$$

因此,Φ 是 I 到 S_5 的同态映射,$\Phi(I)$ 有 3 阶元与 5 阶元, 因此 $\Phi(I) \supseteq A_5$. 又因 I 为 60 阶的单群, 故 $I \cong A_5$.

□

第 3 章 环

3.1 分式域

定义 3.1 (分式域)

若交换整环 R 是域 F 的子环且 $\forall a \in F, \exists b, c \in R$ 且 $c \neq 0$, 使得

$$a = bc^{-1}, \text{其中} c^{-1} \text{是} c \text{在域} F \text{中的乘法逆元},$$

则称 F 为 R 的**分式域**, 记为 $F = \mathrm{Frac}(R)$.

♣

定理 3.1

设 R 为交换整环, 则 R 的分式域一定存在.

♡

注 关于 R 的条件可放宽为 R 是无零因子交换环, 即 R 中不必有幺元.

证明 令 $R^* = R \setminus \{0\}$, 在集合 $R \times R^*$ 中定义加法与乘法,$\forall (a,b),(c,d) \in R \times R^*$,

$$(a,b) + (c,d) = (ad + bc, bd), \tag{3.1}$$

$$(a,b)(c,d) = (ac, bd). \tag{3.2}$$

易验证 $R \times R^*$ 对上述加法与乘法都是交换幺半群, 它们的零元素及幺元分别为 $(0,1)$,$(1,1)$. 在 $R \times R^*$ 中定义一个关系 “$\sim$”,

$$(a,b) \sim (c,d), \quad \text{若} ad = bc.$$

先证明关系 $\sim$ 是等价关系. 事实上, 由 $ab = ab$ 知 $(a,b) \sim (a,b)$. 又若 $(a,b) \sim (c,d)$, 即 $ad = cb$, 因而 $(c,d) \sim (a,b)$. 最后, 假设 $(a,b) \sim (c,d)$,$(c,d) \sim (e,f)$, 则 $adf = bcf = bde$. 由 R 是交换整环,$d \neq 0$, 于是 $af = be$, 即 $(a,b) \sim (e,f)$.

其次证明关系 $\sim$ 对于 $R \times R^*$ 中的乘法是同余关系, 设

$$(a,b) \sim (c,d), \quad (e,f) \sim (g,h).$$

于是由式 (3.2) 知

$$(a,b)(e,f) = (ae, bf), \quad (c,d)(g,h) = (cg, dh),$$

而由 R 是交换整环可得 $(ae)(dh) = adeh = bcfg = (bf)(cg)$, 即有

$$(a,b)(e,f) \sim (c,d)(g,h).$$

再次证明关系 $\sim$ 对于 $R \times R^*$ 中的加法是同余关系. 设

$$(a,b) \sim (c,d), \quad (e,f) \sim (g,h),$$

则由式 (3.1) 知

$$(a,b) + (e,f) = (af + be, bf), \quad (c,d) + (g,h) = (ch + dg, dh).$$

这时由 R 是交换整环可得

$$(af + be)dh = adfh + bedh = bcfh + fgbd = (ch + dg)bf,$$

因而 $((a,b) + (e,f)) \sim ((c,d) + (g,h))$.

令 $F = R \times R^* / \sim$ 为商集合, 以 $\dfrac{a}{b}$ 表示 (a,b) 所在等价类. 于是由定理 1.20, 在 F 中有加法与乘法运算如下:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$

$$\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}.$$

再由定理 1.12知 F 对加法与乘法都是交换幺半群. 零元素与幺元素为 $\frac{0}{1},\frac{1}{1}$, 记 $0=\frac{0}{1},1=\frac{1}{1}$. 对 $\forall d\in R$, 由于 $0\cdot d=0\cdot 1$, 故有 $(0,1)$ 与 $(0,d)$ 等价, 即 $\frac{0}{1}=\frac{0}{d}$. 又由 $1\cdot d=1\cdot d$ 知 $\frac{1}{1}=\frac{d}{d}=1$.

由

$$\frac{a}{b}+\frac{-a}{b}=\frac{ab-ab}{b^2}=\frac{0}{b^2}=0$$

知 F 对加法为交换群.

又若 $\frac{a}{b}\neq 0$, 即 $a\neq 0$, 则 $(b,a)\in R\times R^*$, 即 $\frac{b}{a}\in F$. 这时

$$\frac{a}{b}\cdot\frac{b}{a}=\frac{ab}{ab}=1,$$

故 $F^*=F\setminus\{0\}$ 对乘法为交换群且 $\left(\frac{a}{b}\right)^{-1}=\frac{b}{a}$. 又由

$$\begin{aligned}\left(\frac{a}{b}+\frac{c}{d}\right)\cdot\frac{f}{e}&=\frac{ad+bc}{bd}\cdot\frac{f}{e}=\frac{adf+bcf}{bde}\\&=\frac{adef+bcef}{bdee}=\frac{af}{be}+\frac{cf}{de}\\&=\frac{a}{b}\cdot\frac{f}{e}+\frac{c}{d}\cdot\frac{f}{e}.\end{aligned}$$

知 F 中加法与乘法间分配律成立, 故 F 为域.

记 $R_1\triangleq\left\{\frac{a}{1}:a\in R\right\}$, 则

$$\frac{a}{1}+\frac{b}{1}=\frac{a+b}{1},\quad \frac{a}{1}\cdot\frac{b}{1}=\frac{ab}{1},$$

故 R_1 是 F 的子环. 由于 $\frac{a}{1}=\frac{b}{1}$ 当且仅当 $a=b$, 故 $\frac{a}{1}\to a$ 是 R_1 到 R 上的一个良定义的映射, 不难验证其也是同构映射, 因此可将 R 作为 F 的子环. 而对 F 中任一元素 $\frac{a}{b}$ 有

$$\frac{a}{b}=\frac{a}{1}\cdot\frac{1}{b}=\frac{a}{1}\cdot\left(\frac{b}{1}\right)^{-1},$$

故 F 是 R 的分式域. 综上可知

$$F=R\times R^*/\sim=\left\{\frac{a}{b}\mid a\in R,b\in R^*\right\}$$

是 R 的分式域.

□

定理 3.2

交换整环 R 的分式域 F 是以 R 为子环的最小体, 进而 F 是以 R 为子环的最小域, 因而 R 的分式域唯一. 特别地, 若 F 是一个域, 则 F 的分式域就是其本身.

♡

注 关于 R 的条件可放宽为 R 是无零因子交换环, 即 R 中不必有幺元.

证明 设 F' 是体且以 R 为子环, 则 F' 中子集

$$F_1=\{ab^{-1}\mid a,b\in R,b\neq 0\}$$

是 F' 的子体, 事实上, 对 $\forall ab^{-1},cd^{-1}\in F_1$, 有

$$ab^{-1}+cd^{-1}=(ad+cd)(bd)^{-1},\quad -(ab^{-1})=(-a)b^{-1},$$

故 F_1 对加法为 F' 的子群. 又若 $ab^{-1},cd^{-1}\in F_1\setminus\{0\}$, 则

$$(ab^{-1})(cd^{-1})^{-1}=(ad)(bc)^{-1},$$

故 $F_1\setminus\{0\}$ 对乘法为 $F'\setminus\{0\}$ 的子群, 因此 F_1 是 F' 的子体. 由定理 3.1知, 记 $\frac{a}{b}\triangleq\{(c,d)\in R\times R^*\mid ad=bc\}$, 则

R 的一个分式域为

$$F=\left\{\frac{a}{b}\mid a\in R,b\in R^*\right\}.$$

又 $\frac{a}{b}\to ab^{-1}$ 是 R 的分式域 F 到 F_1 上的同构, 故可将 F 与 F_1 等同, 因而 $F\subseteq F'$.

再设 M 是以 R 为子环的域, 则 M 也是体, 从而 $F\subseteq M$. 故 F 是以 R 为子环的最小域. 因而 R 的分式域唯一, 否则与 F 是以 R 为子环的最小域矛盾!

□

推论 3.1

设 R_1,R_2 都是交换整环,F_1,F_2 分别是 R_1,R_2 的分式域, 则 $R_1\cong R_2\iff F_1\cong F_2$.

♡

证明

□

推论 3.2

设 R 为交换整环,$R^*=R\setminus\{0\}$, 则在 $R\times R^*$ 中定义一个关系 “$\sim$”

$$(a,b)\sim(c,d),\ 若ad=bc.$$

则 $\sim$ 是同余关系. 以 $\frac{a}{b}$ 表示 (a,b) 所在等价类, 即

$$\frac{a}{b}=\{(c,d)\in R\times R^*\mid(a,b)\sim(c,d)\}=\{(c,d)\in R\times R^*\mid ad=bc\}.$$

则

$$F=R\times R^*/\sim=\left\{\frac{a}{b}\mid a\in R,b\in R^*\right\}$$

是 R 的分式域, 也是以 R 为子环的最小域, 进而 F 就是 R 的唯一分式域. 并且记 $a=\frac{a}{1},\forall a\in R$. 其中 F 的加法和乘法分别定义为

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd},\quad \frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd},\quad \forall\frac{a}{b},\frac{c}{d}\in F.$$

进而 $\frac{a}{b}$ 加法和乘法逆元分别为

$$-\frac{a}{b},\quad \frac{b}{a}.$$

♡

证明 由定理 3.1和定理 3.2立得.

□

例题 3.1 设 $\mathbb{P}$ 是任一数域, 设 $\mathbb{P}[x]$ 的分式域为 $\mathbb{P}(x)$, 则

$$\mathbb{P}(x)=\left\{\frac{f(x)}{g(x)}\mid f(x),g(x)\in\mathbb{P}[x],g(x)\neq 0\right\}.$$

证明

□

命题 3.1

设 m 是非零整数, 则 $m\mathbb{Z}$ 的分式域为 $\mathbb{Q}$.

♠

证明

□

3.2 多项式环

定理 3.3

设 $\widetilde{R}$ 是一个交换幺环,R 是 $\widetilde{R}$ 的子环且 $1 \in R$. 又设 $u \in \widetilde{R}$,$\widetilde{R}$ 中由 R 与 u 生成的子环, 即包含 R 与 u 的最小子环记为 $R[u]$. 则

$$R[u] = \{a_0 + a_1u + \cdots + a_nu^n \mid a_i \in R, n \in \mathbb{N} \cup \{0\}\},$$

也称 $R[u]$ 为 R **上添加** u **生成的子环**.

♡

证明 记 $S = \{a_0 + a_1u + \cdots + a_nu^n \mid a_i \in R, n \in \mathbb{N} \cup \{0\}\}$. 首先证明 $S \subseteq R[u]$. 由于 $R[u]$ 是包含 R 和 u 的子环, 而 S 中的所有元素都可以通过有限次运算 (加法、乘法、取逆) 从 R 和 u 得到, 因此 $S \subseteq R[u]$.

接下来证明 $R[u] \subseteq S$. 设 $f(u) = a_0 + a_1u + \cdots + a_mu^m \in S$,$g(u) = b_0 + b_1u + \cdots + b_nu^n \in S$, 不妨设 $m \leqslant n$, 再令 $a_{m+1} = \cdots = a_n = 0$, 则

$$f(u) + g(u) = \sum_{i=0}^{n}(a_i + b_i)u^i \in S.$$

令 $-f(u) \triangleq (-a_0) + (-a_1)u + \cdots + (-a_m)u^m \in S$, 则 $f(u) + (-f(u)) = 0$. 因此 S 对加法封闭且有加法逆元. 又 $\widetilde{R}$ 是交换幺环且 $S \subseteq \widetilde{R}$, 故 S 对加法满足结合律和交换律. 于是 S 对加法构成 $\widetilde{R}$ 的 Abel 群.

由于 $\widetilde{R}$ 是交换环, 故

$$f(u)\,g(u) = \left(\sum_{i=1}^{n} a_iu^i\right)\left(\sum_{i=1}^{n} b_iu^i\right) = \sum_{k=0}^{m+n}\left(\sum_{i+j=k} a_ib_j\right)u^k \in S.$$

令 $a_0 = 1, n = 0$, 则有 $1 \in S$. 因此 S 对乘法封闭且含幺元 1. 又 $\widetilde{R}$ 是交换幺环且 $S \subseteq \widetilde{R}$, 故 S 对乘法满足结合律. 于是 S 对乘法构成 $\widetilde{R}$ 的幺半群. 由于 S 对加法和乘法封闭,$\widetilde{R}$ 为交换幺环且 $S \subseteq \widetilde{R}$, 故 S 的加法与乘法间自然满足分配律. 因此 S 是交换幺环 $\widetilde{R}$ 的子环.

对于任意 $r \in R$, 可取 $r = r + 0 \cdot u + 0 \cdot u^2 + \cdots \in S$, 故 $R \subseteq S$. 同时 $u = 0 + 1 \cdot u + 0 \cdot u^2 + \cdots \in S$. 再设 T 是 $\widetilde{R}$ 的任一包含 R 和 u 的子环, 则 T 必然包含所有的 a_iu^i $(a_i \in R)$ 以及它们的有限和, 即 $S \subseteq T$. 因此 S 是包含 R 和 u 的最小子环.

综上可知 $R[u] = S$.

□

定义 3.2

如果在 R 中存在有限多个元素 $a_0, a_1, \cdots, a_n$ 且 $a_n \neq 0$, 使得

$$a_0 + a_1u + \cdots + a_nu^n = 0,$$

那么称 u 为 R 上的**代数元**, 使上述关系成立的最小正整数 n 称为代数元 u 的**次数**, 记为 $\deg(u, R)$.

♣

例题 3.2 令 $\widetilde{R} = \mathbb{C}$, 则 $\sqrt{-1}$ 为 $\mathbb{Z}$ 上的代数元,

$$\mathbb{Z}[\sqrt{-1}] = \{m + n\sqrt{-1} \mid m, n \in \mathbb{Z}\}$$

称为 **Gauss 的整数环**,$\deg(\sqrt{-1}, \mathbb{Z}) = 2$. 同样 $\sqrt{-1}$ 为 $\mathbb{Q}$ 上的代数元,$\deg(\sqrt{-1}, \mathbb{Q}) = 2$.

证明

□

例题 3.3 令 $\widetilde{R} = \mathbb{Q}$, 则 $\dfrac{1}{2}$ 是 $\mathbb{Z}$ 上代数元且 $\mathbb{Z} \subset \mathbb{Z}\left[\dfrac{1}{2}\right] \subset \mathbb{Q}$,$\deg\left(\dfrac{1}{2}, \mathbb{Z}\right) = 1$.

证明

□

定义 3.3

设 R 是交换幺环 $\widetilde{R}$ 的包含幺元 1 的子环,$u \in \widetilde{R}$,$R[u]$ 为 R 添加 u 生成的 $\widetilde{R}$ 的子环, 若当 R 中有限个元素 $a_0, a_1, \cdots, a_n$ 不全为 0 时,

$$a_0 + a_1 u + \cdots + a_n u^n \neq 0,$$

则称 u 为 R 上的**超越元**或**不定元**.$R[u]$ 中的一个元素 $f(u) = a_0 + a_1 u + \cdots + a_n u^n$ 称为 u 的 (系数在 R 中的) 一个**多项式**. 若 $a_n \neq 0$, 则称 n 为 $f(u)$ 的**次数**, 记为 $\deg f(u)$.$R[u]$ 称为 R 上的一个**一元多项式环**. ♣

例题 3.4 设 $\mathbb{P}$ 是一个数域,x 是一个文字, 则 $\mathbb{P}[x]$ 是 $\mathbb{P}$ 上的一个一元多项式环,x 是 $\mathbb{P}$ 上的超越元.

证明

□

定理 3.4

交换幺环 R 上的一元多项式环一定存在. ♡

证明 令

$$\widetilde{R} = \{(a_0, a_1, \cdots) \mid a_i \in R \text{ 且仅有有限个} a_i \neq 0\}.$$

自然 $\widetilde{R}$ 中元素 $(a_0, a_1, \cdots) = (b_0, b_1, \cdots)$ 当且仅当 $a_i = b_i (i = 0, 1, \cdots)$. 在 $\widetilde{R}$ 中定义加法与乘法

$$(a_0, a_1, \cdots) + (b_0, b_1, \cdots) = (a_0 + b_0, a_1 + b_1, \cdots), \tag{3.3}$$

$$(a_0, a_1, \cdots) \cdot (b_0, b_1, \cdots) = (c_0, c_1, \cdots). \tag{3.4}$$

其中,

$$\begin{aligned} c_n &= a_0 b_n + a_1 b_{n-1} + \cdots + a_{n-1} b_1 + a_n b_0 \\ &= \sum_{i+j=n} a_i b_j, \quad n = 0, 1, \cdots. \end{aligned} \tag{3.5}$$

由于 $(a_0, a_1, \cdots), (b_0, b_1, \cdots) \in \widetilde{R}$, 故 $\exists m \in \mathbb{N}$, 使 $n > m$ 时,$a_n = b_n = 0$. 于是 $a_n + b_n = 0$, 故 $(a_0 + b_0, a_1 + b_1, \cdots) \in \widetilde{R}$. 而当 $n > 2m$ 时,$c_n = \sum_{i+j=n} a_i b_j = 0$, 故 $(c_0, c_1, \cdots) \in \widetilde{R}$. 由此知上面定义的加法与乘法是良定义的.

容易验证 $\widetilde{R}$ 对加法为 Abel 群, 它的零元素为 $0 = (0, 0, \cdots)$ 且 $-(a_0, a_1, \cdots) = (-a_0, -a_1, \cdots)$. 同样容易验证 $\widetilde{R}$ 对乘法是可交换的且有幺元 $(1, 0, \cdots)$. 下面验证乘法的结合律. 设

$$f = (a_0, a_1, \cdots), \quad g = (b_0, b_1, \cdots), \quad h = (c_0, c_1, \cdots),$$

则 $(fg)h$ 的第 k 个元素为

$$\sum_{s+r=k} \left(\sum_{i+j=s} a_i b_j \right) c_r = \sum_{i+j+r=k} a_i b_j c_r = \sum_{i+t=k} a_i \left(\sum_{j+r=t} b_j c_r \right),$$

这也是 $f(gh)$ 的第 k 个元素. 故 $\widetilde{R}$ 对乘法为交换幺半群. 又注意到 $(f + g)h$ 的 k 个元素为

$$\sum_{i+j=k} (a_i + b_i) c_j = \sum_{i+j=k} a_i c_j + \sum_{i+j=k} b_i c_j,$$

这也是 $fh + gh$ 的第 k 个元素.$h(f + g)$ 的 k 个元素为

$$\sum_{i+j=k} c_i \left(a_j + b_j \right) = \sum_{i+j=k} c_i a_j + \sum_{i+j=k} c_i b_j,$$

这也是 $hf + hg$ 的第 k 个元素. 因此 $\widetilde{R}$ 中加法与乘法间的分配律成立, 故 $\widetilde{R}$ 为交换幺环.

令 $R_0 = \{(a_0, 0, 0, \cdots) : a_0 \in R\}$, 则 R_0 显然是 R 的子环. 由

$$(a_0, 0, \cdots) + (b_0, 0, \cdots) = (a_0 + b_0, 0, \cdots),$$

$$(a_0, 0, \cdots) \cdot (b_0, 0, \cdots) = (a_0 b_0, 0, \cdots)$$

知 $a_0 \to (a_0, 0, \cdots)$ 是 R 到 R_0 上的同构映射. 为方便计, 将 R_0 中元素 $(a_0, 0, \cdots)$ 记为 a_0, 即可将 R 视为 $\widetilde{R}$ 的子环. R 的幺元 1 恰为 $\widetilde{R}$ 的幺元 $(1, 0, \cdots)$.

最后证明 $\widetilde{R}$ 是 R 上的一元多项式环. 令

$$u = (0, 1, 0, \cdots),$$

则不难验证

$$u^k = (\underbrace{0, \cdots, 0}_{k}, 1, 0, \cdots),$$

$$a_k u^k = (\underbrace{0, \cdots, 0}_{k}, a_k, 0, \cdots), \quad a_k \in R = R_0.$$

若 $f = (a_0, a_1, \cdots) \in \widetilde{R}$, 则有 n, 使 $a_{n+1} = a_{n+2} = \cdots = 0$. 于是

$$f = a_0 + a_1 u + \cdots + a_n u^n,$$

因而有 $\widetilde{R} = R_0[u] = R[u]$. 又若

$$a_0 + a_1 u + \cdots + a_n u^n = 0,$$

即

$$(a_0, a_1, \cdots, a_n, 0, \cdots) = (0, 0, \cdots),$$

则 $a_0 = a_1 = \cdots = a_n = 0$, 即 u 是 R 上的超越元, 因而 $\widetilde{R} = R[u]$ 是 R 上的一元多项式环.

□

定理 3.5

设 R, S 都是交换幺环, 它们的幺元分别是 $1, 1'$. 又若 η 是 R 到 S 的同态且 $\eta(1) = 1'$, 则对 $\forall u \in S$, 存在唯一的在 R 上的开拓 $\eta_u : R[x] \to S$ 满足

$$\eta_u|_R = \eta, \quad \eta_u(x) = u. \tag{3.6}$$

且 η_u 是环同态.

♡

证明 因 $R[x]$ 为 R 上的一元多项式环, 故 $R[x] = \{a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in R\}$. 定义 η_u,

$$\eta_u(a_0 + a_1 x + \cdots + a_n x^n) = \eta(a_0) + \eta(a_1)u + \cdots + \eta(a_n)u^n \tag{3.7}$$

于是 η_u 是 $R[x]$ 到 S 的映射. 直接计算可知 η_u 为满足式(3.6)的扩充, 并为同态映射.

现设 η' 也是 η 的扩充且 $\eta'(x) = u$, 于是

$$\eta'\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} \eta'(a_i)u^i = \sum_{i=0}^{n} \eta(a_i)u^i = \eta_u\left(\sum_{i=0}^{n} a_i x^i\right),$$

故 $\eta' = \eta_u$, 即 η_u 是满足条件的唯一扩充.

□

推论 3.3

(1) 设 R 是交换幺环,$R[x]$ 与 $R[y]$ 都是 R 上的一元多项式环, 则 $R[x]$ 与 $R[y]$ 是同构的.

(2) 设 R 是交换幺环 $\widetilde{R}$ 的包含幺元 1 的子环,$R[x]$ 为 R 上的一元多项式环, 则对 $\forall u \in \widetilde{R}$, 存在 $R[x] \to R[u]$ 的满同态 η_u, 且满足

$$\eta_u((f(x))) = f(u), \ \forall f(x) \in R[x].$$

♡

笔记 这个推论 (1) 说明: 任何交换幺环上的一元多项式环在同构意义下唯一.

证明

(1) 事实上, 容易验证 R 到 $R[y]$ 的嵌入映射 $i(a) = a(\forall a \in R)$ 是 R 到 $R[y]$ 的环同态, 于是由定理 3.5知有 $R[x]$

到 $R[y]$ 的同态 i_y 满足

$$i_y|_R = i, \quad i_y(x) = y.$$

从而任取 $a_0 + a_1 y + \cdots + a_n y^n \in R[y]$, 都有

$$i_y(a_0 + a_1 x + \cdots + a_n x^n) = a_0 + a_1 y + \cdots + a_n y^n,$$

故 i_y 是满同态. 由 y 是 R 上超越元知 $\ker i_y = \{0\}$, 因此由命题 1.21(2)(ii)知 i_y 是单同态. 故 i_y 是同构映射.

(2) 考虑 R 到 $R[u]$ 的嵌入映射 η, 则不难验证 η 是 R 到 $R[u]$ 上的同态. 于是由定理 3.5知可将 η 扩充为环同态 $\eta_u : R[x] \to R[u]$ 满足

$$\eta_u|_R = \eta, \quad \eta_u(x) = u. \tag{3.8}$$

注意到 $\eta_u(R[x]) = R[u]$, 故 η_u 是满同态. 再利用(3.8)式可得

$$\eta((f(x))) = f(u), \ \forall f(x) \in R[x].$$

□

推论 3.4

设 R 是交换幺环 $\widetilde{R}$ 的包含幺元 1 的子环,$R[x]$ 为 R 上的一元多项式环, 又设 $u \in \widetilde{R}$, 则有 $R[x]$ 中的理想 I 满足 $R \cap I = \{0\}$,$R[u] \cong R[x]/I$, 并且当且仅当 $I \neq \{0\}$ 时,u 为代数元.

♡

证明 由推论 3.3(2)知存在 $R[x] \to R[u]$ 的满同态 i_u, 且满足

$$i_u(f(x)) = f(u), \ \forall f(x) \in R[x].$$

取 $I = \ker i_u$, 则由命题 1.21(2)知 $I = \ker i_u$ 为 $R[x]$ 中理想,$R[u] \cong R[x]/I$. 又若 $a \in R \cap I$, 则 $0 = i_u(a) = i(a) = a$, 故 $R \cap I = \{0\}$. 由于 u 为 R 上代数元当且仅当存在 $a_n \neq 0$, 使得 $\sum_{i=0}^{n} a_i u^i = 0$. 这也当且仅当

$$i_u\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} a_i u^i = 0 \iff 0 \neq \sum_{i=0}^{n} a_i x^i \in I \iff I \neq \{0\}.$$

□

推论 3.5

设 R 是交换幺环,$R[x]$ 是 R 上一元多项式环. 又若 I 是 $R[x]$ 的理想且 $R \cap I = \{0\}$,$I \neq \{0\}$, 则 $R[x]/I$ 是 R 添加一个代数元所得的环.

♡

证明 设 π 是 $R[x]$ 到 $R[x]/I$ 的自然同态, 于是 $\pi(R)$ 是 $R[x]/I$ 中的子环. 由定理 1.20(3)知 I 也是 R 的理想, 从而再由定理 1.43(3)知

$$\pi(R) = R/I = (R + I)/I \cong R/(R \bigcap I) = R/\{0\} = R + 0 = R,$$

故可将 R 视为 $R[x]/I$ 的子环, 令 $u = \pi(x)$, 则 $u \in R[x]/I$, 于是 $R[u] \subseteq R[x]/I$. 注意到

$$\pi(a_0 + a_1 x + \cdots + a_n x^n) = \pi(a_0) + \pi(a_1)u + \cdots + \pi(a_n)u^n,$$

故再结合 π 是满同态可得

$$R[x]/I = \pi(R[x]) \subseteq R[u] \subseteq R[x]/I,$$

即 $R[x]/I = R[u]$. 又由 $I \neq \{0\}$, 故 I 中有非零元素 $a_0 + a_1 x + \cdots + a_n x^n$, 其中 $a_n \neq 0$, 又因为 $\pi(R) \cong R$, 所以 $\pi(a_n) \neq 0$. 而

$$\pi(a_0 + a_1 x + \cdots + a_n x^n) = \pi(a_0) + \pi(a_1)u + \cdots + \pi(a_n)u^n = 0,$$

故 u 为 R 上的代数元.

□

定理 3.6

设 R 是交换幺环 $\widetilde{R}$ 的包含幺元 1 的子环. 又设 $u_1,u_2,\cdots,u_n\in\widetilde{R}$, 则 $\widetilde{R}$ 中包含 R 与 $u_1,u_2,\cdots,u_n$ 的最小子环为

$$R[u_1,u_2,\cdots,u_n]=\left\{\sum_{k_1k_2\cdots k_n}a_{k_1k_2\cdots k_n}u_1^{k_1}u_2^{k_2}\cdots u_n^{k_n}\middle|a_{k_1k_2\cdots k_n}\in R,a_{k_1k_2\cdots k_n}\text{ 中仅有限个不为}0\right\}$$

称为 R **添加** $u_1,u_2,\cdots,u_n$ **所得的环**.

♡

证明 记

$$S=\left\{\sum_{k_1,k_2,\ldots,k_n}a_{k_1k_2\cdots k_n}u_1^{k_1}u_2^{k_2}\cdots u_n^{k_n}\middle|a_{k_1k_2\cdots k_n}\in R,\text{仅有限个}a_{k_1k_2\cdots k_n}\neq 0\right\}.$$

首先, 证明 S 是 $\widetilde{R}$ 的子环. 设

$$x=\sum_{k_1,\ldots,k_n}a_{k_1\cdots k_n}u_1^{k_1}\cdots u_n^{k_n},\quad y=\sum_{k_1,\ldots,k_n}b_{k_1\cdots k_n}u_1^{k_1}\cdots u_n^{k_n}\in S,$$

则

$$x+y=\sum_{k_1,\ldots,k_n}(a_{k_1\cdots k_n}+b_{k_1\cdots k_n})u_1^{k_1}\cdots u_n^{k_n}.$$

由于 $a_{k_1\cdots k_n}$ 和 $b_{k_1\cdots k_n}$ 中仅有限个非零, 故 $a_{k_1\cdots k_n}+b_{k_1\cdots k_n}$ 中也仅有限个非零, 因此 $x+y\in S$. 并且有

$$-x\triangleq\sum_{k_1,\ldots,k_n}(-a_{k_1\cdots k_n})u_1^{k_1}\cdots u_n^{k_n}\in S,$$

使得 $x+(-x)=0$. 因此 S 对加法封闭且有加法逆元. 又因为 $\widetilde{R}$ 是交换幺环且 $S\subseteq\widetilde{R}$, 所以 S 对加法也有结合律和交换律. 故 S 对加法构成 Abel 群.

由于 $\widetilde{R}$ 交换, 有

$$xy=\left(\sum_{k_1,\ldots,k_n}a_{k_1\cdots k_n}u_1^{k_1}\cdots u_n^{k_n}\right)\left(\sum_{l_1,\ldots,l_n}b_{l_1\cdots l_n}u_1^{l_1}\cdots u_n^{l_n}\right)=\sum_{k_1,\ldots,k_n,l_1,\ldots,l_n}a_{k_1\cdots k_n}b_{l_1\cdots l_n}u_1^{k_1+l_1}\cdots u_n^{k_n+l_n}.$$

令 $m_i=k_i+l_i$, 则

$$xy=\sum_{m_1,\ldots,m_n}\left(\sum_{k_1+l_1=m_1,\ldots,k_n+l_n=m_n}a_{k_1\cdots k_n}b_{l_1\cdots l_n}\right)u_1^{m_1}\cdots u_n^{m_n}.$$

由于 $a_{k_1\cdots k_n}$ 和 $b_{l_1\cdots l_n}$ 中仅有限个非零, 故 $xy\in S$. 取 $a_{0\cdots0}=1\in R$, 其余系数为 0, 则 $1=1\cdot u_1^0\cdots u_n^0\in S$. 因此 S 对乘法封闭且含幺元. 又因为 $\widetilde{R}$ 是交换幺环且 $S\subseteq\widetilde{R}$, 所以 S 对乘法也有结合律和交换律. 故 S 对乘法构成交换幺半群. 由于 S 对加法和乘法封闭,$\widetilde{R}$ 为交换幺环且 $S\subseteq\widetilde{R}$, 故 S 的加法与乘法间自然满足分配律. 因此 S 是交换幺环 $\widetilde{R}$ 的子环.

其次, 证明 S 包含 R 和 $u_1,u_2,\cdots,u_n$. 对任意 $a\in R$, 取 $a_{0\cdots0}=a$, 其余系数为 0, 则 $a=a\cdot u_1^0\cdots u_n^0\in S$. 对每个 u_i, 取 $k_i=1$, 其余指数为 0, 且 $a_{0\cdots k_i\cdots0}=1$, 其余系数均为 0, 则 $u_i=1\cdot u_1^0\cdots u_i^1\cdots u_n^0\in S$.

最后, 证明 S 是包含 R 和 $u_1,u_2,\cdots,u_n$ 的最小子环. 设 T 是 $\widetilde{R}$ 的任意子环, 且 T 包含 R 和 $u_1,u_2,\cdots,u_n$. 由于 T 对乘法封闭, 对任意非负整数 $k_1,\ldots,k_n$, 有 $u_1^{k_1}\cdots u_n^{k_n}\in T$. 又因 T 包含 R, 对任意 $a_{k_1\cdots k_n}\in R$, 有 $a_{k_1\cdots k_n}u_1^{k_1}\cdots u_n^{k_n}\in T$. 再由 T 对加法封闭, 任意有限和 $\sum a_{k_1\cdots k_n}u_1^{k_1}\cdots u_n^{k_n}\in T$. 又 S 中元素均为此类有限和 (因系数仅有限个非零), 故 $S\subseteq T$. 因此 S 是包含 R 和 $u_1,u_2,\cdots,u_n$ 的最小子环.

综上,$S=R[u_1,u_2,\cdots,u_n]$ 即为所求.

□

定义 3.4

如果 R 中有有限多个 $a_{k_1k_2\cdots k_n}\neq 0$, 使

$$\sum_{k_1k_2\cdots k_n} a_{k_1k_2\cdots k_n}u_1^{k_1}u_2^{k_2}\cdots u_n^{k_n}=0,$$

则称 $u_1,u_2,\cdots,u_n$ 在 R 上是**代数相关**的, 否则称 $u_1,u_2,\cdots,u_n$ 在 R 上是**代数无关**的.

若 $u_1,u_2,\cdots,u_n$ 在 R 上是代数无关的, 则称 $R[u_1,u_2,\cdots,u_n]$ 为 R 上的 n **元多项式环**, 其元素称为 R 上的 n **元多项式**.

交换幺环 R 上的 n 元多项式环 $R[x_1,x_2,\cdots,x_n]$ 中, 形如 $ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}(a\in R,a\neq 0)$ 的元素称为一个**单项式**, a 称为此单项式的**系数**, $k_1+k_2+\cdots+k_n$ 称为此单项式的**次数**.

n 元多项式 $\sum\limits_{k_1k_2\cdots k_n} a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}\neq 0$ 的**次数**定义为所含单项式的最高次数, 即

$$\deg\left(\sum_{k_1k_2\cdots k_n} a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}\right)=\max\{k_1+k_2+\cdots+k_n\mid a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}\neq 0\}.$$

♣

定理 3.7

交换幺环 R 上的 n 元多项式环一定存在. 并且

$$R[x_1,x_2,\cdots,x_{n-1},x_n]=(R[x_1,x_2,\cdots,x_{n-1}])[x_n].$$

♡

证明 对 n 用数学归纳法证明. 当 $n=1$ 时, 由定理 3.4知本定理成立. 现设 $n-1$ 时本定理成立, 即有 R 上的 $n-1$ 元多项式环 $R[x_1,x_2,\cdots,x_{n-1}]$. 这也是交换幺环且

$$1\in R\subset R[x_1,x_2,\cdots,x_{n-1}].$$

再由定理 3.4, 可构造 $R[x_1,x_2,\cdots,x_{n-1}]$ 上的一元多项式环

$$(R[x_1,x_2,\cdots,x_{n-1}])[x_n]\supset R[x_1,x_2,\cdots,x_{n-1}]\supset R\ni 1.$$

显然有

$$R[x_1,x_2,\cdots,x_{n-1},x_n]\subseteq(R[x_1,x_2,\cdots,x_{n-1}])[x_n].$$

若 $f\in(R[x_1,x_2,\cdots,x_{n-1}])[x_n]$, 于是有 $f_0,f_1,\cdots,f_k\in R[x_1,x_2,\cdots,x_{n-1}]$, 使得

$$f=f_0+f_1x_n+\cdots+f_kx_n^k,$$

而

$$f_i=\sum_{k_1k_2\cdots k_{n-1}} a_{k_1k_2\cdots k_{n-1}i}x_1^{k_1}x_2^{k_2}\cdots x_{n-1}^{k_{n-1}}.$$

于是 $f\in R[x_1,x_2,\cdots,x_{n-1},x_n]$, 故知

$$R[x_1,x_2,\cdots,x_{n-1},x_n]=(R[x_1,x_2,\cdots,x_{n-1}])[x_n].$$

下面证明 $x_1,x_2,\cdots,x_{n-1},x_n$ 在 R 上是代数无关的. 假设 R 中有有限多个 $a_{k_1k_2\cdots k_n}\neq 0$, 使

$$\sum_{k_1k_2\cdots k_n} a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}=0.$$

记 $m\triangleq\max\{k_n:a_{k_1\cdots k_n}\neq 0\}$, 令

$$f_i=\sum_{k_1k_2\cdots k_{n-1}} a_{k_1k_2\cdots k_{n-1}i}x_1^{k_1}x_2^{k_2}\cdots x_{n-1}^{k_{n-1}},\quad 0\leqslant i\leqslant m,$$

则有 $f_i\in R[x_1,x_2,\cdots,x_{n-1}]$ 且满足 $\sum\limits_{i=0}^{m} f_ix_n^i=0$. 由于 x_n 是 $R[x_1,x_2,\cdots,x_{n-1}]$ 上的超越元, 故有 $f_i=0$, 即

$$\sum_{k_1k_2\cdots k_{n-1}} a_{k_1k_2\cdots k_{n-1}i}x_1^{k_1}x_2^{k_2}\cdots x_{n-1}^{k_{n-1}}=0,\quad 0\leqslant i\leqslant m.$$

由于 $x_1, x_2, \cdots, x_{n-1}$ 在 R 上是代数无关的, 故 $a_{k_1k_2\cdots k_{n-1}i} = 0$. 这样证明了 $R[x_1, x_2, \cdots, x_n]$ 是 R 上的 n 元多项式环.

□

定理 3.8

设 $R[x_1, x_2, \cdots, x_n]$ 是交换幺环 R 上的 n 元多项式环, S 是一个交换幺环, η 是 R 到 S 的环同态映射且 $\eta(1) = 1'$, 其中, $1, 1'$ 分别为 R, S 的幺元. 又设 $u_1, u_2, \cdots, u_n \in S$, 则 η 可唯一地开拓为 $R[x_1, x_2, \cdots, x_n]$ 到 S 的同态 η_n, 使得

$$\eta_n(x_i) = u_i, \quad i = 1, 2, \cdots, n.$$

即对 $\forall u_1, u_2, \cdots, u_n \in S$,$\eta$ 存在唯一的在 R 上的开拓 $\eta_u : R[x_1, x_2, \cdots, x_n] \to S$ 满足

$$\eta_n|_R = \eta, \quad \eta_n(x_i) = u_i, \quad i = 1, 2, \cdots, n.$$

且 η_n 是环同态.

♡

证明 事实上, η_n 可定义为

$$\eta_n\left(\sum_{k_1k_2\cdots k_n} a_{k_1k_2\cdots k_n} x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}\right) = \sum_{k_1k_2\cdots k_n} \eta(a_{k_1k_2\cdots k_n}) u_1^{k_1} u_2^{k_2} \cdots u_n^{k_n}.$$

不难验证 η_n 是 $R[x_1, x_2, \cdots, x_n]$ 到 S 的同态映射且 $\eta_n(x_i) = u_i (i = 1, 2, \cdots, n)$.

又若 η' 也满足此性质, 则

$$\begin{aligned}\eta'\left(\sum_{k_1k_2\cdots k_n} a_{k_1k_2\cdots k_n} x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}\right) &= \sum_{k_1k_2\cdots k_n} \eta'(a_{k_1k_2\cdots k_n}) \eta'(x_1)^{k_1} \eta'(x_2)^{k_2} \cdots \eta'(x_n)^{k_n} \\ &= \sum_{k_1k_2\cdots k_n} \eta(a_{k_1k_2\cdots k_n}) u_1^{k_1} u_2^{k_2} \cdots u_n^{k_n} \\ &= \eta_n\left(\sum_{k_1k_2\cdots k_n} a_{k_1k_2\cdots k_n} x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}\right).\end{aligned}$$

由此可知定理成立.

□

推论 3.6

交换幺环 R 上的任意两个 n 元多项式环是同构的.

♡

笔记 这个推论说明: 任何交换幺环上的 n 元多项式环在同构意义下唯一.

证明 设 $R[x_1, x_2, \cdots, x_n]$ 与 $R[y_1, y_2, \cdots, y_n]$ 为 R 上的两个 n 元多项式环. 令 i 为 R 到 $R[y_1, y_2, \cdots, y_n]$ 的嵌入映射, 满足 $i(a) = a (\forall a \in R)$. 容易验证 i 是 R 到 $R[y_1, y_2, \cdots, y_n]$ 的环同态映射. 由定理 3.8知, 可将 i 开拓为 $R[x_1, x_2, \cdots, x_n]$ 到 $R[y_1, y_2, \cdots, y_n]$ 上的同态 i_n, 使

$$i_n|_{R[x_1, x_2, \cdots, x_n]} = i, \quad i_n(x_k) = y_k (k = 1, 2, \cdots, n).$$

任取 $\sum_{k_1k_2\cdots k_n} a_{k_1k_2\cdots k_n} y_1^{k_1} y_2^{k_2} \cdots y_n^{k_n} \in R[y_1, y_2, \cdots, y_n]$, 则

$$i_n\left(\sum_{k_1k_2\cdots k_n} a_{k_1k_2\cdots k_n} x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}\right) = \sum_{k_1k_2\cdots k_n} a_{k_1k_2\cdots k_n} y_1^{k_1} y_2^{k_2} \cdots y_n^{k_n},$$

故 i_n 是满同态. 由 $y_1, y_2, \cdots, y_n$ 是 R 上代数无关的知 $\ker i_n = \{0\}$, 故由命题 1.21(2)(ii)知 i_n 也是单同态, 即 i_n 为同构映射.

□

推论 3.7

设 R 是交换幺环 $\widetilde{R}$ 的包含幺元 1 的子环, R 上的 n 元多项式环 $R[x_1,x_2,\cdots,x_n]$, 又 $u_1,u_2,\cdots,u_n\in\widetilde{R}$, 则有

(1) 存在 $R[x_1,x_2,\cdots,x_n]$ 中理想 I, 满足

$$R\cap I=\{0\},\quad R[u_1,u_2,\cdots,u_n]\cong R[x_1,x_2,\cdots,x_n]/I;$$

(2) $u_1,u_2,\cdots,u_n$ 代数相关当且仅当 $I\neq\{0\}$.

♡

证明

(1) 考虑 R 到 $R[u_1,u_2,\cdots,u_n]$ 的嵌入映射 i, 则不难验证 i 是 R 到 $R[u_1,u_2,\cdots,u_n]$ 上的环同态. 于是由定理 3.8知可将 i 开拓为环同态 $i_u:R[x_1,x_2,\cdots,x_n]\to R[u_1,u_2,\cdots,u_n]$ 满足

$$i_u|_R=i,\quad i_u(x_k)=u_k(k=1,2,\cdots,n).$$

注意到 $i_u(R[x_1,x_2,\cdots,x_n])=R[u_1,u_2,\cdots,u_n]$, 故 i_u 是满同态. 于是由命题 1.21(2)知 $I=\ker i_u$ 为 $R[x_1,x_2,\cdots,x_n]$ 的理想,$R[u_1,u_2,\cdots,u_n]\cong R[x_1,x_2,\cdots,x_n]/I$.

(2) 若 $a\in R\cap I$, 则 $0=i_u(a)=i(a)=a$, 故 $R\cap I=\{0\}$. 由于 $u_1,u_2,\cdots,u_n$ 代数相关当且仅当存在有限多个 $a_{k_1k_2\cdots k_n}\neq0$, 使

$$\sum_{k_1k_2\cdots k_n}a_{k_1k_2\cdots k_n}u_1^{k_1}u_2^{k_2}\cdots u_n^{k_n}=0.$$

这也当且仅当

$$i_u\left(\sum_{k_1k_2\cdots k_n}a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}\right)=\sum_{k_1k_2\cdots k_n}a_{k_1k_2\cdots k_n}u_1^{k_1}u_2^{k_2}\cdots u_n^{k_n}=0$$

$$\Longleftrightarrow 0\neq\sum_{k_1k_2\cdots k_n}a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}\in I\Longleftrightarrow I\neq\{0\}.$$

□

推论 3.8

设 R 是交换幺环, $R[x_1,x_2,\cdots,x_n]$ 是 R 上 n 元多项式环, I 为 $R[x_1,x_2,\cdots,x_n]$ 的理想且 $R\cap I=\{0\}$, $I\neq\{0\}$, 则 $R[x_1,x_2,\cdots,x_n]/I$ 是 R 添加 n 个代数相关元所得的环.

♡

证明 设 π 是 $R[x_1,x_2,\cdots,x_n]$ 到 $R[x_1,x_2,\cdots,x_n]/I$ 的自然同态, 于是 $\pi(R)$ 是 $R[x_1,x_2,\cdots,x_n]/I$ 中的子环. 由定理 1.20(3)知 I 也是 R 的理想, 从而再由定理 1.43(3)知

$$\pi(R)=R/I=(R+I)/I\cong R/(R\bigcap I)=R/\{0\}=R+0=R,$$

故可将 R 视为 $R[x_1,x_2,\cdots,x_n]/I$ 的子环, 令 $u_i=\pi(x_i)(i=1,2,\cdots,n)$, 则 $u_i\in R[x_1,x_2,\cdots,x_n]/I$, 于是

$$R[u_1,u_2,\cdots,u_n]\subseteq R[x_1,x_2,\cdots,x_n]/I,$$

. 注意到

$$\pi\left(\sum_{k_1k_2\cdots k_n}a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}\right)=\sum_{k_1k_2\cdots k_n}\pi\left(a_{k_1k_2\cdots k_n}\right)u_1^{k_1}u_2^{k_2}\cdots u_n^{k_n},$$

故再结合 π 是满同态可得

$$R[x_1,x_2,\cdots,x_n]/I=\pi(R[x_1,x_2,\cdots,x_n])\subseteq R[u_1,u_2,\cdots,u_n]\subseteq R[x_1,x_2,\cdots,x_n]/I,$$

即 $R[x_1,x_2,\cdots,x_n]/I=R[u_1,u_2,\cdots,u_n]$. 又由 $I\neq\{0\}$, 故 I 中有非零元素

$$\sum_{k_1k_2\cdots k_n}a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n},$$

其中有有限多个 $a_{k_1k_2\cdots k_n}\neq 0$. 而

$$\pi\left(\sum_{k_1k_2\cdots k_n}a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}\right)=\sum_{k_1k_2\cdots k_n}a_{k_1k_2\cdots k_n}u_1^{k_1}u_2^{k_2}\cdots u_n^{k_n}=0.$$

又因为 $\pi(R)\cong R$, 所以上式有有限个 $\pi(a_{k_1k_2\cdots k_n})\neq 0$. 故 $u_1,u_2,\cdots,u_n$ 是代数相关的.

□

3.3 对称多项式

定义 3.5

设 R 是一个交换幺环,$R[x_1,x_2,\cdots,x_n]$ 是 R 上的 n 元多项式环. 如果 $R[x_1,x_2,\cdots,x_n]$ 中的 n 元多项式 $f(x_1,x_2,\cdots,x_n)$ 中非零单项式都是 k 次的, 那么称 $f(x_1,x_2,\cdots,x_n)$ 为一个**k 次齐次多项式**.

♣

注 显然任意两个齐次多项式的乘积仍是齐次多项式.

定理 3.9 (齐次多项式分解)

设 R 是一个交换幺环,$R[x_1,x_2,\cdots,x_n]$ 是 R 上的 n 元多项式环. $f(x_1,x_2,\cdots,x_n)$ 是 $R[x_1,x_2,\cdots,x_n]$ 中的 n 元多项式且 $\deg f=m$, 则存在 m 个齐次多项式 $f_1,f_2,\cdots,f_m$, 使得

$$f=f_0+f_1+\cdots+f_m.$$

且上述分解 (除所含零外) 是唯一的.

♡

证明 若 $f(x_1,x_2,\cdots,x_n)=0$, 则 $\deg f=0$, 取 $f_0=f=0$ 即可.

若 $f(x_1,x_2,\cdots,x_n)\neq 0$, 则有

$$f(x_1,x_2,\cdots,x_n)=\sum_{k_1k_2\cdots k_n}a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}=\sum_{k=0}^{m}\left(\sum_{k_1+k_2+\cdots+k_n=k}a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}\right),$$

其中, 当 $k\geqslant 1$ 时, 令

$$f_k(x_1,x_2,\cdots,x_n)=\sum_{k_1+k_2+\cdots+k_n=k}a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n},$$

这是一个 k 次齐次多项式或零,$f_0\in R$. 于是

$$f=f_0+f_1+\cdots+f_m.$$

设存在另外 m 个齐次多项式 $f_0',f_1',\cdots,f_m'$, 使得

$$f=f_0'+f_1'+\cdots+f_m'.$$

令 $h_k=f_k-f_k'(k=0,1,\cdots,m)$, 则由 f_k,f_k' 的齐次性知 $\deg h_k=k$或0. 并且

$$h_0+h_1+\cdots+h_m=(f_0-f_0')+(f_1-f_1')+\cdots+(f_m-f_m')=0.$$

因此 $\deg(h_0+h_1+\cdots+h_m)=\max\limits_{k=0,1,\cdots,k}\{\deg h_k\}=0$. 故 $\deg h_k=0\,(k=0,1,\cdots,m)$, 即 $f_k=f_k'\,(k=0,1,\cdots,m)$. 故上述分解 (除所含零外) 是唯一的.

□

定义 3.6 (单项式的字典排序法)

设 R 是交换幺环,$R[x_1,x_2,\cdots,x_n]$ 是 R 上的 n 元多项式环,$ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n},bx_1^{l_1}x_2^{l_2}\cdots x_n^{l_n}$ 是两个非零单项式. 若有 s, 使得

$$k_i=l_i,\ i=1,2,\cdots,s,\quad k_{s+1}>l_{s+1},$$

则称 $ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ 高于 $bx_1^{l_1}x_2^{l_2}\cdots x_n^{l_n}$, 记为

$$ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n} > bx_1^{l_1}x_2^{l_2}\cdots x_n^{l_n}.$$

♣

笔记 例如, 当 $n=3$ 时, 有 $x_1^3x_2x_3^5 > x_1^3x_3^6 > x_1x_3^5$.

定理 3.10 (单项式的字典排序法的基本性质)

设 R 是交换幺环,$R[x_1,x_2,\cdots,x_n]$ 是 R 上的 n 元多项式环,$ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$,$bx_1^{l_1}x_2^{l_2}\cdots x_n^{l_n}$ 是两个非零单项式.

(1) **传递性:** 若

$$ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n} > bx_1^{l_1}x_2^{l_2}\cdots x_n^{l_n},\quad bx_1^{l_1}x_2^{l_2}\cdots x_n^{l_n} > cx_1^{m_1}x_2^{m_2}\cdots x_n^{m_n},$$

则

$$ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n} > cx_1^{m_1}x_2^{m_2}\cdots x_n^{m_n}.$$

(2) 若 $ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n} > bx_1^{l_1}x_2^{l_2}\cdots x_n^{l_n}$, 则有

$$ax_1^{k_1+m_1}x_2^{k_2+m_2}\cdots x_n^{k_n+m_n} > bx_1^{l_1+m_1}x_2^{l_2+m_2}\cdots x_n^{l_n+m_n}.$$

(3) 设 $f,g\in R[x_1,x_2,\cdots,x_n]$ 且 $f\neq 0, g\neq 0$. 若 f 的最高项与 g 的最高项之积不为 0, 则此积为 $f\cdot g$ 的最高项.

如果 f 与 g 的最高项系数之一为 R 中非零因子, 则 fg 的最高项为 f 的最高项与 g 的最高项之积.

特别地, 当 R 是交换整环且 f,g 为 $R[x_1,x_2,\cdots,x_n]$ 中非零元素时,fg 的最高项为 f 的最高项与 g 的最高项的乘积.

♡

证明

(1)

(2)

(3)

□

定理 3.11

设 R 是交换幺环,$R[x_1,x_2,\cdots,x_n]$ 是 R 上的 n 元多项式环, 对 n 个文字的对称群 S_n 中任一元素 π,π^{-1} 为 π 在 S_n 中的逆元, 则存在 $R[x_1,x_2,\cdots,x_n]$ 中的自同构满足

$$\pi'(a)=a,\forall a\in R,\quad \pi'(x_i)=x_{\pi(i)},i=1,2,\cdots,n.$$

且对任意

$$f=\sum_{k_1k_2\cdots k_n}a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}\in R[x_1,x_2,\cdots,x_n],$$

有

$$(\pi' f)(x_1,x_2,\cdots,x_n)=\sum_{k_1k_2\cdots k_n}a_{k_{\pi(1)}k_{\pi(2)}\cdots k_{\pi(n)}}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}.$$

并且 $\{\pi' \mid \pi\in S_n\}$ 是 $R[x_1,x_2,\cdots,x_n]$ 的自同构群的子群.

若 $f\in R[x_1,x_2,\cdots,x_n]$ 满足

$$\pi' f=f,\quad \forall\pi\in S_n,$$

则称 f 为 $x_1,x_2,\cdots,x_n$ 的一个**对称多项式**.

♡

证明 令 i 为 R 到 $R[y_1,y_2,\cdots,y_n]$ 的嵌入映射, 满足 $i(a)=a(\forall a\in R)$. 容易验证 i 是 R 到 $R[y_1,y_2,\cdots,y_n]$ 的环同

态映射. 由定理 3.8可将 i 开拓为 $R[x_1,x_2,\cdots,x_n]$ 的一个自同态 π'(在定理 3.8中取 $u_i=x_{\pi(i)}$) 满足

$$\pi'(a)=a,\forall a\in R,\quad \pi'(x_i)=x_{\pi(i)},i=1,2,\cdots,n.$$

显然, 对 $f=\sum\limits_{k_1k_2\cdots k_n}a_{k_1k_2\cdots k_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ 有

$$\begin{aligned}(\pi' f)(x_1,x_2,\cdots,x_n)&=\sum_{k_1k_2\cdots k_n}a_{k_1k_2\cdots k_n}x_{\pi(1)}^{k_1}x_{\pi(2)}^{k_2}\cdots x_{\pi(n)}^{k_n}\\&=\sum_{k_1k_2\cdots k_n}a_{k_1k_2\cdots k_n}x_1^{k_{\pi^{-1}(1)}}x_2^{k_{\pi^{-1}(2)}}\cdots x_n^{k_{\pi^{-1}(n)}}\\&\xlongequal[k_i=k_{\pi^{-1}(\pi(i))}=t_{\pi(i)}]{t_i=k_{\pi^{-1}(i)}}\sum_{t_1t_2\cdots t_n}a_{t_{\pi(1)}t_{\pi(2)}\cdots t_{\pi(n)}}x_1^{t_1}x_2^{t_2}\cdots x_n^{t_n}\\&=\sum_{k_1k_2\cdots k_n}a_{k_{\pi(1)}k_{\pi(2)}\cdots k_{\pi(n)}}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}.\end{aligned}$$

同理, 由定理 3.8可将 i 开拓为 $R[x_1,x_2,\cdots,x_n]$ 的一个自同态 $\left(\pi^{-1}\right)'$(在定理 3.8中取 $u_i=x_{\pi^{-1}(i)}$) 满足

$$\left(\pi^{-1}\right)'(a)=a,\forall a\in R,\quad \left(\pi^{-1}\right)'(x_i)=x_{\pi^{-1}(i)},i=1,2,\cdots,n.$$

从而

$$\begin{aligned}\left(\pi^{-1}\right)'\pi'(a)=a,\forall a\in R,\quad \left(\pi^{-1}\right)'\pi'(x_i)=\left(\pi^{-1}\right)'\left(x_{\pi(i)}\right)=x_{\pi^{-1}\pi(i)}=x_i,i=1,2,\cdots,n,\\ \pi'\left(\pi^{-1}\right)'(a)=a,\forall a\in R,\quad \pi'\left(\pi^{-1}\right)'(x_i)=\pi'\left(x_{\pi^{-1}(i)}\right)=x_{\pi\pi^{-1}(i)}=x_i,i=1,2,\cdots,n,\end{aligned}$$

即 $\left(\pi^{-1}\right)'\pi'=\pi'\left(\pi^{-1}\right)'=\mathrm{id}_{R[x_1,x_2,\cdots,x_n]}$. 因此 π' 是双射,$(\pi^{-1})'$ 为其逆映射. 故 π' 是 $R[x_1,x_2,\cdots,x_n]$ 的一个自同构.

由上述证明知 $\forall\pi'\in\{\pi'\mid\pi\in S_n\}$, 都存在逆元 $(\pi^{-1})'$.

对 $\forall\pi_1',\pi_2'\in\{\pi'\mid\pi\in S_n\}$, 则由

$$\begin{aligned}\pi_1'\pi_2'(a)=a=(\pi_1\pi_2)'(a),\quad \forall a\in R,\\ \pi_1'\pi_2'(x_i)=\pi_1'(x_{\pi_2(i)})=x_{\pi_1\pi_2(i)}=(\pi_1\pi_2)'(x_i),\quad i=1,2,\cdots,n\end{aligned}$$

知 $\pi_1'\pi_2'=(\pi_1\pi_2)'\in\{\pi'\mid\pi\in S_n\}$. 故 $\{\pi'\mid\pi\in S_n\}$ 对乘法封闭. 由映射的乘积必满足结合律知 $\{\pi'\mid\pi\in S_n\}$ 对乘法也满足结合律.

对 S_n 中的幺元 id 有 $(\mathrm{id})'=\mathrm{id}_{R[x_1,x_2,\cdots,x_n]}$ 也是 $\{\pi'\mid\pi\in S_n\}$ 的幺元.

综上可知 $\{\pi'\mid\pi\in S_n\}$ 是 $R[x_1,x_2,\cdots,x_n]$ 的自同构群的子群.

□

引理 3.1

设 R 是交换幺环,$R[x_1,x_2,\cdots,x_n]$ 是 R 上的 n 元多项式环,$R[x_1,x_2,\cdots,x_n]$ 中的多项式

$$\begin{aligned}s_1&=x_1+x_2+\cdots+x_n,\\ s_2&=x_1^2+x_2^2+\cdots+x_n^2,\\ &\cdots\cdots\\ s_m&=x_1^m+x_2^m+\cdots+x_n^m\end{aligned}$$

都是对称多项式, 称为 **Newton 对称幂和**或**等幂和**.

♡

证明

□

引理 3.2

设 R 是交换幺环,$R[x_1,x_2,\cdots,x_n]$ 是 R 上的 n 元多项式环,$R[x_1,x_2,\cdots,x_n]$ 中的多项式

$$\begin{aligned}
p_1 &= s_1 = x_1 + x_2 + \cdots + x_n,\\
p_2 &= \sum_{1\leqslant i<j\leqslant n} x_i x_j = x_1x_2 + \cdots + x_1x_n + x_2x_3 + \cdots + x_2x_n + \cdots + x_{n-1}x_n,\\
&\cdots\cdots\\
p_{n-1} &= \sum_{1\leqslant j_1<j_2<\cdots<j_{n-1}\leqslant n} x_{j_1}x_{j_2}\cdots x_{j_{n-1}},\\
p_n &= x_1x_2\cdots x_n.
\end{aligned}$$

等 n 个齐次多项式都是对称多项式, 称它们为 n **元初等对称多项式**.

♡

证明 令 $p_0 = 1$. 考虑 $R[x_1,x_2,\cdots,x_n] = S$ 上的一元多项式环 $S[x]$ 中的元素

$$g(x) = \prod_{i=1}^{n}(x - x_i) = \sum_{k=0}^{n}(-1)^k p_k x^{n-k} = x^n - p_1x^{n-1} + \cdots + (-1)^{n-1}p_{n-1}x + (-1)^n p_n. \tag{3.9}$$

设 $\pi \in S_n$, 由定理 3.11知存在 $R[x_1,x_2,\cdots,x_n]$ 中的自同构 π' 满足

$$\pi'(a) = a, \forall a \in R, \quad \pi'(x_i) = x_{\pi(i)}, i = 1,2,\cdots,n.$$

于是

$$g(x) = \prod_{i=1}^{n}(x - x_{\pi(i)}) = \sum_{k=0}^{n}(-1)^k(\pi' p_k)x^{n-k}, \tag{3.10}$$

故比较(3.9)式和(3.10)式系数知 $\pi' p_k = p_k (0 \leqslant k \leqslant n)$, 即 $p_1, p_2, \cdots, p_n$ 是对称多项式.

□

引理 3.3

设 R 是交换幺环,$R[x_1,x_2,\cdots,x_n]$ 是 R 上的 n 元多项式环, 以 Σ 表示 $R[x_1,x_2,\cdots,x_n]$ 中所有对称多项式的集合, 则 Σ 是 $R[x_1,x_2,\cdots,x_n]$ 的子环且 $\Sigma \supseteq R$. 又若 $f \in R[x_1,x_2,\cdots,x_n]$, 且有齐次多项式分解

$$f = f_0 + f_1 + \cdots + f_k,$$

则 $f \in \Sigma$ 当且仅当 $f_i \in \Sigma (0 \leqslant i \leqslant k)$.

♡

证明 显然 $\Sigma \supseteq R$. 又若 $f, g \in \Sigma, \pi \in S_n$, 则由定理 3.11知存在 $R[x_1,x_2,\cdots,x_n]$ 中的自同构 π' 满足

$$\pi'(a) = a, \forall a \in R, \quad \pi'(x_i) = x_{\pi(i)}, i = 1,2,\cdots,n.$$

于是

$$\begin{aligned}
\pi'(f - g) &= \pi'(f) - \pi'(g) = f - g,\\
\pi'(fg) &= \pi'(f)\pi'(g) = fg,
\end{aligned}$$

因此 $f - g, fg \in \Sigma$, 故 Σ 是一个子环.

又若 $f \in R[x_1,x_2,\cdots,x_n]$, 设 $f = \sum_{i=0}^{k} f_i$ 为 f 的齐次多项式分解,$\pi \in S_n$, 则 $\pi' f = \sum_{i=0}^{k} \pi' f_i$ 为 $\pi' f$ 的齐次多项式分解. 因齐次多项式分解唯一, 故

$$\pi' f = f \iff \pi' f_i = f_i,\ 0 \leqslant i \leqslant k.$$

□

定理 3.12 (对称多项式基本定理)

设 R 是交换幺环,Σ 是 R 上 n 元多项式 $R[x_1,x_2,\cdots,x_n]$ 中对称多项式构成的子环,$p_1,p_2,\cdots,p_n$ 为初等对称多项式, 则

(1) $\Sigma=R[p_1,p_2,\cdots,p_n]$;

(2) $p_1,p_2,\cdots,p_n$ 在 R 上是代数无关的, 即 $R[p_1,p_2,\cdots,p_n]$ 也是 R 上的 n 元多项式环. ♡

注

1. 这个定理的等价命题是**任一对称多项式可唯一地表示为初等对称多项式的多项式**.
2. 这个定理 (1) 的证明实际上给出了一个对称多项式如何表示为初等对称多项式的多项式的有效办法.

证明

(1) 由 $p_1,p_2,\cdots,p_n\in\Sigma$ 和 Σ 是环知 $R[p_1,p_2,\cdots,p_n]\subseteq\Sigma$. 下证 $R[p_1,p_2,\cdots,p_n]\supseteq\Sigma$. 只需证明任一齐次对称多项式 $f\in R[p_1,p_2,\cdots,p_n]$. 假设已经证明, 则对任意 $f\in\Sigma$, 由引理 3.3知 f 有齐次多项式分解 $f=f_0+f_1+\cdots+f_k$ 且 $f_i\in\Sigma(0\leqslant i\leqslant k)$, 即 $f_i(0\leqslant i\leqslant k)$ 都是齐次对称多项式. 于是有假设知 $f_i\in R[p_1,p_2,\cdots,p_n](0\leqslant i\leqslant k)$, 进而 $f\in R[p_1,p_2,\cdots,p_n]$, 故 $R[p_1,p_2,\cdots,p_n]\supseteq\Sigma$.

设 f 是 m 次齐次对称多项式. 按字典序,f 的最高项为 $ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$, 则必有

$$k_1\geqslant k_2\geqslant\cdots\geqslant k_n,\quad k_1+k_2+\cdots+k_n=m.$$

若不然, 设有 i, 使得 $k_i<k_{i+1}$. 于是有 $\pi\in S_n$, 使得

$$\pi(j)=\begin{cases}j, & j\neq i,i+1,\\ i+1, & j=i,\\ i, & j=i+1.\end{cases}$$

由定理 3.11知存在 $R[x_1,x_2,\cdots,x_n]$ 中的自同构 π' 满足

$$\pi'(a)=a,\forall a\in R,\quad \pi'(x_i)=x_{\pi(i)},i=1,2,\cdots,n.$$

由 f 是对称多项式知 $\pi'f=f$. 从而 f 中有一项为 $\pi'(ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n})$, 但

$$\pi'(ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n})=ax_1^{k_1}\cdots x_i^{k_{i+1}}x_{i+1}^{k_i}\cdots x_n^{k_n}>ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}.$$

这与 $ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ 为 f 的最高项矛盾.

令 $d_i=k_i-k_{i+1}(1\leqslant i\leqslant n-1)$ 且 $d_n=k_n$. 由 p_i 的最高项为 $x_1x_2\cdots x_i$ 及定理 3.10(3)知 $p_1^{d_1}p_2^{d_2}\cdots p_n^{d_n}$ 的最高项为

$$x_1^{d_1}(x_1x_2)^{d_2}\cdots(x_1x_2\cdots x_n)^{d_n}=x_1^{d_1+d_2+\cdots+d_n}(x_2)^{d_2+\cdots+d_n}\cdots(x_n)^{d_n}=x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}.$$

由此知 m 次齐次对称多项式 $f_1=f-ap_1^{d_1}p_2^{d_2}\cdots p_n^{d_n}$ 的最高项 $bx_1^{l_1}x_2^{l_2}\cdots x_n^{l_n}<ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ 且

$$l_1\geqslant l_2\geqslant\cdots\geqslant l_n,\quad l_1+l_2+\cdots+l_n=m.$$

否则同理可得矛盾! 类似可知 m 次齐次对称多项式 $f_2=f_1-bp_1^{l_1-l_2}p_2^{l_2-l_3}\cdots p_n^{l_n}$ 的最高项 $cx_1^{m_1}x_2^{m_2}\cdots x_n^{m_n}<bx_1^{l_1}x_2^{l_2}\cdots x_n^{l_n}$ 且

$$m_1\geqslant m_2\geqslant\cdots\geqslant m_n,\quad m_1+m_2+\cdots+m_n=m.$$

由于满足 $k_1\geqslant k_2\geqslant\cdots\geqslant k_n\geqslant0$ 和 $k_1+k_2+\cdots+k_n=m$ 的 n 重数组 $(k_1,k_2,\cdots,k_n)$ 只有有限个, 故有限步后可得

$$f=ap_1^{d_1}p_2^{d_2}\cdots p_n^{d_n}+bp_1^{l_1-l_2}p_2^{l_2-l_3}\cdots p_n^{l_n}+\cdots+cp_1^{t_1}p_2^{t_2}\cdots p_n^{t_n},$$

即 $f\in R[p_1,p_2,\cdots,p_n]$, 所以 $\Sigma=R[p_1,p_2,\cdots,p_n]$.

(2) 由 (1) 可知 $p_1^{d_1}p_2^{d_2}\cdots p_n^{d_n}$ 的最高项为

$$x_1^{d_1+d_2+\cdots+d_n}(x_2)^{d_2+\cdots+d_n}\cdots(x_n)^{d_n},$$

因而由

$$d_i = c_i,\ 1 \leqslant i \leqslant n \iff \sum_{j=i}^{n} d_j = \sum_{j=i}^{n} c_j,\ 1 \leqslant i \leqslant n$$

知 $p_1^{d_1}p_2^{d_2}\cdots p_n^{d_n} = p_1^{c_1}p_2^{c_2}\cdots p_n^{c_n}$ 当且仅当它们的最高项相同. 假设有有限个 $a_{d_1d_2\cdots d_n} \neq 0$ 而使

$$\sum_{d_1d_2\cdots d_n} a_{d_1d_2\cdots d_n} p_1^{d_1}p_2^{d_2}\cdots p_n^{d_n} = 0. \tag{3.11}$$

因为上式中每一项都不相同, 所以由之前的证明知, 上式中每一项 $p_1^{d_1}p_2^{d_2}\cdots p_n^{d_n}$ 的最高项都互不相同. 取所有系数不为 0 的 $p_1^{d_1}p_2^{d_2}\cdots p_n^{d_n}$ 的最高项的所有 x_i 的幂之和最大数为

$$m = \max\left\{ \sum_{j=1}^{n} jd_j = \sum_{i=1}^{n}\sum_{j=i}^{n} d_j = (d_1 + d_2 + \cdots + d_n) + (d_2 + \cdots + d_n) + \cdots + d_n \middle| a_{d_1d_2\cdots d_n} \neq 0 \right\}.$$

再取

$$\left\{ x_1^{l_1}x_2^{l_2}\cdots x_n^{l_n} \middle| l_i = \sum_{j=i}^{n} d_j, \sum_{i=1}^{n} l_i = \sum_{j=1}^{n} jd_j = m, a_{d_1\cdots d_n} \neq 0 \right\}$$

中的最高项是 $x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$, 其中 $k_i = \sum_{j=i}^{n} c_j$. 由此知在 (3.11) 式的左边含有一项 $a_{c_1c_2\cdots c_n}x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n} \neq 0$, 故 (3.11) 式左边不为零, 而右边为零, 矛盾! 因而知 $p_1, p_2, \cdots, p_n$ 在 R 上是代数无关的.

□

例题 3.5 将对称多项式

$$f(x_1, x_2, \cdots, x_n) = \sum_{1\leqslant j_1<j_2<j_3\leqslant n} \left(x_{j_1}^2x_{j_2}^2x_{j_3} + x_{j_1}^2x_{j_2}x_{j_3}^2 + x_{j_1}x_{j_2}^2x_{j_3}^2\right)$$

表为初等对称多项式的多项式.

解 f 是一个 5 次齐次对称多项式, 首项是 $x_1^2x_2^2x_3$, 因而满足

$$k_1 \geqslant k_2 \geqslant \cdots \geqslant k_n, \quad \sum_{i=1}^{n} k_i = 5$$

且 $x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n} < x_1^2x_2^2x_3$ 的项只有 $x_1^2x_2x_3x_4, x_1x_2x_3x_4x_5$. 因而由对称多项式基本定理 (1) 的证明有

$$\begin{aligned} f(x_1, x_2, \cdots, x_n) &= p_1^{2-2}p_2^{2-1}p_3 + Ap_1^{2-1}p_2^{1-1}p_3^{1-1}p_4^1 + Bp_1^{1-1}p_2^{1-1}p_3^{1-1}p_4^{1-1}p_5^1 \\ &= p_2p_3 + Ap_1p_4 + Bp_5, \end{aligned}$$

其中, A, B 是待定系数. 取

$$x_i = \begin{cases} 1, & 1 \leqslant i \leqslant 4, \\ 0, & i \geqslant 5, \end{cases}$$

则有 $p_1 = 4, p_2 = C_4^2 = 6, p_3 = C_4^3 = 4, p_4 = 1$, 而 $f = 3 \times C_4^3 = 12$, 故有 $12 = 24 + 4A$, 即 $A = -3$. 又取

$$x_i = \begin{cases} 1, & 1 \leqslant i \leqslant 5, \\ 0, & i \geqslant 6, \end{cases}$$

则 $p_1 = 5, p_2 = C_5^2, p_3 = C_5^3, p_4 = C_5^4, p_5 = 1$. 而 $f = 3 \times C_5^3 = 30$, 故有 $30 = 100 - 3 \times 25 + B$, 即 $B = 5$. 最后得 $f(x_1, x_2, \cdots, x_n) = p_2p_3 - 3p_1p_4 + 5p_5$.

□

例题 3.6 对 $j_1 \geqslant j_2 \geqslant \cdots \geqslant j_n$, 记

$$s(x_1^{j_1}x_2^{j_2}\cdots x_n^{j_n}) = \sum_{\pi\in S_n} x_{\pi(1)}^{j_1}x_{\pi(2)}^{j_2}\cdots x_{\pi(n)}^{j_n},$$

如

$$s(x_1^k)=\sum_{\pi\in S_n}x_{\pi(1)}^k=x_1^k+x_2^k+\cdots+x_n^k,$$
$$s(x_1^2x_2^2)=\sum_{\pi\in S_n}x_{\pi(1)}^2x_{\pi(2)}^2=\sum_{1\leqslant j_1<j_2\leqslant n}x_{j_1}^2x_{j_2}^2,$$

则 $s(x_1^{j_1}x_2^{j_2}\cdots x_n^{j_n})$ 是对称多项式.

证明

□

定理 3.13 (Newton 公式)

等幂和 $s_k=\sum_{i=1}^n x_i^k$ 与初等对称多项式 p_i 有下列关系:

(1) 当 $k\leqslant n$ 时,

$$s_k-s_{k-1}p_1+\cdots+(-1)^{k-1}s_1p_{k-1}+(-1)^k kp_k=0; \tag{3.12}$$

(2) 当 $k>n$ 时,

$$s_k-s_{k-1}p_1+s_{k-2}p_2-\cdots+(-1)^n s_{k-n}p_n=0. \tag{3.13}$$

♡

证明 用例题 3.6的符号, 显然有

$$\begin{cases} s_{k-1}p_1=s_k+s(x_1^{k-1}x_2),\\ -s_{k-2}p_2=-s(x_1^{k-1}x_2)-s(x_1^{k-2}x_2x_3),\\ \cdots\cdots\\ (-1)^{j-1}s_{k-j}p_j=(-1)^{j-1}s(x_1^{k-j+1}x_2\cdots x_j)+(-1)^{j-1}s(x_1^{k-j}x_2\cdots x_jx_{j+1}),\\ \cdots\cdots \end{cases} \tag{3.14}$$

且当 $k\leqslant n$ 时,

$$(-1)^{k-2}s_1p_{k-1}=(-1)^{k-2}s(x_1^2x_2\cdots x_{k-1})+(-1)^{k-2}kp_k. \tag{3.15}$$

当 $k>n$ 时,

$$(-1)^{n-1}s_{k-n}p_n=(-1)^{n-1}s(x_1^{k-n+1}x_2\cdots x_n). \tag{3.16}$$

当 $k\leqslant n$ 时, 将联立式 (3.14) 中各式及式 (3.15) 相加得

$$s_{k-1}p_1-s_{k-2}p_2+\cdots+(-1)^{k-2}s_1p_{k-1}=s_k+(-1)^k kp_k,$$

即式 (3.12) 成立.

当 $k>n$ 时, 将联立式 (3.14) 中各式及式 (3.16) 相加得

$$s_{k-1}p_1-s_{k-2}p_2+\cdots+(-1)^{n-1}s_{k-n}p_n=s_k,$$

即式 (3.13) 成立.

□

3.4 唯一析因环 (唯一分解整环)

因本节讨论并未用到 R 中的加法, 因而可以认为 R^* 是满足消去律的幺半群. 因此, 可定义**唯一析因幺半群** (或 **Gauss 幺半群**). 引理 3.5, 引理 3.6与定理 3.20对 Gauss 幺半群也成立.

定理 3.14

设 R 是交换整环, 由命题 1.11(1)知 $R^*=R\setminus\{0\}$ 对乘法构成交换幺半群且消去律成立. 以 U 表示 R^* 中乘法可逆元素的集合, 则 U 对乘法构成一个 Abel 群, 称为 R 的**单位群**. U 中元素称为 R 的**单位**.

证明

□

定义 3.7 (整数)

设 R 是交换整环,$R^*=R\setminus\{0\}, a,b\in R^*$, 若 $\exists c\in R^*$, 使 $b=ac$, 则称 a 能**整除** b, 或 a 是 b 的**因子**, 或 b 是 a 的**倍式**. 记为 $a|b$. a 不能整除 b, 记为 $a\nmid b$. 在 R 中约定 $a|0,\forall a\in R$.

定义 3.8 (相伴)

设 R 是交换整环,$R^*=R\setminus\{0\}, a,b\in R^*$, 且 $a|b,b|a$, 则称 a 与 b **相伴**, 记为 $a\sim b$.

定理 3.15

设 R 是交换整环,$R^*=R\setminus\{0\}, a,b,c\in R^*$, U 表示 R^* 中乘法可逆元素的集合, 则

(1) $a|a,\forall a\in R^*$.

(2) 若 $a|b,b|c$, 则 $a|c$.

(3) $a\sim b$ 的充要条件是 $ac\sim bc$.

(4) 若 $u\in U$, 则 $u|a,\forall a\in R^*$.

(5) $u\in U\iff u|1$.

(6) $a\sim b\iff\exists u\in U$, 使$b=au\iff\langle a\rangle=\langle b\rangle$.

(7) 相伴关系是乘法幺半群 R^* 中的同余关系.

(8) $u\in U\iff u\sim 1$.

(9) 若 $a|b,a|c$, 则 $a|(xb+yc),\forall x,y\in R$.

证明

(1) 这是因为 $a=1\cdot a$.

(2) 由 $b=ad,c=be$ 得 $c=a(de)$.

(3) **必要性**: 由 $a\sim b$ 知 $b=ad,a=be(d,e\in R)$, 于是 $bc=adc,ac=bec$, 故 $ac\mid bc,bc\mid ac$, 即 $ac\sim bc$.
充分性: 由 $ac\sim bc$ 知 $ac=dbc,bc=eac(d,e\in R)$. 由命题 1.11(1)知 R^* 对乘法满足消去律, 故 $a=db,b=ea$, 因此 $a\sim b$.

(4) 这是因为 $a=u(u^{-1}a)$.

(5) 由性质 (4)知 $u\in U$ 时,$u|1$. 反之, 若 $u|1$, 即有 v, 使得 $1=vu$, 故 $v=u^{-1}(u\in U)$. 再利用定理 1.22(3)可得

$$\langle b\rangle=bR=auR\overset{\text{定理 1.22(3)}}{=\!=\!=}aR=\langle a\rangle.$$

(6) 事实上, 若 $b=au(u\in U)$, 则 $a=bu^{-1}$. 因而 $a|b,b|a$, 即 $a\sim b$.
反之, 若 $a|b,b|a$, 即有 $c,d\in R^*$, 使得 $b=ac,a=bd$. 于是 $b=b(dc)$. 由命题 1.11(1)知 R^* 对乘法满足消去律, 故 $dc=1$, 因而 $d,c\in U$.

(7) 相伴关系显然是等价关系. 设 $a\sim b,c\sim d$. 于是 $\exists u_1,u_2\in U$, 使得 $b=au_1,d=cu_2$. 于是 $bd=ac(u_1u_2)$. 由 $u_1u_2\in U$ 及性质 (6)知 $ac\sim bd$, 即相伴关系是同余关系.

(8) 注意到 $1\in U$, 故由性质 (4)知 $1|u$. 再由性质 (5)知 $u\in U\iff u|1\iff u\sim 1$.

(9)

□

定义 3.9

设 R 是交换整环,$R^* = R \setminus \{0\}$, U 表示 R^* 中乘法可逆元素的集合, 则 $\forall u \in U, a \in R^*$, 由定理 3.15(1)和定理 3.15(4)知 u 是 a 的因子, 这种因子称为**平凡因子**.

定义 3.10

设 R 是交换整环,$R^* = R \setminus \{0\}$,$a, b \in R^*$. 若 $b|a$, 但 $a \nmid b$, 则称 b 为 a 的**真因子**. 换言之,b 为 a 的真因子当且仅当 b 是 a 的因子且 b 与 a 不相伴.

定理 3.16

设 R 是交换整环,$R^* = R \setminus \{0\}$, U 表示 R^* 中乘法可逆元素的集合, 则如果 $u \in U$, 则 u 无真因子.

证明 事实上若 v 是 u 的因子, 即 $v|u$, 又由定理 3.15(5)知 $u|1$, 故 $v|1$, 因而再由定理 3.15(5)知 $v \in U \subseteq R^*$, 故由定理 3.15(4)知 $u|v$. 因此 $v \sim u$, 由此知 u 无真因子.

□

定义 3.11

设 R 是交换整环,$R^* = R \setminus \{0\}$,U 表示 R^* 中乘法可逆元素的集合, $a \in R^* \setminus U$. 若 a 无非平凡的真因子, 则称 a 为**不可约元素**. 若 a 有非平凡的真因子, 则称 a 为**可约元素**.

特别地,R 的一元多项式环 $R[x]$ 上的不可约元素称为 $R[x]$ 上的**不可约多项式**.

注 由定义知若 a 是不可约元素, 则 $n \mid a \iff n \sim 1$或$n \sim a$.

命题 3.2

设 R 是交换整环,$R^* = R \setminus \{0\}$,U 表示 R^* 中乘法可逆元素的集合,$u \in U$,a 为 R 的不可约元素, 则 au 也是不可约的. 进而, 若 $a \sim b$, 则 b 也不可约.

证明 反证, 假设 au 可约, 则存在 $e \in R^*$ 为 au 的非平凡真因子. 从而存在 $x \in R^*$, 使 $au = ex$, 进而 $a = exu^{-1}$. 于是 e 也是 a 的非平凡真因子, 这与 a 不可约矛盾! 故 au 不可约. 由定理 3.15(6)可知存在 $u' \in U$, 使 $b = au'$. 由之前证明知 $b = au'$ 也不可约.

□

定义 3.12

设 R 是交换整环,$R^* = R \setminus \{0\}$,U 表示 R^* 中乘法可逆元素的集合, 若 $p \in R^* \setminus U$ 且满足

$$p|ab \Rightarrow p|a或p|b,$$

则称 p 为**素元素**.

命题 3.3

设 R 是交换整环,$R^* = R\setminus\{0\}$,U 表示 R^* 中乘法可逆元素的集合, 若 p 是素元素,$u \in U$,$a_i \in R (i = 1, 2, \cdots, l)$, 且 $p \mid u\prod\limits_{i=1}^{k} a_i$, 则存在 $i_0 \in \{1, 2, \cdots, k\}$, 使 $p \mid a_{i_0}$.

证明 由素元素定义可得 $p \mid u$ 或 $p \mid \prod\limits_{i=1}^{k} a_i$. 若 $p \mid u$, 则由定理 3.15(4)知 $u \mid p$, 故 $p \sim u$. 再由定理 3.15(6)知存在 $u' \in U$, 使 $p = uu' \in U$, 这与 p 不可约矛盾! 故下设 $p \mid \prod\limits_{i=1}^{k} a_i$.

由素元素定义可得 $p \mid a_k$ 或 $p \mid \prod_{i=1}^{k-1} a_i$. 若 $p \mid a_k$ 则结论已经成立. 若 $p \mid \prod_{i=1}^{k-1} a_i$, 则再由素元素定义可得 $p \mid a_{k-1}$ 或 $p \mid \prod_{i=1}^{k-2} a_i$. 若 $p \mid a_{k-1}$ 则结论已经成立. 若 $p \mid \prod_{i=1}^{k-2} a_i$, 则再由素元素定义可得 $p \mid a_{k-2}$ 或 $p \mid \prod_{i=1}^{k-3} a_i$. 继续做下去, 因为 $\prod_{i=1}^{k} a_i$ 中只有 k 个元素, 所以必在有限步终止, 故必存在 $i_0 \in \{1, 2, \cdots, k\}$, 使 $p \mid a_{i_0}$.

□

例题 3.7 在整数环 $\mathbb{Z}$ 中,$U = \{1, -1\}$, 于是 $a \sim b \iff a = \pm b$, 因而 a 为不可约元素当且仅当 a 为素数或负素数. 并且整数环 $\mathbb{Z}$ 的不可约元素都是素元素.

证明

□

例题 3.8 设 $\mathbb{P}$ 为数域, 则 $\mathbb{P}$ 上一元多项式环 $\mathbb{P}[x]$ 为交换整环. 此时 $U = \mathbb{P}^* = \mathbb{P} \setminus \{0\}$. $f(x) \sim g(x) \iff \exists c \in \mathbb{P}^*$, 使得 $f(x) = cg(x)$, 因而 $f(x)$ 为不可约元素当且仅当 $f(x)$ 为不可约多项式. 并且一元多项式环 $\mathbb{P}[x]$ 的不可约元素都是素元素.

证明

□

引理 3.4

设 R 是整环, 则 R 中的素元素一定是不可约元素.

♡

注 不可约元素不一定是素元素, 反例见例题 3.9.

证明 记 $R^* = R \setminus \{0\}$,U 表示 R^* 中乘法可逆元素的集合. 若 a 是素元素 p 的一个因子, 即有 $b \in R^*$, 使 $p = ab$, 因而 $p|a$ 或 $p|b$. 在 $p|a$ 的情况, 说明 a 不是 p 的真因子. 若 $p|b$, 即有 $c \in R^*$, 使 $b = pc$, 于是 $p = pac$, 由命题 1.11(1)知 R^* 对乘法满足消去律, 故 $ac = 1$, 从而 $a \in U$, 即 a 为平凡因子. 这说明 p 没有非平凡的真因子, 故 p 是不可约元素.

□

定义 3.13

设 $d \neq 1, 0$ 且为无平方因子的整数, 对任意的 $a + b\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$, 称

$$N(a + b\sqrt{d}) = |a^2 - db^2|$$

为 $a + b\sqrt{d}$ 的**范数** (norm).

♣

定理 3.17

设 $d \neq 1, 0$ 且为无平方因子的整数,$D = \mathbb{Z}[\sqrt{d}]$, 则对任意的 $\alpha, \beta \in D$, 有

(1) $N(\alpha) \in \mathbb{N} \cup \{0\}$, 且 $N(\alpha) = 0$ 当且仅当 $\alpha = 0$.

(2) $N(\alpha\beta) = N(\alpha)N(\beta)$, 且 α 为单位当且仅当 $N(\alpha) = 1$.

(3) 如果 $\alpha \mid \beta$(在 D 中), 则 $N(\alpha) \mid N(\beta)$(在 $\mathbb{Z}$ 中).

♡

证明

(1) 若 $\alpha = a + b\sqrt{d}, a, b \in \mathbb{Z}$, 则显然 $N(\alpha) = |a^2 - db^2| \in \mathbb{N} \cup \{0\}$. 若存在不全为零的 $a, b \in \mathbb{Z}$, 使得 $a + b\sqrt{d} = 0$, 则 $a = -b\sqrt{d}$, 所以两边平方得

$$a^2 = b^2 d. \tag{3.17}$$

若 $b = 0$, 则由(3.17)式得 $a = 0$. 若 $a = 0$, 则由(3.17)式得 $b^2 d = 0$, 而 $d \neq 0$, 于是 $b = 0$. 从而 a, b 都不为 0, 所以

$$d = \frac{a^2}{b^2} > 0. \tag{3.18}$$

由于等式(3.18)的右边是一平方数, 因此 d 必定也是个平方数. 这与 d 无平方因子的假设相矛盾. 于是

$$a+b\sqrt{d}=0 \iff a=b=0. \tag{3.19}$$

当 $\alpha=a+b\sqrt{d}=0$ 时, 由(3.19)式知 $a=b=0$, 故此时 $N(\alpha)=N(0)=0$.

当 $N(\alpha)=|a^2-db^2|=0$ 时, 有 $a^2=b^2d$, 故由上述证明同理可得 $a=b=0$, 即 $\alpha=0$.

(2) 设 $\alpha=a+b\sqrt{d},\beta=a'+b'\sqrt{d}$, 则 $\alpha\beta=aa'+bb'd+(ab'+ba')\sqrt{d}$. 因为

$$\begin{aligned}(a^2-db^2)(a'^2-db'^2)&=(aa')^2+(bb'd)^2-[(ab')^2+(ba')^2]d\\&=[(aa')^2+(bb'd)^2+2aa'bb'd]-[(ab')^2+(ba')^2+2aa'bb']d\\&=(aa'+bb'd)^2-d(ab'+ba')^2,\end{aligned}$$

所以

$$N(\alpha)N(\beta)=N(\alpha\beta). \tag{3.20}$$

当 $N(\alpha)=1$ 时, 有 $N(\alpha)=|a^2-b^2d|=1$. 取 $\alpha_1=a-b\sqrt{d}$, 则

$$\alpha\alpha_1=\alpha_1\alpha=a^2-b^2d=1.$$

故此时 α 可逆, 即 α 为单位.

当 α 为单位时, 由定理 3.17(1)知 $N(\alpha),N(\alpha^{-1})\in\mathbb{N}\cup\{0\}$, 若 $N(\alpha)\neq 1$, 则 $N(\alpha)>1$, 从而由(3.20)可得

$$1=N(1)=N(\alpha\alpha^{-1})=N(\alpha)N(\alpha^{-1})\Longrightarrow N(\alpha^{-1})=\frac{1}{N(\alpha)}\notin\mathbb{N}\cup\{0\}.$$

这与 $N(\alpha^{-1})\in\mathbb{N}\cup\{0\}$ 矛盾! 故 $N(\alpha)=1$.

(3) 如果 $\alpha\mid\beta$(在 D 中), 则存在 $\gamma\in D$, 使得 $\beta=\alpha\gamma$. 因此由定理 3.17(2)得 $N(\beta)=N(\alpha)N(\gamma)$. 而 $N(\gamma)\in\mathbb{Z}$, 所以 $N(\alpha)\mid N(\beta)$.

□

例题 3.9 令 $R=\mathbb{Z}[\sqrt{-5}]=\{a+b\sqrt{-5}\mid a,b\in\mathbb{Z}\}$. 设 $\alpha=a+b\sqrt{-5}$, 则 $\mathbb{Z}[\sqrt{-5}]$ 的单位群 $U=\{1,-1\}$, 且 3 是 $\mathbb{Z}[\sqrt{-5}]$ 的不可约元素, 但不是 $\mathbb{Z}[\sqrt{-5}]$ 的素元素.

证明 注意到 $\forall\alpha,\beta\in R$ 有 $N(\alpha\beta)=N(\alpha)N(\beta)$. 先求 R 的单位群 U.$\alpha\in U$, 则有 $\alpha\alpha^{-1}=1$, 故 $N(\alpha)N(\alpha^{-1})=N(1)=1$, 故 $N(\alpha)=1$. 由此即得 $U=\{1,-1\}$, 因而 $\alpha\sim\beta\iff\alpha=\pm\beta$.

再证明 3 是 $\mathbb{Z}[\sqrt{-5}]$ 的不可约元素, 但不是 $\mathbb{Z}[\sqrt{-5}]$ 的素元素. 设 $\alpha=a+b\sqrt{-5}$ 是 3 的一个因子, 故有 β, 使 $3=\alpha\beta$, 于是 $N(3)=N(\alpha)N(\beta)$. 由 $N(3)=9$ 知 $N(\alpha)$ 有以下三种可能:

(1) $N(\alpha)=1$, 则 $\alpha=\pm1$, 即 α 是 3 的平凡因子;

(2) $N(\alpha)=3$, 于是 $a^2+5b^2=3$, 但此方程无整数解, 故这种情况不存在;

(3) $N(\alpha)=9$, 于是 $N(\beta)=1,\beta=\pm1$, 即有 $\alpha=\pm3,\alpha\sim3$, 即 α 不是 3 的真因子.

由上知 3 是不可约元素. 另一方面,$3\mid 9,9=(2+\sqrt{-5})(2-\sqrt{-5})$. 由于 $N(2+\sqrt{-5})=N(2-\sqrt{-5})=N(3)=9$, 而 3 与 $2\pm\sqrt{-5}$ 不相伴, 因而 $3\nmid 2\pm\sqrt{-5}$, 即 3 不是素元素. □

定义 3.14

若一个交换整环 R 的不可约元素是素元素, 则称 R 满足**素性条件**.

♣

定义 3.15

设 R 是交换整环,$R^*=R\setminus\{0\},b,c\in R^*$. 若 $d\in R^*$ 满足 $d\mid b,d\mid c$, 则称 d 为 b,c 的**公因子**. 若对 b,c 的任一公因子 d_1 有 $d_1\mid d$, 则称 d 是 b,c 的**最大公因子**. 也记为 (b,c). 若 $(a,b)\sim1$, 则称 a 与 b 为**互素**

对 R^* 中任意有限个元素也可类似地定义它们的最大公因子.

♣

注 一般来说,R^* 中任意两个元素的最大公因子不一定存在.

定义 3.16

设 R 是交换整环,$R^* = R \setminus \{0\}$, 如果 R^* 中任意两个元素的最大公因子存在, 则称 R 满足**最大公因子条件**. ♣

引理 3.5

设交换整环 R 满足最大公因子条件,$a, b, c, a_1, \cdots, a_r, b_1, \cdots, b_r \in R$, 则有下列结论:

(1) 设 d 是 a, b 的一个最大公因子, 则 d_1 为 a, b 的最大公因子当且仅当 $d_1 \sim d$, 即 a, b 的最大公因子在相伴意义下是唯一的;

(2) $\forall a_1, a_2, \cdots, a_r \in R$ 均有最大公因子;

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

(4) $((a, b), c) \sim (a, (b, c))$;

(5) $c(a_1, a_2, \cdots, a_r) \sim (ca_1, ca_2, \cdots, ca_r)$;

(6) 若 $a \in U$, 则 $(a, b) \sim 1$.

(7) 若 $(a, b_i) \sim 1, 1 \leqslant i \leqslant r$, 则 $(a, b_1 b_2 \cdots b_r) \sim 1$.

(8) 若 p 是不可约元素, 则 $p \nmid a \iff (p, a) \sim 1$.

(9) 若 p 是不可约元素, 则 $(p, (a_1, a_2, \cdots, a_r)) \sim 1$ 当且仅当存在 $s \in \{1, 2, \cdots, r\}$, 使

$$p \mid a_i,\ 1 \leqslant i \leqslant s-1, \quad p \nmid a_s.$$

♡

证明

(1) 由于 d, d_1 是 a, b 的最大公因子, 故 $d \mid d_1, d_1 \mid d$. 于是 $d \sim d_1$. 反之,$d_1 \sim d$, 故 $d_1 \mid d$. 又 $d \mid a, b$, 于是 $d_1 \mid a, b$, 因而 d_1 是 a, b 的公因子. 又若 c 是 a, b 的公因子, 则 $c \mid d$, 而 $d \mid d_1$, 故有 $c \mid d_1$, 因而 d_1 是 a, b 的最大公因子.

(2) 令 $d_1 = (a_1, a_2), d_2 = (d_1, a_3), d_3 = (d_2, a_4), \cdots, d = d_{r-1} = (d_{r-2}, a_r)$. 下面证明 d 是 $a_1, a_2, \cdots, a_r$ 的最大公因子. 显然有 $d \mid d_k$ $(1 \leqslant k \leqslant r-2), d \mid a_r$. 又 $d_k \mid a_{k+1}$, 故 $d \mid a_i$ $(1 \leqslant i \leqslant r)$, 即 d 为公因子. 又若 $a \mid a_i$ $(1 \leqslant i \leqslant r)$, 则 $a \mid d_1$ 且依次 $a \mid d_2, a \mid d_3, \cdots$, 最后有 $a \mid d_{r-1}$, 即 $a \mid d$, 因而 d 是最大公因子.

(3) 设 $d = (a, b)$, 则 $d \mid a, b$. 由 $b \sim c$ 知 $b \mid c$, 故 $d \mid a, c$, 即 d 是 a, c 的公因子. 又设 d_1 也是 a, c 的公因子, 又 $b \sim c$, 故 $c \mid b$, 从而 $d_1 \mid a, b$, 即 d_1 是 a, b 的公因子. 故 $d_1 \mid d$. 因此 d 是 a, c 的最大公因子. 由结论 (1)知 $d \sim (a, c)$.

(4) 由结论 (2)同理可知 $((a, b), c)$ 与 $(a, (b, c))$ 都是 a, b, c 的最大公因子. 由结论 (1) 知它们相伴.

(5) 设 $d = (a, b), e = (ca, cb)$, 则 $cd \mid ca, cd \mid cb$. 于是 $cd \mid e$, 因而 $e = cdu (u \in R^*)$. 又由 $ca \mid e$ 知 $ca = ex (x \in R^*)$. 由此知 $ca = ex = xucd$. 由命题 1.11(1)知 R^* 对乘法满足消去律, 故 $a = xud$, 即 $ud \mid a$, 同样有 $ud \mid b$, 故 $ud \mid d$, 于是 $d = udk (k \in R^*)$, 同样由 R^* 对乘法满足消去律可得 $uk = 1$, 因而 $u \in U$. 于是由定理 3.15(6)知 e 与 cd 相伴. 再利用数学归纳法易证.

(6) 显然 $1 \mid a, b$. 设 $d \mid a, b$, 则存在 $a_1 \in R^*$, 使 $a = da_1$. 于是由 $a \in U$ 知 $1 = aa^{-1} = d\left(a_1 a^{-1}\right)$, 故 $d|1$. 因此 $(a, b) \sim 1$.

(7) 因为 $(a, b) \sim 1, (1, c) \sim 1$, 由结论 (5) 知 $(ac, bc) \sim c, (a, ac) \sim a$, 故由结论 (4)及结论 (3)有 $1 \sim (a, c) \sim (a, (ac, bc)) \sim ((a, ac), bc) \sim (a, bc)$. 再利用数学归纳法易证.

(8) $\Longleftarrow$: 假设 $p \mid a$, 则存在 $a_1 \in R^*$, 使 $a = pa_1$. 于是由结论 (5)和结论 (6)知 $1 \sim (p, a) = (p, pa_1) = p(1, a_1) = p$. 但由 p 不可约知 $p \notin U$, 由定理 3.15(6)知 $p \nmid 1$, 矛盾!

$\Longrightarrow$: 设 $d = (p, a)$, 则存在 $p_1, a_1 \in R^*$, 使 $p = dp_1, a = da_1$. 假设 $d \nmid 1$, 则由定理 3.15(6)知 $d \notin U$, 从而 $d \in R^* \setminus U$. 若 $p \mid d$, 则由 $d \mid a$ 知 $p \mid a$, 这与 $p \nmid a$ 矛盾! 故 $p \nmid d$.

若 $d \neq p$, 则由 $p = dp_1, p \nmid d$ 及 $d \in R^* \setminus U$ 知 d 是 p 的非平凡真因子, 这与 p 不可约矛盾!

若 $d = p$, 则由 $a = da_1$ 知 $a = pa_1$, 即 $p \mid a$, 这与 $p \nmid a$ 矛盾!

因此 $d \mid 1$, 故 $d \sim 1$.

(9) $\Longrightarrow$: 假设 $p \mid a_i, 1 \leqslant i \leqslant s$, 则 $p \mid (a_1, a_2, \cdots, a_r)$. 从而 $(p, (a_1, a_2, \cdots, a_r)) \sim p$ 矛盾! 故可设 $s_1, s_2, \cdots, s_k \in$

$\{1,2,\cdots,r\}$, 使

$$p \mid a_i,\ i \notin \{s_1,s_2,\cdots,s_k\}, \quad p \nmid a_s,\ i \in \{s_1,s_2,\cdots,s_k\}.$$

取 $s = \min\limits_{j=1,2,\cdots,k} s_j$, 则

$$p \mid a_i,\ 1 \leqslant i \leqslant s-1, \quad p \nmid a_s.$$

$\Longleftarrow$: 由 $p \nmid a_s$ 知 $p \nmid (a_1,a_2,\cdots,a_r)$, 否则由 $p \mid (a_1,a_2,\cdots,a_r)$ 知 $p \mid a_s$ 矛盾! 于是由结论 (8)知

$$(p,(a_1,a_2,\cdots,a_r)) \sim 1.$$

□

定义 3.17 (唯一析因环)

设 R 是交换整环,$R^* = R \setminus \{0\}$,U 表示 R^* 中乘法可逆元素的集合, 如果 R 满足下列条件:

(1) **有限析因条件**: $\forall a \in R^* \setminus U$, 可分解为有限个不可约元素的乘积, 即有不可约元素 $p_i (1 \leqslant i \leqslant r)$ 及单位 $u \in U$, 使

$$a = p_1 p_2 \cdots p_r.$$

(2) 若 $a \in R^* \setminus U$ 有两种不可约元素乘积的分解:

$$a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

则有 $r = s$ 且 $\exists \pi \in S_n$, 使 $p_i \sim q_{\pi(i)} (1 \leqslant i \leqslant r)$.

那么称 R 为**唯一析因环** (简记为 **UFD**) 或**唯一分解整环**或 **Gauss 环**. 称 $|a| \triangleq r$ 为 a 的**长度**. 若 $u \in U$, 约定 $|u| \triangleq 0$.

♣

注 所谓唯一析因环也就是使因式分解唯一性定理成立的交换整环, 因而前面例题 3.7与例题 3.8中的环 $\mathbb{Z}$ 与 $\mathbb{P}[x]$ 都是 UFD, 而例题 3.9中的环 $\mathbb{Z}[\sqrt{-5}]$ 就不是. 因为 $9 = 3^2$ 与 $9 = (2+\sqrt{-5})(2-\sqrt{-5})$ 是 9 的两种本质上不同的分解, 即 $\mathbb{Z}[\sqrt{-5}]$ 不满足唯一析因环定义中的条件 (2).

定理 3.18

设 R 是唯一析因环 (UFD),$R^* = R \setminus \{0\}$,U 表示 R^* 中乘法可逆元素的集合, 则

(1) 对 $\forall a \in R^* \setminus U$, 都存在 $r \in \mathbb{N}$, 单位 $u \in U$ 以及互不相伴的不可约元素 $p_1,p_2,\cdots,p_r$, 使

$$a = u p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}, \quad n_i \in \mathbb{N}.$$

若 c 是 a 的一个非平凡因子, 则存在 $u_1 \in U$ 以及 $n_i' \leqslant n_i$ 且 $n_i' \in \mathbb{N} (i = 1,2,\cdots,r)$, 使

$$c = u_1 p_1^{n_1'} p_2^{n_2'} \cdots p_r^{n_r'}.$$

(2) 若 $a,b \in R^* \setminus U$, 则存在 $r \in \mathbb{N}$, 单位 $u,v \in U$ 以及互不相伴的不可约元素 $p_1,p_2,\cdots,p_r$, 使

$$a = u p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}, \quad n_i \in \mathbb{N} \cup \{0\};$$

$$b = v p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}, \quad m_i \in \mathbb{N} \cup \{0\}.$$

若还有 d 是 a,b 的公因子, 则存在 $w \in U$ 以及 $n_i' \leqslant \min\{n_i,m_i\}$ 且 $n_i' \in \mathbb{N} (i = 1,2,\cdots,r)$, 使

$$d = w p_1^{n_1'} p_2^{n_2'} \cdots p_r^{n_r'}.$$

♡

证明

(1) 由 a 满足有限析因条件知, 存在不可约元素 $q_1,q_2,\cdots,q_s$, 使得

$$a = q_1 q_2 \cdots q_s.$$

将 $q_1,q_2,\cdots,q_s$ 按相伴关系分类, 不妨设存在 $r \in \mathbb{N}$ 和

$$0 = i_0 \leqslant i_1 \leqslant \cdots \leqslant i_r = s,$$

使 $q_{i_1}, q_{i_2}, \cdots, q_{i_r}$ 互不相伴且

$$q_{i_0+1} = q_1 \sim q_2 \sim \cdots \sim q_{i_1};$$

$$q_{i_1+1} \sim q_{i_1+2} \sim \cdots \sim q_{i_2};$$

$$\cdots\cdots$$

$$q_{i_{r-1}+1} \sim q_{i_{r-1}+2} \sim \cdots \sim q_{i_r} = q_s.$$

由定理 3.15(6)知存在

$$u_{11}, u_{12}, \cdots, u_{1,i_1-1}, u_{21}, u_{22}, \cdots, u_{2,i_2-1}, \cdots, u_{r1}, u_{r2}, \cdots, u_{r,i_r-1} \in U,$$

使得

$$q_1 = u_{11}q_{i_1}, \quad q_2 = u_{12}q_{i_1}, \cdots\cdots, q_{i_1-1} = u_{1,i_1-1}q_{i_1};$$

$$q_{i_1+1} = u_{21}q_{i_2}, \quad q_{i_1+2} = u_{22}q_{i_2}, \cdots\cdots, q_{i_2-1} = u_{2,i_2-1}q_{i_2};$$

$$\cdots\cdots\cdots\cdots$$

$$q_{i_{r-1}+1} = u_{r1}q_{i_r}, \quad q_{i_{r-1}+2} = u_{r2}q_{i_r}, \cdots\cdots, q_{i_r-1} = u_{r,i_r-1}q_{i_r}.$$

记 $p_j = q_{i_j}, n_j = i_j - i_{j-1} (j = 1, 2, \cdots, r), u = \prod_{j=1}^{r} \prod_{i=1}^{i_j-1} u_{ji} \in U$, 则 $p_1, p_2, \cdots, p_r$ 互不相伴且

$$a = q_1 q_2 \cdots q_s = q_{i_1}^{i_1-1} \prod_{i=1}^{i_1-1} u_{1i} \cdot q_{i_2}^{i_2-1} \prod_{i=1}^{i_2-1} u_{2i} \cdots q_{i_r}^{i_r-1} \prod_{i=1}^{i_r-1} u_{ri}$$

$$= \prod_{j=1}^{r} \prod_{i=1}^{i_j-1} u_{ji} \cdot q_{i_1}^{i_1-1} q_{i_2}^{i_2-1} \cdots q_{i_r}^{i_r-1} = u p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}.$$

由 c 是 a 的非平凡因子知, 存在 $d \in R^*$, 使 $a = cd$. 由 R 是唯一析因环 (UFD) 知 c, d 都满足有限析因条件, 故存在不可约元素 $c_1, c_2, \cdots, c_t$ 和 $d_1, d_2, \cdots, d_m$ 使

$$c = c_1 c_2 \cdots c_t, \quad d = d_1 d_2 \cdots d_m.$$

从而

$$q_1 q_2 \cdots q_s = a = cd = c_1 c_2 \cdots c_t \cdot d_1 d_2 \cdots d_m.$$

由 R 是唯一析因环 (UFD) 知 a 的不可约分解在相伴意义下唯一, 再记 $f_i = \begin{cases} c_i, & i = 1, 2, \cdots, t \\ d_{i-t}, & i = t+1, \cdots, t+m \end{cases}$, 故 $s = t + m$ 且存在 $\pi \in S_s$, 使 $q_i \sim f_{\pi(i)} (i = 1, 2, \cdots, s)$, 即 $q_{\pi^{-1}(i)} \sim f_i (i = 1, 2, \cdots, s)$. 于是 $c_i \sim q_{\pi^{-1}(i)} (i = 1, 2 \cdots, t)$. 不妨设存在

$$0 = i'_0 \leqslant i'_1 \leqslant \cdots \leqslant i'_r = t,$$

使

$$\pi^{-1}(i'_{j-1} + 1), \cdots, \pi^{-1}(i'_j) \in \{i_{j-1} + 1, \cdots, i_j\}, \quad j = 1, 2, \cdots, r.$$

记 $n'_j = i'_j - i'_{j-1}$, 则由 $n_j = i_j - i_{j-1}$ 知 $n'_j \leqslant n_j$. 又因为

$$q_k \sim q_{i_j} = p_j, \quad k = i_{j-1} + 1, \cdots, i_j, \ j = 1, 2, \cdots, r.$$

所以

$$q_{\pi^{-1}(i'_{j-1}+1)} \sim \cdots \sim q_{\pi^{-1}(i'_j)} \sim p_j, \quad j = 1, 2, \cdots, r.$$

因此

$$c_{i'_{j-1}+1} \sim \cdots \sim c_{i'_j} = c_{i'_{j-1}+n'_j} \sim p_j, \quad j = 1, 2, \cdots, r.$$

由定理 3.15(6)知存在

$$u_{j1}, u_{j2}, \cdots, u_{jn'_j}, \quad j = 1, 2, \cdots, r.$$

使得

$$c_{i'_{j-1}+k} = u_{jk} p_j, \quad k = 1, 2, \cdots, n'_j, \ j = 1, 2, \cdots, r.$$

再记 $u_1 = \prod_{j=1}^{r} \prod_{k=1}^{n'_j} u_{jk}$, 于是

$$\begin{aligned} c = c_1 c_2 \cdots c_t &= \prod_{j=1}^{r} \prod_{k=1}^{n'_j} c_{i'_{j-1}+k} \\ &= \prod_{j=1}^{r} \left(\prod_{k=1}^{n'_j} u_{jk} p_j \right) = \prod_{j=1}^{r} p_j^{n'_j} \left(\prod_{k=1}^{n'_j} u_{jk} \right) \\ &= \prod_{j=1}^{r} p_j^{n'_j} \left(\prod_{k=1}^{n'_j} u_{jk} \right) = \left(\prod_{j=1}^{r} p_j^{n'_j} \right) \left(\prod_{j=1}^{r} \prod_{k=1}^{n'_j} u_{jk} \right) \\ &= u_1 p_1^{n'_1} p_2^{n'_2} \cdots p_r^{n'_r}. \end{aligned}$$

(2) 由 (1) 知存在 $t, s \in \mathbb{N}$, 单位 $u_1, v_1 \in U$, 互不相伴的不可约元素 $p_1, p_2, \cdots, p_s$ 和互不相伴的不可约元素 $q_1, q_2, \cdots, q_t$, 使

$$a = u_1 p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s}, \quad n_i \in \mathbb{N};$$

$$b = v_1 q_1^{m_1} q_2^{m_2} \cdots q_t^{m_t}, \quad m_i \in \mathbb{N}.$$

不妨设存在 $k \leqslant \min\{s, t\}$, 使

$$p_j \sim q_j, \quad j = 1, 2, \cdots, k.$$

由定理 3.15(6)知存在 $w_j \in U (j = 1, 2, \cdots, k)$, 使

$$q_j = w_j p_j, \quad j = 1, 2, \cdots, k.$$

于是

$$\begin{aligned} b &= v_1 (w_1 p_1)^{m_1} (w_2 p_2)^{m_2} \cdots (w_k p_k)^{m_k} \cdot q_{k+1}^{m_{k+1}} \cdots q_t^{m_t} \\ &= (v_1 w_1 w_2 \cdots w_k) \left(p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k} \cdot q_{k+1}^{m_{k+1}} \cdots q_t^{m_t} \right). \end{aligned}$$

再记 $p_{s+j} = q_j (j = k+1, \cdots, t), u = u_1, v = v_1 w_1 w_2 \cdots w_k$, 则

$$\begin{aligned} a &= u p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s} p_{s+1}^0 \cdots p_{s+t}^0, \\ b &= v p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k} p_{k+1}^0 \cdots p_s^0 p_{s+1}^{m_{k+1}} \cdots p_{s+t}^{m_t}. \end{aligned}$$

再取 $r = s + t, n_j = m_l = 0 (j = s+1, \cdots, s+t; l = k+1, \cdots, s)$ 即得

$$a = u p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}, \quad b = v p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}.$$

若 $d \in U$, 则取 $n'_i = 0 (i = 1, 2, \cdots, r)$ 即可.

若 $d \in R^* \setminus U$, 则由 d 是 a, b 的公因子和 (1) 的结论可知, 存在单位 $u', u'' \in U$, 互不相伴的不可约元素 $p_1, p_2, \cdots, p_r$ 以及 $n'_i \leqslant n_i, n''_i \leqslant m_i (i = 1, 2 \cdots, r)$ 使

$$d = u' p_1^{n'_1} p_2^{n'_2} \cdots p_r^{n'_r} = u'' p_1^{n''_1} p_2^{n''_2} \cdots p_r^{n''_r}.$$

若存在 $j_1, j_2 \cdots, j_k \in \{1, 2 \cdots, r\}$, 使 $n'_{j_l} \neq n''_{j_l} (l = 1, 2, \cdots, k)$. 由命题 1.11(1)知 R^* 对乘法满足消去律, 故

$$u' (u'')^{-1} p_{j_1}^{n'_{j_1} - n''_{j_1}} p_{j_2}^{n'_{j_2} - n''_{j_2}} \cdots p_{j_k}^{n'_{j_k} - n''_{j_k}} = 1.$$

由此可知 $p_{j_l} \in U (l = 1, 2, \cdots, k)$, 这与 p_{j_l} 不可约矛盾! 故 $n'_i = n''_i (i = 1, 2, \cdots, r)$, 从而 $n'_i = n''_i \leqslant$

$\min\{n_i, m_i\}(i = 1, 2\cdots, r)$, 取 $w = u'$, 则

$$d = wp_1^{n_1'} p_2^{n_2'} \cdots p_r^{n_r'}.$$

□

定理 3.19

设 R 是唯一析因环,$R^* = R \setminus \{0\}$,U 表示 R^* 中乘法可逆元素的集合,$a, b, c \in R^*$, 则

(1) $|ab| = |a| + |b|$;

(2) $a \mid b \Longrightarrow |a| \geqslant |b|$;

(3) $a \in U \iff |a| = 0$;

(4) $b \sim c \iff |b| = |c|,\ b|c$.

♡

证明

(1)

(2) 根据定义显然成立.

(3)

□

定义 3.18

设 R 是交换整环,$R^* = R \setminus \{0\}$,R^* 中的一个序列 $a_1, a_2, \cdots, a_n, a_{n+1}, \cdots$ 满足

$$a_{n+1} \mid a_n, \quad n = 1, 2, \cdots,$$

则称为 R 的一个**因子链**.

若对 R^* 中任一因子链, 存在自然数 m, 使

$$a_m \sim a_n, \quad \forall n \geqslant m,$$

则称 R 满足**因子链条件**.

♣

引理 3.6

设 R 是交换整环,$R^* = R \setminus \{0\}$,U 表示 R^* 中乘法可逆元素的集合, 若 R 满足因子链条件, 则必满足有限析因条件.

♡

证明 设 $a \in R^* \setminus U$. 先证 a 有不可约因子. 不妨设 a 是可约的, 则 a 有非平凡的真因子 a_1, 即有 $a = a_1 b_1$. 这时 b_1 也是 a 的非平凡真因子, 否则,$b_1 \in U$, 由定理 3.15(6)知 $a \sim a_1$, 这与 a_1 为 a 真因子矛盾! 若有 a_1, b_1 都可约, 则 $a_1 = a_2 b_2$, 其中,a_2, b_2 为 a_1 的真因子. 如此继续, 可得因子链

$$a, a_1, a_2, \cdots, a_n, a_{n+1}, \cdots$$

且 $a_{n+1} \mid a_n, a_n \mid a$. 这个因子链是在假设 $a_1, a_2, \cdots, a_n, \cdots$ 都可约且对 $\forall n \in \mathbb{N}$ 有 a_{n+1} 是 a_n 的真因子的条件下得到的. 而由因子链条件有 m, 使得 $a_m \sim a_{m+1}$, 这与 a_{m+1} 是 a_m 的真因子矛盾! 因而 a_m 是不可约的, 即 a_m 是 a 的不可约因子.

再证 a 可分解为有限多个不可约因子的乘积. 设 p_1 是 a 的一个不可约因子, 于是 $a = p_1 a^{(1)}$. 若 $a^{(1)} \in U$, 则由命题 3.2知 a 不可约. 此时 a 满足有限析因条件.

若 $a^{(1)} \in R^* \setminus U$, 则 $a^{(1)}$ 有不可约因子 p_2, 使 $a^{(1)} = p_2 a^{(2)}$, 即 $a = p_1 p_2 a^{(2)}$. 继续此过程, 即得因子链

$$a, a^{(1)}, a^{(2)}, \cdots, a^{(n)}, a^{(n+1)}, \cdots$$

且 $a^{(n+1)} \mid a^{(n)}, a^{(n)} \mid a, p_{n+1}$ 都是 $a^{(n)}$ 的不可约因子,$a^{(n)} = p_{n+1} a^{(n+1)}$. 这个因子链是在假设 $a^{(n)} \in R^* \setminus U (\forall n \in \mathbb{N})$ 的条件下得到的. 而由因子链条件有 s, 使 $a^{(s-1)} \sim a^{(s)}$. 于是存在 $b \in R^*$, 使 $a^{(s)} = b a^{(s-1)}$, 从而 $a^{(s-1)} = p_s a^{(s)} = p_s b a^{(s-1)}$. 由命题 1.11(1)知 R^* 对乘法满足消去律, 故 $p_s b = 1$, 即 $p_s \in U$, 这与 p_s 不可约矛盾! 故存在 m, 使得

$a^{(m)} \in U$. 于是记 $q_m = p_m a^{(m)}$, 则由命题 3.2知 q_m 不可约. 故此时

$$a = p_1 p_2 \cdots p_m a^{(m)} = p_1 p_2 \cdots q_m.$$

满足有限析因条件. 这就证明了 R 满足有限析因条件.

□

定理 3.20

设 R 是交换整环,$R^* = R \setminus \{0\}$,U 表示 R^* 中乘法可逆元素的集合, 则下列条件等价:

(1) R 是唯一析因环 (UFD);

(2) R 满足因子链条件与素性条件;

(3) R 满足因子链条件与最大公因子条件.

♡

注 由这个定理的结论 (2) 和引理 3.4知唯一析因环 (UFD) 中的素元素等价于不可约元素.

证明 (1) ⇒ (3). 设 R 为唯一析因环. 先证 R 满足因子链条件. $\forall a \in R^* \setminus U$,$a$ 有不可约元素乘积分解 $a = up_1 p_2 \cdots p_r$. 现设 $a_1, a_2, \cdots, a_n, a_{n+1}, \cdots$ 是 R^* 的一个因子链. 于是由定理 3.19(2)知必有 $|a_i| \geqslant 0$ 且

$$|a_1| \geqslant |a_2| \geqslant \cdots \geqslant |a_n| \geqslant |a_{n+1}| \geqslant \cdots,$$

由于 $|a_1|$ 是一个有限数, 因而有 m, 使得当 $n \geqslant m$ 时,$|a_n| = |a_m|$, 由定理 3.19(4)知 $a_n \sim a_m$, 故 R 满足因子链条件.

现证 R 满足最大公因子条件. 设 $a, b \in R^*$, 若 a, b 中有一个是单位, 则由引理 3.5(6)知 $(a, b) = 1$, 故假定 $a, b \in R^* \setminus U$. 这时由定理 3.18(1), 不妨设

$$a = up_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}, \quad b = vp_1^{m_1} p_2^{m_2} \cdots p_r^{m_r},$$

其中,$u, v \in U$,$p_1, p_2, \cdots, p_r$ 是互不相伴的不可约元素,$n_i \geqslant 0$,$m_j \geqslant 0$,$1 \leqslant i, j \leqslant r$. 令 $k_i = \min\{n_i, m_i\}$, 记

$$d = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \tag{3.21}$$

显然 d 是 a, b 的公因子. 又设 d_1 也是 a, b 的公因子, 则由定理 3.18(2)知存在 $u_1 \in U$ 以及 $n_i' \leqslant k_i$ 且 $n_i' \in \mathbb{N} (i = 1, 2, \cdots, r)$, 使

$$d_1 = u_1 p_1^{n_1'} p_2^{n_2'} \cdots p_r^{n_r'}.$$

故 $d_1 \mid d$. 因此 d 是 a, b 的最大公因子.

(3) ⇒ (2). 为此只需证明素性条件成立. 设 p 是一个不可约元素且 $p \nmid a$,$p \nmid b$, 由定理 3.5(8)有 $(p, a) \sim 1$,$(p, b) \sim 1$. 由引理 3.5(7)知 $(p, ab) \sim 1$, 因而再由定理 3.5(8)知 $p \nmid ab$. 换言之, 若 $p \mid ab$, 则有 $p \mid a$ 或 $p \mid b$, 故 p 为素元素.

(2) ⇒ (1). 由引理 3.6知 R 满足有限析因环条件, 故只需证因式分解的唯一性. 不妨设 $a \in R^* \setminus U$ 且 a 有两个不可约元素乘积的分解

$$a = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t. \tag{3.22}$$

现对 s 用数学归纳法证. 若 $s = 1$, 则 a 为不可约元素, 由素性条件知 a 为素元素. 根据素元素的定义, 可不妨设 $a \mid q_1$, 则 $a \sim q_1$. 从而由定理 3.15(6)知存在 $u \in U$, 使 $a = q_1 u = q_1 q_2 \cdots q_t$, 故 $t = 1$. 设 $s - 1$ 时已成立, 现证 s 时成立. 因 $p_s \mid a$, 故 $p_s \mid q_1 q_2 \cdots q_t$, 由素性条件知 p_s 也是素元素, 于是不妨设 $p_s \mid q_t$, 于是 $q_t = u_s p_s (u_s \in U)$. 由命题 1.11(1)知 R^* 对乘法满足消去律, 因而结合(3.22)式有

$$p_1 p_2 \cdots p_{s-1} p_s = q_1 q_2 \cdots q_{t-1} q_t = u_s q_1 q_2 \cdots q_{t-1} p_s \Longrightarrow p_1 p_2 \cdots p_{s-1} = u_s \prod_{i=1}^{t-1} q_i.$$

记 $q_1' = u_s q_1, q_i' = q_i (2 \leqslant i \leqslant t - 1)$, 由命题 3.2知 q_1' 也不可约, 并且由定理 3.15(6)知 $q_i' \sim q_i (1 \leqslant i \leqslant t - 1)$, 则

$$p_1 p_2 \cdots p_{s-1} = q_1' q_2' \cdots q_{t-1}'.$$

由归纳假设可知,$s - 1 = t - 1$ 且存在 $\pi \in S_{t-1}$, 使 $p_i \sim q'_{\pi(i)} \sim q_{\pi(i)} (1 \leqslant i \leqslant t - 1)$. 由命题 1.11(1)知 R^* 对乘法满足

消去律, 再结合(3.22)式及定理 3.15(6)知

$$u_s p_s \prod_{i=1}^{t-1} q_i = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t \Longrightarrow u_s p_s = q_t \Longrightarrow p_s \sim q_t.$$

故 $s = t$ 且有 $\pi' \in S_t$, 使得 $p_i \sim q_{\pi'(i)} (1 \leqslant i \leqslant t)$, 即 R 是一个 UFD.

□

命题 3.4

设 R 是唯一析因环, 若一组两两互素的素元素 $p_1, p_2, \cdots, p_k$ 都整除 a, 则 $\prod_{i=1}^{k} p_i \mid a$.

♠

证明 由定理 3.18知存在 $u \in U$ 和互不相伴的不可约元素 $q_1, q_2, \cdots, q_r$, 使

$$a = u q_1^{n_1} q_2^{n_2} \cdots q_r^{n_r}, \quad n_i \in \mathbb{N}.$$

对 $\forall i \in \{1, 2, \cdots, k\}$, 由条件知 $p_i \mid a$, 故由命题 3.3知存在 $r_i \in \{1, 2, \cdots, r\}$, 使 $p_i \mid q_{r_i}$. 若 $q_{r_i} \nmid p_i$, 则 p_i 是 q_{r_i} 的真因子. 由 q_{r_i} 不可约知 $p_i \in U$, 这与 p_i 是素元素矛盾! 故 $p_i \sim q_{r_i}$, 由定理 3.15(6)知存在 $u_i \in U$, 使

$$q_{r_i} = u_i p_i, \quad i = 1, 2, \cdots, k.$$

因此

$$\begin{aligned} a &= u \prod_{i=1}^{r} q_i^{n_i} = u \prod_{i \notin \{r_1, \cdots, r_k\}} q_i^{n_i} \prod_{i=1}^{k} q_{r_i}^{n_{r_i}} \\ &= u \prod_{i \notin \{r_1, \cdots, r_k\}} q_i^{n_i} \prod_{i=1}^{k} u_i p_i^{n_i} \\ &= \left(u \prod_{i \notin \{r_1, \cdots, r_k\}} q_i^{n_i} \prod_{i=1}^{k} u_i \right) \prod_{i=1}^{k} p_i^{n_i}. \end{aligned}$$

故 $\prod_{i=1}^{k} p_i^{n_i} \mid a$.

□

3.5 主理想整环与 Euclid 环

定义 3.19

若交换幺环的每个理想都是主理想, 则称此环为**主理想环**. 一个主理想环若又是整环, 则称此环为**主理想整环**, 记为 p.i.d..

♣

命题 3.5

整环 $\mathbb{Z}$ 是主理想整环.

♠

证明 事实上, 设 I 为 $\mathbb{Z}$ 的一个非平凡理想, 于是 $\exists m \in I$ 满足

$$m = \min\{|k| \mid k \in I, k \neq 0\}.$$

$\forall k \in I$, 若 $k = 0$, 则 $k = 0 \cdot m$; 若 $k \neq 0$, 则 $\exists q, r \in \mathbb{Z}$, 满足 $k = qm + r (0 \leqslant r < m)$, 由 $I \lhd \mathbb{Z}$ 和 $m \in I$ 知 $qm \in I$, 于是 $r \in I$. 由 m 的取法知 $r = 0$, 即 $k = qm$, 否则与 m 的最小值定义矛盾! 故 $I = \{xm \mid x \in \mathbb{Z}\} = \langle m \rangle$, 因而 $\mathbb{Z}$ 是主理想整环.

□

例题 3.10 $\mathbb{Z}[x]$ 不是主理想整环.

证明 事实上, 若 $\mathbb{Z}[x]$ 是主理想整环, 则有 $g(x)$, 使得 $\langle 2, x^2+1\rangle = \langle g(x)\rangle$. 由定理 1.22(3)知

$$\left\{2u(x)+\left(x^2+1\right)v(x) \mid u(x), v(x) \in \mathbb{Z}[x]\right\} = \langle 2, x^2+1\rangle = \langle g(x)\rangle = \{u(x)g(x) \mid u(x) \in \mathbb{Z}[x]\}. \tag{3.23}$$

因为 $2 \in \langle 2, x^2+1\rangle$, 所以由(3.23)式知存在 $f(x) \in \mathbb{Z}[x]$, 使 $2 = f(x)g(x)$, 即 $g(x) \mid 2$, 故 $g(x) = \pm 1, \pm 2$. 另一方面, 由 $g(x) \in \langle 2, x^2+1\rangle$, 故由(3.23)式有 $u(x), v(x) \in \mathbb{Z}[x]$, 使得

$$g(x) = 2u(x) + (x^2+1)v(x).$$

令 $x = 1$, 则有 $g(1) = 2(u(1)+v(1))$. 于是 $g(x) = \pm 2$, 但 $\pm 2 \nmid (x^2+1)$, 即 $g(x) \nmid (x^2+1)$, 从而 $x^2+1 \notin \langle g(x)\rangle$. 这与(3.23)式矛盾! 因而 $\mathbb{Z}[x]$ 不是主理想整环.

□

定理 3.21

设 R 是交换整环, 则

(1) $a \mid b \iff \langle a\rangle \supseteq \langle b\rangle$.

(2) $a \sim b \iff \langle a\rangle = \langle b\rangle$.

(3) $a \sim 1 \iff \langle a\rangle = \langle 1\rangle = R$.

(4) R 满足因子链条件当且仅当 R 满足**主理想的升链条件**, 即任一**主理想升链**

$$\langle a_1\rangle \subseteq \langle a_2\rangle \subseteq \cdots \subseteq \langle a_n\rangle \subseteq \langle a_{n+1}\rangle \subseteq \cdots,$$

一定存在 $m \in \mathbb{N}$, 使得当 $n \geqslant m$ 时,$\langle a_n\rangle = \langle a_m\rangle$.

♡

证明

(1) 若 $a \mid b$, 则存在 $r_1 \in R$, 使 $b = r_1 a$. 从而由定理 1.22(3)知

$$\langle b\rangle = \{rb \mid r \in R\} = \{rr_1 a \mid r \in R\} \subseteq \{ra \mid r \in R\} = \langle a\rangle.$$

若 $\langle b\rangle \subseteq \langle a\rangle$, 则由定理 1.22(3)知

$$\langle b\rangle = \{rb \mid r \in R\} \subseteq \{ra \mid r \in R\} = \langle a\rangle.$$

于是由 $b \in \langle b\rangle$ 知存在 $r_1 \in R$, 使得 $b = r_1 a$, 故 $a \mid b$.

(2) 这就是(1)的直接推论.

(3) 这就是(2)的直接推论.

(4) 对任一主理想升链

$$\langle a_1\rangle \subseteq \langle a_2\rangle \subseteq \cdots \subseteq \langle a_n\rangle \subseteq \langle a_{n+1}\rangle \subseteq \cdots,$$

由结论 (2)知 $a_{n+1} \mid a_n (n \in \mathbb{N})$. 故

$$a_1, a_2, \cdots, a_n, a_{n+1}, \cdots$$

是 R 的因子链. 若 R 满足因子链条件, 则存在 $m \in \mathbb{N}$, 使得当 $n \geqslant m$ 时, 有 $a_n \sim a_m$. 由结论 (2), 此即 $\langle a_n\rangle = \langle a_m\rangle$.

若存在 $m \in \mathbb{N}$, 使得当 $n \geqslant m$ 时,$\langle a_n\rangle = \langle a_m\rangle$. 由结论 (2), 此即 $a_n \sim a_m$. 故此时 R 满足因子链条件.

□

定理 3.22

主理想整环一定是唯一析因环.

♡

证明 由定理 3.21(4)与定理 3.20(3), 只需证一个主理想整环 R 满足主理想升链条件与最大公因子条件. 设

$$\langle a_1\rangle \subseteq \langle a_2\rangle \subseteq \cdots \subseteq \langle a_n\rangle \subseteq \cdots$$

是 R 中一个主理想升链. 令 $I = \bigcup_{i=1}^{\infty} \langle a_i\rangle$. 若 $a, b \in I$, 则 $\exists i, j \in \mathbb{N}$, 使 $a \in \langle a_i\rangle, b \in \langle a_j\rangle$. 不妨设 $j \geqslant i$. 由此知 $a-b \in \langle a_j\rangle \subseteq I$, 故 I 是 R 中加法子群, 也是 Abel 群. 显然 I 对乘法封闭且满足结合律, 故 I 是 R 的子环. 又由定理

1.22(3)知 $\forall c \in R, ca \in \langle a_i \rangle \subseteq I$, 故 I 是 R 中理想. 由 R 是主理想整环知 $\exists d \in R$, 使 $I = \langle d \rangle$. 因 $d \in I$, 故 $\exists m \in \mathbb{N}$, 使 $d \in \langle a_m \rangle$, 因而当 $n \geqslant m$ 时, 由定理 1.22有

$$I = \langle d \rangle \subseteq \langle a_m \rangle \subseteq \langle a_n \rangle \subseteq \bigcup_{i=1}^{\infty} \langle a_i \rangle = I,$$

即 $\langle a_n \rangle = \langle a_m \rangle = I$. 这就证明了 R 满足主理想升链条件.

其次, 设 $a, b \in R^*$. 由定理 1.43(1)知 $\langle a \rangle + \langle b \rangle$ 是 R 的子环, 利用定理 1.22显然有 $R(\langle a \rangle + \langle b \rangle) \subseteq \langle a \rangle + \langle b \rangle$, 故 $\langle a \rangle + \langle b \rangle$ 是 R 中理想. 由 R 是主理想整环知 $\exists d \in R$, 使 $\langle a \rangle + \langle b \rangle = \langle d \rangle$, 因而有 $\langle a \rangle \subseteq \langle d \rangle, \langle b \rangle \subseteq \langle d \rangle$, 由定理 3.21(1)知 $d \mid a, d \mid b$, 即 d 为 a, b 的公因子. 又若 $c \mid a, c \mid b$, 则由定理 3.21(1)知 $\langle a \rangle \subseteq \langle c \rangle, \langle b \rangle \subseteq \langle c \rangle$, 故 $\langle d \rangle = \langle a \rangle + \langle b \rangle \subseteq \langle c \rangle$, 由定理 3.21(1)知 $c \mid d$, 故 d 为 a, b 的最大公因子.

综上知 R 为唯一析因环.

□

推论 3.9

设 R 是主理想整环, 若 d 为 a, b 的最大公因子, 则存在 $u, v \in R$, 使得

$$d = au + bv.$$

♡

证明 设 $a, b \in R^*$. 由定理 1.43(1)知 $\langle a \rangle + \langle b \rangle$ 是 R 的子环, 利用定理 1.22显然有 $R(\langle a \rangle + \langle b \rangle) \subseteq \langle a \rangle + \langle b \rangle$, 故 $\langle a \rangle + \langle b \rangle$ 是 R 中理想. 由 R 是主理想整环知 $\exists d_1 \in R$, 使 $\langle a \rangle + \langle b \rangle = \langle d_1 \rangle$, 因而有 $\langle a \rangle \subseteq \langle d_1 \rangle, \langle b \rangle \subseteq \langle d_1 \rangle$, 由定理 3.21(1)知 $d_1 \mid a, d_1 \mid b$, 即 d_1 为 a, b 的公因子. 又若 $c \mid a, c \mid b$, 则由定理 3.21(1)知 $\langle a \rangle \subseteq \langle c \rangle, \langle b \rangle \subseteq \langle c \rangle$, 故 $\langle d_1 \rangle = \langle a \rangle + \langle b \rangle \subseteq \langle c \rangle$, 由定理 3.21(1)知 $c \mid d_1$, 故 d_1 为 a, b 的最大公因子. 从而 $d_1 \sim d$, 再由定理 3.21(2)知 $\langle d \rangle = \langle d_1 \rangle = \langle a \rangle + \langle b \rangle$. 由定理 1.22知

$$\langle d \rangle = \langle a \rangle + \langle b \rangle = \{ua + bv \mid u, v \in R\}.$$

又 $d \in \langle d \rangle$, 故存在 $u, v \in R$, 使得

$$d = au + bv.$$

□

推论 3.10

设 R 是主理想整环, 若 d 为 a, b 的最大公因子, 则存在 $a_1, b_1 \in R$, 使得 $a = da_1, b = db_1$ 且 $(a_1, b_1) = 1$.

♡

证明 由 $d \mid a, b$ 知存在 $a_1, b_1 \in R$, 使 $a = da_1, b = db_1$. 于是由引理 3.5(5)知 $d = (a, b) = (da_1, db_1) \sim d(a_1, b_1)$. 从而存在 $r \in R$, 使 $d = d(a_1, b_1)r$. 由命题 1.11(1)知 R^* 对乘法满足消去律, 故 $1 = (a_1, b_1)r$. 因此 $(a_1, b_1) \in U$, 再由定理 3.15(8)知 $(a_1, b_1) \sim 1$.

□

推论 3.11

设 R 是主理想整环, a, b 互素 (即 $(a, b) \sim 1$) 的充要条件是 $\exists u, v \in R$, 使得

$$au + bv = 1.$$

♡

证明 必要性已含于推论 3.9中. 下证充分性. 设 $au + bv = 1 (u, v \in R)$, 若 $d = (a, b)$, 则 $d \mid a, d \mid b$, 故 $d \mid au + bv$, 因而 $d \mid 1$, 故 $d \sim 1$.

□

定义 3.20 (Euclid 环)

设 R 为交换整环. 若存在 R 到非负整数集 $\mathbb{N} \cup \{0\}$ 的映射 δ, 使得 $\forall a, b \in R, b \neq 0, \exists q, r \in R$ 满足

$$a = qb + r, \quad \delta(r) < \delta(b), \tag{3.24}$$

则称 R 为 **Euclid 环**. ♣

例题 3.11 $\mathbb{Z}$ 是 Euclid 环.

证明 事实上, 任何两个整数之间都可做带余除法, 故只需取 $\delta(m)=|m|$ 即可验证 δ 满足定义.

□

例题 3.12 设 $\mathbb{P}$ 为数域, 则 $\mathbb{P}[x]$ 是 Euclid 环. 定义 δ 为

$$\delta(f(x))=\begin{cases}2^{\deg f(x)}, & f(x)\neq 0,\\ 0, & f(x)=0.\end{cases}$$

不难验证 δ 满足Euclid 环所要求的条件.

例题 3.13 Gauss 整数环 $\mathbb{Z}[\sqrt{-1}]=\{a+b\sqrt{-1}\mid a,b\in\mathbb{Z}\}$ 是 Euclid 环.

证明 事实上, 令 $\delta(a+b\sqrt{-1})=a^2+b^2$, 则显然有

$$\delta(\alpha\beta)=\delta(\alpha)\delta(\beta),\quad \forall\alpha,\beta\in\mathbb{Z}[\sqrt{-1}].$$

设 $\beta\neq 0$. 不难看出其乘法逆元 $\beta^{-1}\in\mathbb{Q}[\sqrt{-1}]$, 即有

$$\alpha\beta^{-1}=\mu+\nu\sqrt{-1},\quad \mu,\nu\in\mathbb{Q}.$$

于是 $\exists c,d\in\mathbb{Z}$, 使得 $|c-\mu|\leqslant 1/2$, $|d-\nu|\leqslant 1/2$. 令 $\varepsilon=\mu-c$, $\eta=\nu-d$, 则有 $|\varepsilon|\leqslant 1/2$, $|\eta|\leqslant 1/2$, 而

$$\alpha=\beta((c+\varepsilon)+(d+\eta)\sqrt{-1})=\beta q+r,$$

其中, $q=c+d\sqrt{-1}\in\mathbb{Z}[\sqrt{-1}]$, $r=\beta(\varepsilon+\eta\sqrt{-1})=\alpha-\beta q\in\mathbb{Z}[\sqrt{-1}]$. 又

$$\delta(r)=|r|^2=\delta(\beta)(\varepsilon^2+\eta^2)\leqslant\delta(\beta)(1/4+1/4)<\delta(\beta),$$

故 $\mathbb{Z}[\sqrt{-1}]$ 为 Euclid 环.

□

定理 3.23

Euclid 环是主理想整环. 因而也是唯一析因环. ♡

注 确有主理想整环不是 Euclid 环. 例如, 环

$$D=\left\{a+\frac{b}{2}(1+\sqrt{-19})\mid a,b\in\mathbb{Z}\right\}$$

是一个主理想整环, 但不是 Euclid 环.

证明 设 I 是 Euclid 环 R 中的一个理想. 若 $I=\{0\}$, 显然是主理想, 故假设 $I\neq\{0\}$. 取 I 中元素 b, 使得

$$\delta(b)=\min\{\delta(c)\mid c\in I, c\neq 0\}. \tag{3.25}$$

设 $a\in I$, 则有 $q,r\in R$, 使

$$a=qb+r,\quad \delta(r)<\delta(b).$$

因 $a,b\in I$, 故 $r=a-qb\in I$. 由 b 的取法知 $r\notin I\setminus\{0\}$, 否则与 $\delta(b)$ 的最小值定义矛盾! 故 $r=0$, 因而 $a\in\langle b\rangle$, 故 $I=\langle b\rangle$. 即 R 为主理想环. 又 R 是整环, 故 R 为主理想整环. 再由定理 3.22知 Euclid 环也是唯一析因环.

□

命题 3.6 (辗转相除法)

设 R 是 Euclid 环,$R^*=R\setminus\{0\}$,$a,b\in R^*$, 求 a 与 b 的最大公因子. ♠

笔记 在 Euclid 环中, 可用辗转相除法来求两个元素的最大公因子.

解 不妨设 $\delta(a)\geqslant\delta(b)$, 并记 $a=a_1$, $b=a_2$. 于是 $\exists q_1,a_3\in R$, 使

$$a_1=q_1a_2+a_3,\quad \delta(a_3)<\delta(a_2).$$

若 $a_3=0$, 则由引理 3.5(5)和定理 3.15(3)知

$$(a_1,a_2)=(q_1a_2,a_2)=(q_1,1)\,a_2\sim a_2,$$

设 $a_3\neq 0$, 由推论 3.10知存在 $a_2',a_3'\in R$, 使 $a_2=a_2'(a_2,a_3)$,$a_3=a_3'(a_2,a_3)$ 且 $(a_2',a_3')=1$. 再由推论 3.11知存在 $u,v\in R$, 使

$$ua_2'+va_3'=1.$$

从而

$$v(q_1a_2'+a_3')+(u-vq_1)a_2'=ua_2'+va_3'=1.$$

又 $v,u-vq_1\in R$, 故由推论 3.11知 $(q_1a_2'+a_3',a_2')\sim 1$. 再利用引理 3.5(5)和定理 3.15(3)得

$$(a_1,a_2)=(q_1a_2+a_3,a_2)=(q_1a_2'(a_2,a_3)+a_3'(a_2,a_3),a_2'(a_2,a_3))\sim(q_1a_2'+a_3',a_2')(a_2,a_3)\sim(a_2,a_3).$$

再对 a_2,a_3 作除法运算

$$a_2=q_2a_3+a_4,\quad \delta(a_4)<\delta(a_3).$$

若 $a_4=0$, 则同理可知 $(a_1,a_2)\sim(a_2,a_3)\sim a_3$, 若 $a_4\neq 0$, 则同理可知 $(a_1,a_2)\sim(a_2,a_3)\sim(a_3,a_4)$. 再继续下去有

$$\delta(a_1)\geqslant\delta(a_2)>\delta(a_3)>\delta(a_4)>\cdots,$$

因为 $\delta(a_1)$ 是有限数, 所以在有限步后必然终止, 即有 $a_n\neq 0$, 而 $a_{n+1}=0$. 于是 $(a_1,a_2)\sim a_n$. 综上, 存在 $a_3,a_4,\cdots,a_n$ 以及 $q_1,q_2,\cdots,q_{n-1}$, 使得

$$\begin{aligned}
a_1&=q_1a_2+a_3,\quad \delta(a_3)<\delta(a_2);\\
a_2&=q_2a_3+a_4,\quad \delta(a_4)<\delta(a_3);\\
&\cdots\cdots\cdots\\
a_{n-2}&=q_{n-2}a_{n-1}+a_n,\quad \delta(a_n)<\delta(a_{n-1});\\
a_{n-1}&=q_{n-1}a_n,\quad \delta(a_n)<\delta(a_{n-1}).
\end{aligned}$$

并且

$$(a_1,a_2)\sim(a_2,a_3)\sim\cdots\sim(a_{n-1},a_n)\sim a_n.$$

□

3.6 域上一元多项式

定义 3.21

设 $R[x]$ 是交换整环 R 上的一元多项式环, 若 $f(x)\in R[x]$ 且 $f(x)\neq 0$, 有

$$f(x)=a_0+a_1x+\cdots+a_nx^n,\quad a_n\neq 0.$$

则 a_ix^i 称为 $f(x)$ 的 ***i* 次项**,a_i 称为 i 次项的**系数**,a_0 称为**常数项**,a_nx^n 称为**首项**,n 称为 $f(x)$ 的**次数**, 记为 $\deg f(x)=n$. 如果 $f(x)\neq 0$ 且 $f(x)$ 的首项系数为 1, 则称 $f(x)$ 为**首一多项式**. 今后以 $(f(x),g(x))$ 表示 $f(x),g(x)$ 的最大公因式中的首一多项式.

若 $f(x)=a_0\neq 0$, 则记 $\deg f(x)=0$, 一般对零元素 0 是不规定次数的, 但规定 0 的次数为 $-\infty$, 即 $\deg 0=-\infty$ 且规定

$$-\infty+(-\infty)=-\infty,\quad -\infty+n=-\infty,\quad -\infty<n,\quad 2^{-\infty}=0.$$

♣

定理 3.24

设 $R[x]$ 是交换整环 R 上的一元多项式环,$R^* = R \setminus \{0\}$,$f(x), g(x) \in R[x]$, 则

(1) $\deg f(x) = 0 \iff f(x) \in R^*$.

(2) $\deg(f(x) + g(x)) \leqslant \max\{\deg f(x), \deg g(x)\}$.

(3) $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$.

(4) 令 $\delta(f(x)) = 2^{\deg f(x)}$, 则有

$$\deg f(x) < \deg g(x) \iff \delta(f(x)) < \delta(g(x)),$$

$$\delta(f(x)g(x)) = \delta(f(x))\delta(g(x)).$$

(5) 首一多项式的乘积仍为首一多项式.

(6) $R[x]$ 也是交换整环且 $R[x]$ 的单位就是 R 的单位.

(7) R 上 n 元多项式环 $R[x_1, x_2, \cdots, x_n]$ 也是交换整环且其单位就是 R 的单位.

♡

证明

(1)

(2)

(3)

(4)

(5)

(6)

(7)

□

定理 3.25

设 F 是一个域,$F[x]$ 为 F 上一元多项式环, 则

(1) $\forall f(x), g(x) \in F[x]$, $g(x) \neq 0$, 存在唯一的一对多项式 $q(x), r(x)$, 使得

$$f(x) = q(x)g(x) + r(x), \quad \deg r(x) < \deg g(x);$$

分别称 $q(x), r(x)$ 为 $f(x)$ 除以 $g(x)$ 的**商**、**余式**.

(2) $F[x]$ 是 Euclid 环.

♡

注 由这个定理的结论 (2) 知 $F[x]$ 是 Euclid 环, 故再由定理 3.23知 $F[x]$ 是主理想整环, 进而也是唯一析因环.

证明

(1) 首先证明 $q(x), r(x)$ 的存在性. 对 $\deg f(x)$ 作归纳. 设 $\deg g(x) = m$. 由假设知 $m \geqslant 0$, 当 $\deg f(x) < m$ 时可取 $q(x) = 0$, 即 $r(x) = f(x)$. 现设 $\deg f(x) < n$ 时,$q(x)$ 与 $r(x)$ 已存在. 设 $\deg f(x) = n$. 不妨设 $n \geqslant m$. 又设

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0,$$

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0.$$

由 $b_m \neq 0$, 取 $q_0(x) = a_n b_m^{-1} x^{n-m}$. 令

$$f_1(x) = f(x) - q_0(x)g(x) = (a_{n-1} - a_n b_m^{-1} b_{m-1})x^{n-1} + \cdots,$$

故 $\deg f_1(x) \leqslant n - 1 < n$. 由归纳假设有 $q_1(x), r_1(x)$, 使得

$$f_1(x) = q_1(x)g(x) + r_1(x), \quad \deg r_1(x) < \deg g(x),$$

因而有

$$f(x) = q_0(x)g(x) + q_1(x)g(x) + r_1(x) = (q_0(x) + q_1(x))g(x) + r_1(x).$$

取 $q(x) = q_0(x) + q_1(x), r(x) = r_1(x)$, 它们满足定理条件.

下面证明 $q(x)$ 与 $r(x)$ 的唯一性. 设有 $q_2(x), r_2(x)$ 也满足

$$f(x) = q_2(x)g(x) + r_2(x), \quad \deg r_2(x) < \deg g(x),$$

于是有 $(q(x) - q_2(x))g(x) = r_2(x) - r(x)$. 若 $q(x) - q_2(x) \neq 0$, 则

$$\deg(r_2(x) - r(x)) \geqslant \deg g(x) > \max\{\deg r_2(x),\ \deg r(x)\}.$$

另一方面有

$$\deg(r_2(x) - r(x)) \leqslant \max\{\deg r_2(x),\ \deg r(x)\},$$

这就导出矛盾. 故 $q(x) = q_2(x), r_2(x) = r(x)$. $q(x)$ 与 $r(x)$ 的唯一性得证.

(2) 令 $\delta(f(x)) = 2^{\deg f(x)}$, 注意到 $\deg r(x) < \deg g(x)$, 由定理 3.24(4)得

$$\delta(r(x)) < \delta(g(x)),$$

故 $F[x]$ 为 Euclid 环.

□

定义 3.22

设 F 是一个域,$F[x]$ 为 F 上一元多项式环, 若 $f_1(x)$ 与 $f_2(x)$ 除以 $g(x)$ 的余式相同, 则称 $f_1(x)$ 与 $f_2(x)$ 模 $g(x)$ **同余**. 记为 $f_1(x) \equiv f_2(x) \pmod{g(x)}$.

♣

推论 3.12

设 $F[x]$ 为域 F 上的一元多项式环,$f_1(x), f_2(x), g(x) \in F[x]$ 且 $g(x) \neq 0$, 则

$$f_1(x) \equiv f_2(x) \pmod{g(x)} \iff g(x) \mid (f_1(x) - f_2(x)),$$

而且 $f_1(x) \equiv f_2(x) \pmod{g(x)}$ 无论对 $F[x]$ 的加法或乘法都是同余关系.

♡

证明 $f_1(x) \equiv f_2(x) \pmod{g(x)}$ 当且仅当存在 $q_1(x), q_2(x), r(x) \in F[x]$, 使

$$f_1(x) = q_1(x)g(x) + r(x), \quad f_2(x) = q_2(x)g(x) + r(x).$$

这也当且仅当

$$f_1(x) - f_2(x) = (q_1(x) - q_2(x))g(x) \iff g(x) \mid (f_1(x) - f_2(x)).$$

设 $f_1(x) \equiv f_2(x) \pmod{g(x)}, f_3(x) \equiv f_4(x) \pmod{g(x)}$, 则存在 $q_1(x), q_2(x), q_3(x), q_4(x), r_1(x), r_2(x) \in F[x]$, 使

$$f_1(x) = q_1(x)g(x) + r_1(x), \quad f_2(x) = q_2(x)g(x) + r_1(x),$$
$$f_3(x) = q_3(x)g(x) + r_2(x), \quad f_4(x) = q_4(x)g(x) + r_2(x).$$

于是

$$f_1(x) + f_3(x) = (q_1(x) + q_3(x))g(x) + r_1(x) + r_2(x),$$
$$f_2(x) + f_4(x) = (q_2(x) + q_4(x))g(x) + r_1(x) + r_2(x),$$
$$f_1(x)f_3(x) = (q_1(x)q_3(x)g(x) + q_1(x)r_2(x) + q_3(x)r_1(x))g(x) + r_1(x)r_2(x),$$
$$f_2(x)f_4(x) = (q_2(x)q_4(x)g(x) + q_2(x)r_2(x) + q_4(x)r_1(x))g(x) + r_1(x)r_2(x).$$

故

$$f_1(x) + f_3(x) \equiv f_2(x) + f_4(x) \pmod{g(x)},$$
$$f_1(x)f_3(x) \equiv f_2(x)f_4(x) \pmod{g(x)}.$$

因此 $f_1(x) \equiv f_2(x) \pmod{g(x)}$ 对 $F[x]$ 的加法和乘法都是同余关系.

□

定义 3.23

设 F 是一个域,$F[x]$ 为 F 上一元多项式环, 若 $c \in F$ 且使 $f(c)=0$, 则称 c 是 $f(x)$ 的一个**根**.

推论 3.13

设 $F[x]$ 为域 F 上的一元多项式环且 $f(x) \in F[x], c \in F$, 则

$$f(x) \equiv f(c) \pmod{(x-c)} \tag{3.26}$$

且 $(x-c) \mid f(x) \iff f(c)=0 \iff c$是$f(x)$的根.

证明 事实上, 由定理 3.5,F 的恒等映射 id_F 可开拓为 $F[x]$ 到 F 的同态 η, 使得

$$\eta_F = \mathrm{id}_F, \quad \eta(x) = c.$$

从而

$$\eta(f(x)) = f(c), \quad \forall f(x) \in F[x].$$

现因 $\deg(x-c)=1$, 故 $\exists q(x) \in F[x]$, $r \in F$, 使得

$$f(x) = (x-c)q(x) + r.$$

两边作用以 η, 则有

$$f(c) = (c-c)q(c) + r = r,$$

因而式(3.26)成立. 特别地,$(x-c) \mid f(x) \iff f(x) \equiv 0 \pmod{(x-c)} \iff f(c)=0$.

□

推论 3.14

设 F 是一个域,$F[x]$ 为 F 上一元多项式环,$f(x) \in F[x], c_i \in F(i=1,2,\cdots,k)$, 若 $c_1, c_2, \cdots, c_k$ 是 $f(x)$ 的互不相同的根, 则有 $\prod_{i=1}^{k}(x-c_i) \mid f(x)$, 从而 $k \leqslant \deg f(x)$.

证明 显然 $x-c_i$ 是 $F[x]$ 中不可约元素, 由定理 3.25(2)知 $F[x]$ 是 Euclid 环, 又由定理 3.23知 $F[x]$ 是唯一析因环. 再由定理 3.20知 $F[x]$ 满足素性条件. 因而 $x-c_i$ 是素元素. 又由 $c_i \neq c_j$ $(i \neq j, 1 \leqslant i, j \leqslant k)$. 由

$$\frac{1}{c_i - c_j}(x-c_j) - \frac{1}{c_i - c_j}(x-c_i) = 1$$

及定理 3.11知 $(x-c_i, x-c_j)=1$. 又由推论**??**知 $(x-c_i) \mid f(x)$, 故由定理**??**知 $\prod_{i=1}^{k}(x-c_i) \mid f(x)$, 从而 $k \leqslant \deg f(x)$.

□

命题 3.7

设 S 为交换整环,R 为 S 的子环且 $1 \in R$, 则 $f(x) \in R[x]$ 在 S 中不同根的个数不超过 $\deg f(x)$.

注 设 R 为交换幺环,S 为 R 的扩环,$f(x) \in R[x]$,$\deg f(x) > 0$, 那么 $f(x)$ 在 S 中不同根的数目是否超过 $\deg f(x)$? 如果 S 为交换整环, 则回答是肯定的. 若 S 非交换或有零因子则不然.

证明 事实上, 设 F 为 S 的分式域. 于是 $R[x] \subseteq S[x] \subseteq F[x]$, 即 $f(x) \in F[x]$. 由推论 3.14知结论成立.

□

例题 3.14 设 $\mathbf{H}$ 为四元数体 (见定理 1.18), 由命题 1.13知

$$\mathbf{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\},$$

因而 $\{a + 0\cdot i + 0\cdot j + 0\cdot k \mid a \in \mathbb{R}\} \cong \mathbb{R}$ 是 $\mathbf{H}$ 的一个子环. 由命题 1.13知 $i^= j^2 = k^2 = -1$, 故 i, j, k 都是 $\mathbb{R}$ 上的多项式 x^2+1 的根, 从而 $bi + cj + dk$ 都是 x^2+1 的根, 因此 x^2+1 在 $\mathbf{H}$ 中有无穷多个根.

例题 3.15 设 $R=S=\mathbb{Z}_8$. 不难看出 $x^2-1\in R[x]$ 有 4 个不同的根 $\overline{1},\overline{3},\overline{5},\overline{7}$, 其中,$\overline{n}$ 表示 $n+8\mathbb{Z}$.

命题 3.8

设 $a,b\in\mathbb{N}$, 若 $a\nmid b$, 则存在素数 p, 使得

$$a=p^rl,\quad b=p^sk,\quad (p,l)=(p,k)=(p,lk)=1,\quad r>s.$$

♠

证明 由算术基本定理知, 存在 $n\in\mathbb{N}$ 以及互不相同的素数 $p_1,p_2,\cdots,p_n$, 使得

$$a=\prod_{i=1}^n p_i^{k_i},\quad b=\prod_{i=1}^n p_i^{k_i'},$$

其中 $k_i,k_i'\in\mathbb{N}$. 因为 $a\mid b$ 当且仅当 $k_i\leqslant k_i',i=1,2,\cdots,n$, 所以由 $a\nmid b$ 可得, 存在 $i_0\in\{1,2,\cdots,n\}$, 使得 $k_{i_0}>k_{i_0}'$. 于是记 $p=p_{i_0},r=k_{i_0},s=k_{i_0}',l=\prod\limits_{i\neq i_0}p_i^{k_i},k=\prod\limits_{i\neq i_0}p_i^{k_i'}$, 则 $r>s$ 且

$$a=p_{i_0}^{k_{i_0}}\prod_{i\neq i_0}p_i^{k_i}=p^rl,\quad b=p_{i_0}^{k_{i_0}'}\prod_{i\neq i_0}p_i^{k_i'}=p^sk.$$

由 $p_1,p_2,\cdots,p_n$ 是互不相同的素数可知 $(p,l)=(p,k)=1$, 故 $(p,lk)=1$.

□

定理 3.26

设 F 是一个域,G 是 $F^*=F\setminus\{0\}$ 的一个有限的乘法子群, 则 G 为循环群.

♡

证明 设 $|G|=n$,g 是 G 中最大阶的元素且其阶为 m, 因而 $\langle g\rangle=\{1,g,g^2,\cdots,g^{m-1}\}\subseteq G$, 由Lagrange 定理知 $m|n$. 任取 $h\in G$, 设 h 的阶为 m_1, 如果 $m_1\nmid m$, 则由命题 3.8知有素数 p, 使得

$$m_1=p^rl,\quad m=p^sk,\quad (p,l)=(p,k)=(p,lk)=1,\quad r>s.$$

由 h 的阶为 m_1, 故 h^l 的阶为 p^r,g^{p^s} 的阶为 k, 由于 G 为 Abel 群, 故 $h^lg^{p^s}=g^{p^s}h^l$,$(p^r,k)=1$, 由定理 1.48(5)知 $h^lg^{p^s}$ 的阶为 p^rk, 但 $p^rk>p^sk=m$. 这与 m 的选取矛盾, 故 $m_1|m$.

由此得 $\forall h\in G$,h 都是 x^m-1 的根, 即 $G\subseteq\{x\mid x^m-1=0\}$. 由命题 3.7知 x^m-1 至多有 m 个根, 又 $\langle g\rangle$ 中 m 个元素都是 x^m-1 的根, 故 $\langle g\rangle\subseteq\{x\mid x^m-1=0\}$ 且 $|\{x\mid x^m-1=0\}|=m=|\langle g\rangle|$, 因此 $\langle g\rangle=\{x\mid x^m-1=0\}$. 于是 $G\subseteq\langle g\rangle$. 故 $G=\langle g\rangle$, 这就证明了 G 是循环群.

□

推论 3.15

有限域 F 的非零元素集 F^* 对乘法为循环群.

♡

注 这个推论对有限域理论是很重要的.

证明 由定理 3.26立得.

□

定理 3.27

设 F 为域,$f(x),g(x)\in F[x]^*=F[x]\setminus\{0\}$, 则 $f(x),g(x)$ 非互素的充分必要条件为 $\exists f_0(x),g_0(x)\in F[x]^*$, 使得

$$g_0(x)f(x)=f_0(x)g(x),$$

其中,

$$0\leqslant\deg f_0(x)<\deg f(x),\quad 0\leqslant\deg g_0(x)<\deg g(x).$$

♡

证明 显然这样的最大公因式是唯一的. 设 $d(x)=(f(x),g(x))$, 于是有 $f(x)=d(x)f_0(x)$,$g(x)=d(x)g_0(x)$. 由 $f(x),g(x)$ 非互素, 故 $\deg d(x)>0$, 因而

$$0\leqslant\deg f_0(x)<\deg f(x),\quad 0\leqslant\deg g_0(x)<\deg g(x)$$

且有

$$g_0(x)f(x) = d(x)f_0(x)g_0(x) = f_0(x)g(x).$$

由此知必要性成立.

反之, 假设 $(f(x), g(x)) = 1$, 于是 $\exists u(x), v(x) \in F[x]$, 使 $u(x)f(x) + v(x)g(x) = 1$, 因而有

$$\begin{aligned} f_0(x) &= f_0(x) \cdot 1 = f_0(x)u(x)f(x) + v(x)f_0(x)g(x) \\ &= f(x)(f_0(x)u(x) + v(x)g_0(x)), \end{aligned}$$

即得 $\deg f_0(x) \geqslant \deg f(x)$. 这与条件矛盾, 故 $(f(x), g(x)) \neq 1$.

□

推论 3.16

设 F 为域, $f(x), g(x) \in F[x]^* = F[x] \setminus \{0\}$, 记

$$f(x) = \sum_{k=0}^{n} a_k x^{n-k}, \quad a_0 \neq 0, n \in \mathbb{N},$$

$$g(x) = \sum_{k=0}^{m} b_k x^{m-k}, \quad b_0 \neq 0, m \in \mathbb{N}.$$

再记

$$f_0(x) = \sum_{k=1}^{n} x_k x^{n-k}, \quad g_0(x) = \sum_{k=1}^{m} x_{n+k} x^{m-k},$$

则 $(f(x), g(x)) \neq 1$ 当且仅当存在 $(x_1, x_2, \cdots, x_{m+n}) \neq 0$, 使 $f(x)g_0(x) = g(x)f_0(x)$,

♡

证明 由定理 3.27立得.

□

定义 3.24 (结式/Sylvester 行列式)

设 F 是一个域, $f(x), g(x) \in F[x]^* = F[x] \setminus \{0\}$, 则称

$$R(f,g) = \begin{vmatrix} a_0 & a_1 & \cdots & \cdots & a_n & & & \\ & a_0 & a_1 & \cdots & \cdots & a_n & & \\ & & \ddots & \ddots & & & \ddots & \\ & & & a_0 & a_1 & \cdots & \cdots & a_n \\ b_0 & b_1 & \cdots & \cdots & b_m & & & \\ & b_0 & b_1 & \cdots & \cdots & b_m & & \\ & & \ddots & \ddots & & & \ddots & \\ & & & b_0 & b_1 & \cdots & \cdots & b_m \end{vmatrix},$$

为 $f(x)$ 与 $g(x)$ 的**结式**或 **Sylvester 行列式**. 显然有

$$\begin{cases} \mathrm{ent}_{i\ i+j}(R(f,g)) = a_j, & 1 \leqslant i \leqslant m,\ 0 \leqslant j \leqslant n, \\ \mathrm{ent}_{n+i\ i+j}(R(f,g)) = b_j, & 1 \leqslant i \leqslant n,\ 0 \leqslant j \leqslant m, \\ \mathrm{ent}_{i\ j}(R(f,g)) = 0, & \text{其他}. \end{cases}$$

♣

定理 3.28

设 F 是一个域, $f(x), g(x) \in F[x]^* = F[x] \setminus \{0\}$ 非互素的充分必要条件是 $f(x)$ 与 $g(x)$ 的结式 $R(f,g) = 0$.

♡

证明 记

$$f(x)=\sum_{k=0}^{n}a_kx^{n-k},\quad a_0\neq 0,n\in\mathbb{N},$$
$$g(x)=\sum_{k=0}^{m}b_kx^{m-k},\quad b_0\neq 0,m\in\mathbb{N}.$$

再记

$$f_0(x)=\sum_{k=1}^{n}x_kx^{n-k},\quad g_0(x)=\sum_{k=1}^{m}x_{n+k}x^{m-k},$$

由推论 3.16知 $(f(x),g(x))\neq 1$ 当且仅当存在 $(x_1,x_2,\cdots,x_{m+n})\neq 0$, 使 $f(x)g_0(x)=g(x)f_0(x)$, 所以有

$$\sum_{l=0}^{n+m-1}\left(\sum_{\substack{j+k=l\\0\leqslant k\leqslant m-1}}a_jx_{k+n+1}\right)x^{n+m-1-l}=\sum_{r=0}^{n+m-1}\left(\sum_{\substack{p+q=r\\0\leqslant q\leqslant n-1}}b_px_{q+1}\right)x^{n+m-1-r}.$$

由对应项系数相等, 即得

$$\sum_{\substack{j+k=l\\0\leqslant k\leqslant m-1}}a_jx_{k+n+1}=\sum_{\substack{p+q=r\\0\leqslant q\leqslant n-1}}b_px_{q+1},\quad l=r=0,1,\cdots,n+m-1.$$

这样得到一个齐次线性方程组

$$\boldsymbol{A}^T\mathbb{X}=\curlywedge,$$

其中,$\mathbb{X}=(x_1,x_2,\cdots,x_{m+n})'$,

$$\begin{cases}\mathrm{ent}_{i,i+j}(\boldsymbol{A})=b_j, & 1\leqslant i\leqslant n,\ 0\leqslant j\leqslant m,\\ \mathrm{ent}_{n+i,i+j}(\boldsymbol{A})=-a_j, & 1\leqslant i\leqslant m,\ 0\leqslant j\leqslant n,\\ \mathrm{ent}_{i,j}(\boldsymbol{A})=0, & \text{其他}.\end{cases}$$

显然当且仅当 $\det\boldsymbol{A}=0$ 时才能找到定理 3.27中的 $f_0(x)$ 与 $g_0(x)$. 又注意到 $R(f,g)=\pm\det\boldsymbol{A}$, 故 $(f(x),g(x))\neq 1$ 当且仅当 $R(f,g)=0$.

□

例题 3.16 设 $f(x)=x^2+x+1,g(x)=x^3-1\in\mathbb{Q}[x]$. 证明 $f(x),g(x)$ 不互素并求 $f_0(x),g_0(x)$, 使得 $f(x)g_0(x)=g(x)f_0(x)$.

解

$$R(f,g)=\begin{vmatrix}1&1&1&0&0\\0&1&1&1&0\\0&0&1&1&1\\1&0&0&-1&0\\0&1&0&0&-1\end{vmatrix}=0.$$

故由定理 3.28知 $f(x),g(x)$ 不互素. 令 $f_0(x)=1,g_0(x)=x-1$, 则 $f(x)g_0(x)=g(x)f_0(x)$.

□

命题 3.9

设

$$f(x)=(x-x_1)(x-x_2)\cdots(x-x_n)=x^n+a_1x^{n-1}+\cdots+a_n,$$
$$g(x)=(x-y_1)(x-y_2)\cdots(x-y_m)=x^m+b_1x^{m-1}+\cdots+b_m,$$

证明

$$R(f,g)=\prod_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant m}}(x_i-y_j).$$

♠

证明 注意 $(-1)^i a_i,(-1)^j b_j$ 分别是 $x_1,x_2,\cdots,x_n$ 的 i 次初等对称多项式,$y_1,y_2,\cdots,y_m$ 的 j 次初等对称多项式.

在行列式 $R(f,g)$ 按组合求和定义的完全展开式中任一非零项

$$\prod_{i=1}^{m+n} \mathrm{ent}_{i\ \sigma(i)} R(f,g), \quad \sigma \in S_{m+n}$$

是 $x_1,x_2,\cdots,x_n,y_1,y_2,\cdots,y_m$ 的齐次多项式, 其次数为

$$\sum_{i=1}^{m}(\sigma(i)-i)+\sum_{i=m+1}^{m+n}(\sigma(i)-(i-m))=\sum_{i=1}^{m+n}\sigma(i)-\sum_{i=1}^{m+n} i+mn=mn.$$

因此,$R(f,g)$ 是 $x_1,x_2,\cdots,x_n,y_1,y_2,\cdots,y_m$ 的 mn 次齐次多项式.

当 $x_i=y_j$ 时, 此时 $f(x),g(x)$ 有公共根, 从而 $f(x),g(x)$ 不互素, 故由定理 3.28知 $R(f,g)=0$. 将 $R(f,g)$ 视为关于 x_i 的一元多项式, 则 y_j 为其根. 于是 $(x_i-y_j)\mid R(f,g)$, 所以

$$\prod_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}} (x_i-y_j)\mid R(f,g).$$

又 $\deg \prod\limits_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}} (x_i-y_j)=mn=\deg R(f,g)$, 于是

$$\prod_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}} (x_i-y_j)=\pm R(f,g).$$

注意

$$\prod_{i=1}^{m+n} \mathrm{ent}_{i\ i} R(f,g)=a_0^m b_m^n=(-1)^{mn}(y_1y_2\cdots y_m)^n,$$

$\prod\limits_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}} (x_i-y_j)$ 中 $(y_1y_2\cdots y_m)^n$ 的系数亦为 $(-1)^{mn}$, 因此有

$$R(f,g)=\prod_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}} (x_i-y_j).$$

□

3.7 唯一析因环的多项式环

定义 3.25 (容度)

设 R 为唯一析因环,$f(x)=\sum\limits_{k=0}^{n} a_k x^k\in R[x]$. 若 $f(x)\neq 0$, 则称 $a_0,a_1,\cdots,a_n$ 的最大公因子为 $f(x)$ 的**容度**, 记为 $c(f(x))$ 或 $c(f)$.

♣

注 由引理 3.5(1)知 $f(x)$ 的容度 $c(f)$ 在相伴意义下是唯一的. 由引理 3.5(5)易知 $c(df(x))=d\cdot c(f(x)),\forall d\in R$.

定义 3.26 (本原多项式)

若 $f(x)\in R[x],f(x)\neq 0,c(f)\sim 1$, 则称 $f(x)$ 为**本原多项式**.

♣

注 设 $R[x]$ 的单位群也就是 R 的单位群 U, 于是若 $f(x)\in U$, 则 $c(f)\sim 1$.

定理 3.29

设 $R[x]$ 是唯一析因环 R 上的一元多项式环, 则有下列结论:

(1) $R[x]$ 中任一非零多项式 $f(x)$ 是 $c(f)$ 与一本原多项式 $f_1(x)$ 的积, 即

$$f(x) = c(f)f_1(x) \tag{3.27}$$

且这种分解在相伴意义下唯一;

(2) 次数大于零的不可约多项式是本原多项式;

(3) 本原多项式的积为本原多项式.

♡

证明

(1) 设 $c(f) = d, f(x) = \sum_{k=0}^{n} a_k x^k$, 于是 $a_k = da'_k$, 因而由引理 3.5(5)知 $d(a'_0, a'_1, \cdots, a'_n) \sim (a_0, a_1, \cdots, a_n) = d$, 从而再由定理 3.15(3)知 $(a'_0, a'_1, \cdots, a'_n) \sim 1$, 故 $f_1(x) = \sum_{k=0}^{n} a'_k x^k$ 为本原多项式且式(3.27)成立.

若另有 $f(x) = d_1 f_2(x), d_1 \in R, c(f_2) \sim 1$, 则 $d_1 c(f_2) \sim c(d_1 f_2(x)) \sim c(f) = d$, 故由定理 3.15(3)知 $d_1 \sim d$, 再由定理 3.15(6)知 $d_1 = du(u \in U)$, 因而 $f(x) = df_1(x) = duf_2(x)$, 从而由命题 1.11(1)得 $f_1(x) = uf_2(x)$, 由定理 3.15(6)知 $f_1(x) \sim f_2(x)$, 亦即 $f(x)$ 的上述分解在相伴意义下唯一.

(2) 设 $f(x)$ 不可约且 $\deg f(x) > 0, d = c(f)$. 由结论 (1) 知 $f(x) = df_1(x)$. 由 $\deg f(x) > 0$ 知 $\deg f_1(x) > 0$, 从而 $f_1(x) \notin U$. 若 $d \notin U$, 则 $f(x)$ 有非平凡的真因子 d, 与 $f(x)$ 不可约矛盾. 故必有 $d \in U$, 即 $c(f) = d \sim 1$, 即 $f(x)$ 是本原的.

(3) 设 $f(x) = \sum_{k=0}^{n} a_k x^k, a_n \neq 0; g(x) = \sum_{k=0}^{m} b_k x^k, b_m \neq 0$ 都是本原多项式. 又

$$h(x) = f(x)g(x) = \sum_{k=0}^{m+n} c_k x^k,$$

其中,

$$c_k = \sum_{i+j=k} a_i b_j, \quad k = 0, 1, \cdots, m+n.$$

假设 $c(h) \notin U$, 则由有限析因条件和定理 3.20知有 R 中素元素 $p | c(h)$, 即有 $p | c_k (k = 0, 1, \cdots, m+n)$.

由 $c(f) \sim c(g) \sim 1$ 及引理 3.5(3)知 $(p, c(f)) \sim (p, c(g)) \sim (p, 1) \sim 1$. 因此 p 于是由引理 3.5(9)知存在 r, s, 使得

$$p | a_i, 0 \leqslant i \leqslant r-1, \quad p \nmid a_r; \quad p | b_j, 0 \leqslant i \leqslant s-1, \quad p \nmid b_s,$$

再由

$$c_{r+s} = \sum_{i+j=r+s} a_i b_j = a_r b_s + \sum_{\substack{i<r, \\ i+j=r+s}} a_i b_j + \sum_{\substack{j<s, \\ i+j=r+s}} a_i b_j$$

及 $p \mid c_{r+s}$ 可知

$$p \left| \sum_{\substack{i<r, \\ i+j=r+s}} a_i b_j, \quad p \right| \sum_{\substack{j<s, \\ i+j=r+s}} a_i b_j, \quad p | a_r b_s,$$

这与 $p \nmid a_r, b_s$ 矛盾! 故 $c(h) \sim 1$, 即 $f(x)g(x)$ 是本原多项式.

□

定理 3.30

设 F 是唯一析因环 R 的分式域. 于是 $F[x] \supseteq R[x]$. 又设 S 为 $R[x]$ 中本原多项式的集合, $R[x]$ 中相伴关系记为 $\overset{R}{\sim}$, $F[x]$ 中相伴关系记为 $\overset{F}{\sim}$, 则有下列结论:

(1) $\forall f(x) \in F[x], f(x) \neq 0, \exists g(x) \in S$, 使 $f(x) \overset{F}{\sim} g(x)$ 且 $g(x)$ 在 $\overset{R}{\sim}$ 意义下是唯一的;

(2) 设 $f_1(x), f_2(x) \in F[x], g(x), g_1(x), g_2(x) \in S$ 且

$$f_1(x) \overset{F}{\sim} g_1(x), \quad f_2(x) \overset{F}{\sim} g_2(x), \quad f_1(x)f_2(x) \overset{F}{\sim} g(x),$$

则有

$$g_1(x)g_2(x) \overset{R}{\sim} g(x);$$

(3) 设 $f(x) \in R[x], \deg f(x) \geqslant 1$, 则 $f(x)$ 在 $R[x]$ 中不可约的充要条件是 $f(x)$ 在 $F[x]$ 中也不可约.

♡

证明

(1) 设 $f(x) = \sum_{k=0}^{n} d_k x^k \in F[x]$, 即 $d_k \in F$. 于是由 F 是 R 的分式域知 $d_k = \frac{a_k}{b_k}, a_k, b_k \in R, b_k \neq 0, 0 \leqslant k \leqslant n$. 令 $b = b_0 b_1 \cdots b_n$, 则有

$$d_k b = a_k \prod_{i \neq k} b_i \in R, \quad 0 \leqslant k \leqslant n.$$

再令 $d = (d_0 b, d_1 b, \cdots, d_n b) \in R \setminus \{0\}$, 则由 $d \mid d_k b$ 知存在 $c_k \in R \setminus \{0\}$, 使 $dc_k = d_k b$. 于是由引理 3.5(5)知

$$d(c_0, c_1, \cdots, c_n) \overset{R}{\sim} (dc_0, dc_1, \cdots, dc_n) = (d_0 b, d_1 b, \cdots, d_n b) = d.$$

于是再由定理 3.15(3)得

$$(c_0, c_1, \cdots, c_n) \overset{R}{\sim} 1.$$

而

$$f(x) = \frac{d}{b} \sum_{k=0}^{n} c_k x^k = \frac{d}{b} g(x),$$

其中 $\frac{d}{b} \in F, g(x) = \sum_{k=0}^{n} c_k x^k \in R[x], (c_0, c_1, \cdots, c_n) \overset{R}{\sim} 1$, 故 $g(x) \in S$ 且 $g(x) = \frac{b}{d} f(x)$. 这样得到 $f(x) \overset{F}{\sim} g(x)$.

现设 $f(x) \overset{F}{\sim} g_1(x), g_1(x) \in S$. 又 $f(x) \overset{F}{\sim} g(x)$, 所以 $g_1(x) \overset{F}{\sim} g(x)$, 即 $\exists u \in F^*$, 使 $g_1(x) = ug(x)$. 又 $u = \frac{d'}{d}, d', d \in R$, 故有 $dg_1(x) = d'g(x) \in R[x]$. 由定理 3.29(1)知 $d'g(x)$ 是其自身的一个分解, 从而 $g_1(x) \overset{R}{\sim} g(x)$. 唯一性得证.

(2) 由于 $f_1(x) \overset{F}{\sim} g_1(x), f_2(x) \overset{F}{\sim} g_2(x)$, 故由相伴关系对乘法构成同余关系知

$$f_1(x)f_2(x) \overset{F}{\sim} g_1(x)g_2(x) \overset{F}{\sim} g(x).$$

由定理 3.29(3)知 $g_1(x)g_2(x) \in S$. 再由本定理的结论 (1)知 $g_1(x)g_2(x) \overset{R}{\sim} g(x)$.

(3) **必要性**: 用反证法证明. 假设 $f(x)$ 作为 $F[x]$ 中的多项式是可约的, 由 $F[x]$ 的单位群为 F^*, 故有 $f_1(x), f_2(x) \in F[x]$ 且 $\deg f_i(x) \geqslant 1$, 使得 $f(x) = f_1(x)f_2(x)$. 由本定理的结论 (1)知 $\exists g_1(x), g_2(x) \in S$, 使

$$g_i(x) \overset{F}{\sim} f_i(x), \quad i = 1, 2.$$

于是相伴关系对乘法构成同余关系知

$$f(x) \overset{F}{\sim} g_1(x)g_2(x).$$

因为 $f(x)$ 在 $R[x]$ 中不可约, 所以由定理 3.29(2)有 $f(x) \in S$. 又 $f(x) \overset{F}{\sim} f(x)$, 故再由本定理的结论 (2)知 $f(x) \overset{R}{\sim} g_1(x)g_2(x)$. 这与已知的 $f(x)$ 在 $R[x]$ 中不可约矛盾, 故 $f(x)$ 在 $F[x]$ 中也不可约.

充分性: 若 $f(x)$ 在 $R[x]$ 中可约, 则存在 $f_1(x), f_2(x) \in R[x] \subseteq F[x]$, 使 $f(x) = f_1(x)f_2(x)$. 从而 $f(x)$ 在 $F[x]$ 中也可约, 矛盾!

□

定理 3.31

唯一析因环 R 上的一元多项式环 $R[x]$ 也是唯一析因环.

♡

证明 设 U 为 R^* 中可逆元素的集合,$f(x)\in R[x],f(x)\neq 0$. 于是由定理 3.29(1)知 $\exists d\in R,g(x)\in S$, 使得

$$f(x)=dg(x).$$

因 $d\in R$, 则有 $d=p_1p_2\cdots p_t,p_i(1\leqslant i\leqslant t)$ 为 R 中不可约元素, 在 $R[x]$ 中也不可约. 若 $\deg f(x)=0$, 则 $\deg g(x)=0,g(x)\sim 1$, 故 $g(x)\in U$, 即 $f(x)$ 可分解为有限个不可约元素之积. 再设 $\deg g(x)>0$, 于是 $\deg g(x)=\deg f(x)$. 设 F 为 R 的分式域, 则由定理 3.25(2)知 $F[x]$ 是 Euclid 环, 进而也是唯一析因环. 于是 $g(x)\in F[x]$ 可分解为不可约多项式的积

$$g(x)=g_1(x)g_2(x)\cdots g_r(x).$$

根据定理 3.30(1)有 $p_i(x)\in S$(其中 S 为 $R[x]$ 中本原多项式的集合) 且满足 $p_i(x)\overset{F}{\sim}g_i(x)$, 由命题 3.2知 $p_i(x)$ 是 $F[x]$ 中不可约多项式. 并且由相伴关系对乘法构成同余关系知

$$g(x)\overset{F}{\sim}p_1(x)p_2(x)\cdots p_r(x).$$

由定理 3.29(3)知 $p_1(x)p_2(x)\cdots p_r(x)$ 为本原多项式, 又 $g(x)$ 也是本原多项式, 故由定理 3.30(2)得

$$g(x)\overset{R}{\sim}p_1(x)p_2(x)\cdots p_r(x).$$

因此可不妨设 $g(x)=p_1(x)p_2(x)\cdots p_r(x),p_i(x)$ 是 $F[x]$ 中的不可约多项式, 由定理 3.30(3)知 $p_i(x)$ 在 $R[x]$ 中也不可约, 故 $f(x)$ 可分解为 $R[x]$ 中有限个不可约元素之积

$$f(x)=p_1p_2\cdots p_tp_1(x)p_2(x)\cdots p_r(x).$$

下面证因式分解的唯一性. 设 $f(x)$ 还有分解式

$$f(x)=q_1q_2\cdots q_{t'}q_1(x)q_2(x)\cdots q_s(x),$$

其中,q_i 为 R 中不可约元素,$q_j(x)$ 为 $R[x]$ 中不可约多项式且 $\deg q_j(x)>0$. 由定理 3.29(2)知 $q_j(x)\in S$, 故由定理 3.29(3)知 $q_1(x)q_2(x)\cdots q_s(x)\in S$. 再由定理 3.29(1)知有

$$p_1p_2\cdots p_t\sim q_1q_2\cdots q_{t'},$$

$$p_1(x)p_2(x)\cdots p_r(x)\overset{R}{\sim}q_1(x)q_2(x)\cdots q_s(x).$$

由 R 为唯一析因环知 $t=t'$ 且 $\exists\pi_1\in S_t$, 使得 $p_i\sim q_{\pi_1(i)}$. 又由定理 3.30(3)知 $p_i(x),q_j(x)$ 均为 $F[x]$ 中不可约多项式, 而 $F[x]$ 为 Euclid 环, 由定理 3.23知 $F[x]$ 也是唯一析因环, 故 $r=s$ 且 $\exists\pi_2\in S_r$, 使得 $p_i(x)\overset{F}{\sim}q_{\pi_2(i)}(x)$. 又由定理 3.29(2)知 $p_i(x),q_{\pi_2(i)}(x)$ 都是 $R[x]$ 中的本原多项式且 $p_i(x)\overset{F}{\sim}p_i(x)$, 故再由定理 3.30(1)知 $p_i(x)\overset{R}{\sim}q_{\pi_2(i)}(x)$. 因此, 在 $R[x]$ 中因式分解唯一性定理成立, 即 $R[x]$ 也是唯一析因环.

□

推论 3.17

唯一析因环 R 上的 n 元多项式环 $R[x_1,x_2,\cdots,x_n]$ 也是唯一析因环.

证明 对 n 用数学归纳法, 再根据定理 3.31同理可证.

□

定理 3.32

设 F 是唯一析因环 R 的分式域, 又 $f(x)=\sum_{k=0}^{n}a_kx^k\in R[x],a_n\neq 0(n>1)$. 若有 R 中素元素 p 满足

(1) $p\nmid a_n$;

(2) $p|a_k,0\leqslant k\leqslant n-1$;

(3) $p^2\nmid a_0$,

则 $f(x)$ 是 $F[x]$ 中不可约元素.

证明 由定理 3.30(3), 只需证明 $f(x)$ 在 $R[x]$ 中不能分解为两个次数大于零的多项式的乘积即可. 若不然, 则有

$f(x)=g(x)h(x)$, 其中

$$g(x)=\sum_{k=0}^{r}b_kx^k,\quad b_k\in R,\ b_r\neq 0,\ r\geqslant 1,$$

$$h(x)=\sum_{k=0}^{s}c_kx^k,\quad c_k\in R,\ c_s\neq 0,\ s\geqslant 1$$

且有

$$r+s=n,\quad a_k=\sum_{i+j=k}b_ic_j,\quad p|a_0,\quad p^2\nmid a_0.$$

从而 $p\mid b_0c_0$. 由素元素定义知 $p\mid b_0$ 或 $p\mid c_0$, 不妨设 $p|c_0$,$p\nmid b_0$. 又 $p\nmid a_n$, 故 $p\nmid c_s$,$p\nmid b_r$, 因而存在 $t\in\{1,2,\cdots,s\}$, 使得 $p|c_i(0\leqslant i\leqslant t-1)$,$p\nmid c_t$. 而

$$a_t=\sum_{i+j=t}c_ib_j=\sum_{\substack{i<t,\\ i+j=t}}c_ib_j+c_tb_0.$$

由 p 能整除上式右端第一项, 而 $p\nmid c_tb_0$, 故 $p\nmid a_t$. 这与定理中条件 (2) 矛盾, 故 $f(x)$ 在 $F[x]$ 中不可约.

□

例题 3.17 设 p 为素数,$f(x)=x^{p-1}+x^{p-2}+\cdots+1\in\mathbb{Q}[x]$ 是不可约多项式.

证明 令 $g(x)=f(x+1)$,

$$g(x)=\frac{(x+1)^p-1}{x}=\sum_{k=1}^{p}\mathrm{C}_p^kx^{k-1}.$$

由 $\mathrm{C}_p^p=1$,$p|\mathrm{C}_p^k(1\leqslant k\leqslant p-1)$,$p^2\nmid\mathrm{C}_p^1=p$ 知 $g(x)$ 为 $\mathbb{Q}[x]$ 中不可约多项式, 从而 $f(x)$ 为不可约多项式.

□

例题 3.18 $f(x,y)=x^2y+x^2+y^2+2y+2\in\mathbb{Q}[x,y]$ 是不可约多项式.

证明 由定理 3.7知 $\mathbb{Q}[x,y]=(\mathbb{Q}[x])[y]$, 而 $x^2y+x^2+y^2+2y+2=y^2+y(x^2+2)+(x^2+2)$. 又 x^2+2 是 $\mathbb{Q}[x]$ 中不可约多项式, 由定理 3.29(3)知 x^2+2 也是 $\mathbb{Q}[x]$ 中的素元素, 故由 Eisenstein 判别法知 $f(x,y)$ 为不可约多项式.

□

3.8 素理想与极大理想

定义 3.27 (素理想)

若交换幺环 R 的理想 P 满足

(1) $P\neq R$, 即 P 是 R 的真理想;

(2) 若 $ab\in P$, 则 $a\in P$ 或 $b\in P$,

则称 P 为 R 的**素理想**.

♣

定义 3.28 (极大理想)

设环 R 中的理想 $M\neq R$ 且不存在 R 的理想 A, 使 $M\subset A\subset R$, 则称 M 为 R 的**极大理想**.

♣

注 由定义可知

$$A\text{为环}R\text{的极大理想}\Longleftrightarrow\forall A\subset M\subseteq R,\text{有}M=R\Longleftrightarrow\forall A\subseteq M\subseteq R,\text{有}M=R\text{或}M=A.$$

命题 3.10

(1) 设 p 为素数, 则 $\langle p\rangle=p\mathbb{Z}$ 为 $\mathbb{Z}$ 的素理想, 同时也是 $\mathbb{Z}$ 的极大理想.

(2) $\mathbb{Z}$ 中非平凡理想 $I=m\mathbb{Z}$ 为素理想或极大理想当且仅当 m 为素数 (或负素数).

♠

证明

(1) 设 $ab \in \langle p\rangle = p\mathbb{Z}$, 即 $p \mid ab$. 由 p 为素数知 $p \mid a$ 或 $p \mid b$, 亦即 $a \in p\mathbb{Z} = \langle p\rangle$ 或 $b \in p\mathbb{Z} = \langle p\rangle$, 因而 $\langle p\rangle$ 为素理想.

其次, 设 $\mathbb{Z}$ 的理想 A 满足 $\langle p\rangle \subseteq A \subseteq \mathbb{Z}$. 由命题 3.5知 $\mathbb{Z}$ 为 p.i.d., 故有 $A = \langle n\rangle$. 由 $p \in \langle n\rangle$, 因而 $n \mid p$. 因 p 为素数, 故 $n = \pm 1$ 或 $n = \pm p$. 若 $n = \pm 1$, 则 $A = \mathbb{Z}$; 若 $n = \pm p$, 则 $A = \langle p\rangle$. 由此知 $\langle p\rangle$ 是 $\mathbb{Z}$ 的极大理想.

(2) 若 $m = m_1m_2(m_i \neq \pm 1, i = 1, 2)$, 则 $m_1m_2 = m \in I$. 但 $m_i \notin I(i = 1, 2)$, 故 I 不是素理想. 又 $m\mathbb{Z} \subset m_1\mathbb{Z} \subset \mathbb{Z}$, 故 I 不是极大理想.

□

引理 3.7

设 R 为交换幺环, 则有

(1) $\{0\}$ 是 R 的素理想当且仅当 R 为整环;

(2) $\{0\}$ 是 R 的极大理想当且仅当 R 为域.

♡

证明

(1) 设 R 为整环. 若 $a \neq 0, b \neq 0$, 即 $a \notin \{0\}, b \notin \{0\}$, 则 $ab \neq 0$, 即 $ab \notin \{0\}$, 因而由素理想的逆否定义知 $\{0\}$ 为素理想.

反之, 设 $\{0\}$ 为素理想. 又 $a, b \notin \{0\}$, 故 $ab \notin \{0\}$, 即 $a \neq 0, b \neq 0$ 得出 $ab \neq 0$. 又 R 是交换幺环, 故 R 为整环.

(2) 设 $\{0\}$ 为极大理想.$\forall a \in R$ 且 $a \neq 0$ 有 $\langle a\rangle \supset \{0\}$, 故 $\langle a\rangle = R$. 由 R 含有幺元 1, 故 $1 \in \langle a\rangle = aR$. 因而 $\exists a^{-1} \in R$, 使得 $aa^{-1} = 1$. 再由 R 可交换知 R 是一个域.

反之, 设 R 是一个域,A 为 R 的理想且 $A \neq \{0\}$, 即 $\exists a \in A, a \neq 0$. 又 R 为域, 故 $\exists a^{-1}$, 使 $1 = a^{-1}a$, 再由 A 为 R 的理想知 $= a^{-1}a \in A$. 进而对 $\forall b \in R$ 有 $b = b \cdot 1 \in A$, 因而 $A = R$, 故 $\{0\}$ 为极大理想.

□

定理 3.33

设 R 为交换幺环,P 与 M 为 R 的理想, 则

(1) 当且仅当 R/P 为整环时,P 为素理想;

(2) 当且仅当 R/M 为域时,M 为极大理想.

♡

证明

(1) 设 π 为 R 到 R/P 上的自然同态. 若 P 为素理想, 由 π 为满同态, 故可设 $\pi(a), \pi(b) \in R/P$ 且 $\pi(a) \neq 0, \pi(b) \neq 0$, 亦即 $a, b \notin P$, 则由 P 为素理想知 $ab \notin P$, 即 $\pi(ab) = \pi(a)\pi(b) \neq 0$, 因而 R/P 为整环.

反之, 若 R/P 为整环且 $ab \in P$, 则有 $\pi(ab) = \pi(a)\pi(b) = 0$, 因而 $\pi(a) = 0$ 或 $\pi(b) = 0$, 即 $a \in P$ 或 $b \in P$, 所以 P 是素理想.

(2) 设 R 的理想 A 满足 $M \subseteq A \subseteq R$, 于是由推论 1.5知 A/M 是 R/M 的理想. 当 M 为极大理想时有 $M = A$ 或 $R = A$. 故 R/M 仅有的理想为 $M/M = M = \{0\}$ 与 R/M, 即 $\{0\}$ 为极大理想, 故由引理 3.7知 R/M 为域.

反之, 设 R 的理想 A 满足 $M \subset A \subseteq R$, 由推论 1.5知 A/M 是 R/M 的理想且 $A/M \neq M = \{0\}$. 若 R/M 为域, 则由引理 3.7知 $\{0\}$ 为 R/M 的极大理想, 于是 $A/M = R/M$. 故 $A = R$, 即 M 为极大理想.

□

推论 3.18

交换幺环 R 的极大理想 M 必为素理想.

♡

证明 事实上, 由定理 3.33(2)知 R/M 为域, 由命题 1.10(2)知 R/M 是整环, 所以再由定理 3.33(1)知 M 为素理想.

□

定理 3.34

设 R, R' 都是交换幺环,σ 是 R 到 R' 上的同态,$N = \ker\sigma$.

若 H 是 R 中包含 N 的素理想 (或极大理想), 则 $\sigma(H)$ 是 R' 中的素理想 (或极大理想).

反之, 若 H' 是 R' 的素理想 (或极大理想), 则

$$\sigma^{-1}(H') = \{x \in R | \sigma(x) \in H'\}$$

为 R 中包含 N 的素理想 (或极大理想).

♡

证明 根据定理 1.42(3)有 $R/H \cong R'/\sigma(H)$, 故由定理 3.33知 $H(H \supseteq N)$ 为素理想 (或极大理想) 当且仅当 R/H 为整环 (或域) 当且仅当 $R'/\sigma(H)$ 为整环 (或域), 也当且仅当 $\sigma(H)$ 为素理想 (或极大理想).

□

定理 3.35

若 R 是交换整环,$a \in R^*$, 则由 a 生成的主理想 $\langle a\rangle$ 为素理想的充分必要条件是 a 为素元素.

♡

证明 由定理 1.22(3)知当且仅当 a 为 R 的单位, 即 $a \in U$ 时,$\langle a\rangle = R$, 故可设 $a \in R^* \setminus U$. 由 $bc \in \langle a\rangle = aR \iff a \mid bc$, 故 $\langle a\rangle$ 为素理想当且仅当 $b \in \langle a\rangle$ 或 $c \in \langle a\rangle$ 当且仅当 $a \mid b$ 或 $a \mid c$ 当且仅当 a 为素元素.

□

推论 3.19

设 R 为唯一析因环,$a \in R^*$, 则 $\langle a\rangle$ 为素理想当且仅当 a 为不可约元素.

♡

注 从这里可认为素理想的概念在一定意义下是素元素概念的推广.

证明 由定理 3.35知 $\langle a\rangle$ 为素理想当且仅当 a 为素元素. 又由定理 3.20 的注知 a 为素元素当且仅当 a 不可约, 故结论得证.

□

例题 3.19 设 F 是一个域,$R = F[x_1, x_2, \cdots, x_n]$ 是 F 上 n 元多项式环. 由定理 3.17,定理 3.35及推论 3.19知对 $f \in R$,$\langle f\rangle$ 为素理想当且仅当 f 为不可约多项式. 因 $R/\langle x_1, x_2\rangle \cong F[x_3, \cdots, x_n]$, 故由定理 3.33知由 x_1, x_2 生成的理想 $\langle x_1, x_2\rangle$ 也是素理想, 而 $\langle x_1, x_2\rangle$ 不是主理想. 当 $n > 2$ 时, 看到 $\langle x_1, x_2\rangle$ 也不是极大理想.

定理 3.36

设 R 为主理想整环,$a \in R^*$, 则 $\langle a\rangle$ 为极大理想的充分必要条件是 a 为素元素.

♡

证明 若 $\langle a\rangle$ 为极大理想, 由推论 3.18知 $\langle a\rangle$ 为素理想, 再由定理 3.35知 a 为素元素.

反之, 设 a 为素元素. 若有 R 的理想 A, 使得 $\langle a\rangle \subseteq A \subseteq R$. 由于 R 为 p.i.d., 故有 $n \in R$, 使得 $A = \langle n\rangle$. 于是由 $a \in \langle n\rangle = nR$ 得 $n \mid a$. 因为 a 为素元素, 所以由引理 3.4知 a 也是不可约元素. 从而 $n \sim 1$ 或 $n \sim a$, 于是由定理 3.15(6)有 $A = \langle n\rangle = R$ 或 $A = \langle n\rangle = \langle a\rangle$, 故 $\langle a\rangle$ 为极大理想.

□

定理 3.37

设 F 是一个域,$F[x]$ 是 F 上的一元多项式环,S 为交换整环且 $F \subseteq S$,F, S 有相同的幺元.

(1) 若 $u \in S$ 是 F 上的代数元, 则 $F[u]$ 是一个域且存在唯一的次数大于等于 1 的首一不可约多项式 $p(x) \in F[x]$, 使得

$$\{f(x) \in F[x] | f(u) = 0\} \supset \{0\} = \langle p(x)\rangle,\ F[u] \cong F[x]/\langle p(x)\rangle,\ \langle p(x)\rangle \cap F = \{0\}.$$

反之, 若 $p(x)$ 是不可约多项式, 则 $F[x]/\langle p(x)\rangle$ 是 F 的扩域.

(2) 若 $u \in S$ 是域 F 上的超越元, 则 $F[u]$ 是 F 上的一元多项式环, 且 $F[u] \cong F[x]$.

♡

证明

(1) 由代数元的定义知

$$I = \{f(x) \in F[x] | f(u) = 0\} \supset \{0\}. \tag{3.28}$$

显然 I 是 $F[x]$ 的子环. 由定理 3.25(2)知 $F[x]$ 为 Euclid 环, 再由定理 3.23知 $F[x]$ 为主理想整环, 进而 I 也是主理想整环. 于是存在 $p_1(x) \neq 0$, 使得 $I = \langle p_1(x)\rangle$. 若 $\deg p_1(x) = 0$, 则 $I \subseteq F^* = F \setminus \{0\}$. 从而对 $\forall f(x) \in I$, 都存在 $a \in F^*$, 使得 $a = f(u) = 0$. 故 $I = \{0\}$, 这与(3.28)式矛盾! 因此 $\deg p_1(x) \geqslant 1$. 于是由定理 1.22(3)可得

$$\langle p_1(x)\rangle \cap F = p_1(x)F[x] \cap F = \{0\}.$$

令 g 为 $F[x]$ 到 $F[u]$ 的映射, 满足

$$g|_F = \mathrm{id}_F, \quad g(x) = u.$$

显然 g 为 $F[x]$ 到 $F[u]$ 的同态且

$$g(f(x)) = f(u), \forall f(x) \in F[x].$$

从而 $\ker g = I$. 于是由环的同态基本定理知

$$F[u] \cong F[x]/\langle p_1(x)\rangle.$$

又由 S 为整环知 $F[u]$ 为 S 上添加 u 生成的子环也是整环, 故由定理 3.33知 $\langle p_1(x)\rangle$ 为素理想. 由推论 3.19知 $p_1(x)$ 也是不可约多项式. 不妨设 $p_1(x) = up(x)$, 其中 u 是单位,$p(x)$ 是首一多项式. 又由于 F 是域, 故由定理 3.15(6)知 $p_1(x)$ 与次数大于等于 1 的首一多项式 $p(x)$ 相伴, 从而 $\deg p(x) \geqslant 1$. 再由定理 3.21(2)知 $\langle p(x)\rangle = \langle p_1(x)\rangle$. 又由命题 3.2知 $p(x)$ 也是不可约多项式, 因而 $p(x)$ 为次数大于等于 1 的首一不可约多项式, 且

$$\{f(x) \in F[x] | f(u) = 0\} \supset \{0\} = \langle p_1(x)\rangle = \langle p(x)\rangle,\ F[u] \cong F[x]/\langle p_1(x)\rangle = F[x]/\langle p(x)\rangle,\ \langle p(x)\rangle \cap F = \langle p_1(x)\rangle \cap F = \{0\}.$$

再由定理 3.33知 $p(x)$ 为 $F[x]$ 中的素元素, 再结合定理 3.36知 $\langle p(x)\rangle$ 为极大理想, 由定理 3.33知 $F[u] \cong F[x]/\langle p(x)\rangle$ 为域. 又显然 $F[x]/\langle p(x)\rangle \supseteq F$, 故 $F[x]/\langle p(x)\rangle$ 是 F 的扩域.

最后证明 $p(x)$ 的唯一性. 若还存在次数大于等于 1 的首一不可约多项式 $p'(x) \in F[x]$, 使得

$$F[u] \cong F[x]/\langle p'(x)\rangle, \quad \langle p'(x)\rangle \cap F = \{0\}.$$

则

$$F[x]/\langle p(x)\rangle \cong F[u] \cong F[x]/\langle p'(x)\rangle.$$

从而由命题 1.22(2)(ii)知 $\langle p(x)\rangle = \langle p'(x)\rangle$, 再由定理 3.21(2)知 $p(x) \sim p'(x)$. 而 $p(x), p'(x)$ 都是首一不可约多项式, 故 $p'(x) = p(x)$ 或 1. 若 $p'(x) = 1$, 则与 $\deg p'(x) \geqslant 1$ 矛盾! 因此 $p'(x) = p(x)$.

反之, 若 $p(x)$ 是不可约多项式, 则由推论 3.19知 $\langle p(x)\rangle$ 为素理想, 再由定理 3.35知 $p(x)$ 为 $F[x]$ 中的素元素, 于是由定理 3.36知 $\langle p(x)\rangle$ 为极大理想. 故由定理 3.33知 $F[x]/\langle p(x)\rangle$ 是域, 显然 $F[x]/\langle p(x)\rangle \supseteq F$, 故 $F[x]/\langle p(x)\rangle$ 是 F 的扩域.

(2) 因为 $u \in S$ 是域 F 上的超越元, 所以 $F[u]$ 是 F 上的一元多项式环. 从推论 3.3知 u 是超越元时上述结论成立.

□

第 4 章 域

4.1 域的单扩张

定义 4.1 (环的特征)

设 R 为环. 如果存在最小的正整数 n, 使得对所有的 $a \in R$, 有 $na = 0$, 则称 n 为环 R 的**特征**. 如果这样的正整数不存在, 则称环 R 的**特征**为 0. 环 R 的特征记作 $\operatorname{Char} R$ 或 $\operatorname{ch} R$.

例题 4.1 $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ 的特征都等于 0.

命题 4.1

设 $\mathbb{Z}_m$ 是模 m 剩余类环, 则 $\operatorname{Char}\mathbb{Z}_m = m$,$\operatorname{Char}\mathbb{Z}_m[x] = m$.

证明 对每个 $\overline{n} \in \mathbb{Z}_m$, 有

$$m\overline{n} = \overline{mn} = \overline{0}.$$

而对于任何正整数 $k < m$, 有

$$k\overline{1} = \overline{k} \neq \overline{0},$$

所以 $\operatorname{Char}\mathbb{Z}_m = m$. 类似地可以证明, 对于 $\mathbb{Z}_m$ 上的一元多项式环 $\mathbb{Z}_m[x]$, 也有 $\operatorname{Char}\mathbb{Z}_m[x] = m$.

□

定理 4.1

设 R 是有单位元 e 的环. 如果 e 关于加法的阶为无穷大, 那么 R 的特征等于 0. 如果 e 关于加法的阶等于 n, 那么 $\operatorname{Char} R = n$.

证明 如果 e 关于加法的阶为无穷大, 那么不存在正整数 n, 使得 $ne = 0$. 所以由特征的定义知, R 的特征等于 0.

如果 e 关于加法的阶等于正整数 n, 则 $ne = 0$. 而且 n 是满足这一性质的最小正整数. 因此, 对于任意的 $a \in R$, 有

$$na = n(e \cdot a) = (ne) \cdot a = 0 \cdot a = 0.$$

于是 R 的特征等于 n.

□

定理 4.2

整环的特征是 0 或者是一个素数.

证明 由定理 4.1, 只要证明, 如果整环 R 的单位元 e 关于加法的阶有限, 则它必为素数.

设 e 关于加法的阶为 n. 显然 $n > 1$. 假设 $n = p_1 p_2 \cdots p_s$, $1 \leqslant p_i \leqslant n$ 且 p_i 都是素数. 则

$$0 = ne = (p_1 p_2 \cdots p_s)e = (p_1 e) \cdot (p_2 e) \cdots (p_s e).$$

由 R 是整环和命题 1.11(2)可知存在 $i_0 \in [1, s] \cap \mathbb{N}$, 使 $p_{i_0} e = 0$. 因为 n 是使得 $ne = 0$ 成立的最小正整数, 所以 $p_{i_0} = n$. 因此 n 是素数.

□

定义 4.2 (素域/素体)

不包含任何平凡子体的体称为**素体**或**素域**, 即子体只有自身的体.

定理 4.3

设 K 是一个体, 则 K 的所有子体之交就是 K 包含的唯一素域 (素体), 也是 K 的子体.

♡

注 这个定理表明: 每个体可以看成是某个素域 (素体) 的扩张.

证明 记 K 的所有子体之交为 R, 则由命题 1.10(4)知 R 仍为 K 的子体. 设 R_1 是 R 的子体且 $R_1 \subseteq R$, 则 R_1 也是 K 的子体, 从而由 R 的定义知 $R \subseteq R_1$, 故 $R_1 = R$. 故 R 是 K 的素域.

若 K 还包含一个素域 R', 则 R' 也是 K 的子体, 从而 $R' \supseteq R$. 又因为 R' 是素域, 所以 $R' = R$. 故唯一性得证.

□

定理 4.4

(1) $\mathbb{Z}_p, \mathbb{Q}$ 都是素域 (素体).

(2) 设 Π 是一个素域 (素体), 则 $\Pi \cong \mathbb{Z}_p (p$ 为素数) 或 $\Pi \cong \mathbb{Q}$.

进而素域 (素体) 一定是域.

♡

证明

(1) $\mathbb{Z}_p$ 对于加法是素数阶群. 由Lagrange 定理知 $\mathbb{Z}_p$ 无非平凡子群, 故 $\mathbb{Z}_p$ 无非平凡子体, 因而 $\mathbb{Z}_p$ 是素域 (素体).

若 F 为域 $\mathbb{Q}$ 的子体, 于是 $1 \in F$, 从而 $\mathbb{Z} \subset F$, 由命题 3.1知 $\mathbb{Z}$ 的分式域是 $\mathbb{Q}$. 因而由定理 3.2知 $\mathbb{Q} \subseteq F$, 故 $F = \mathbb{Q}$, 所以 $\mathbb{Q}$ 为素域 (素体).

(2) 设 e 为 Π 的幺元, 于是易知 $\mathbb{Z}e = \{ne | n \in \mathbb{Z}\}$ 为 Π 的可交换子环且有 $\mathbb{Z}$ 到 $\mathbb{Z}e$ 的同态 $\pi : \pi(n) = ne (n \in \mathbb{Z})$. 于是由环的同态基本定理知

$$\mathbb{Z}e \cong \mathbb{Z}/\ker\pi.$$

由于 $\mathbb{Z}$ 为 Euclid 环, 进而也是主理想整环, 故有 $p \in \mathbb{Z}$, 使得 $\ker\pi = \langle p \rangle$. 因为 Π 为体, 故由命题 1.10(2)知 $\mathbb{Z}e$ 为交换整环, 即 $\mathbb{Z}/\ker\pi = \mathbb{Z}/\langle p \rangle$ 也是交换整环. 因此由定理 3.33(1)知 $\langle p \rangle$ 为素理想, 再由定理 3.35知 p 为 $\mathbb{Z}$ 中的素元素, 进而 p 只能为素数或零.

当 p 为素数时, 由命题 1.12知 $\mathbb{Z}e \cong \mathbb{Z}/\langle p \rangle = \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$ 为域, 从而 $\mathbb{Z}e$ 是 Π 的子体. 又 Π 无非平凡子体, 故 $\Pi = \mathbb{Z}e \cong \mathbb{Z}_p$.

当 $p = 0$ 时, 有 $\mathbb{Z}e \cong \mathbb{Z}/\langle 0 \rangle = \mathbb{Z}$. 由命题 3.1知 $\mathbb{Z}$ 的分式域是 $\mathbb{Q}$. 记 $\mathbb{Z}e$ 的分式域为 F, 则由推论 3.1知 $F \cong \mathbb{Q}$. 又 $\mathbb{Z}e \subset \Pi$, 故由定理 3.2知 $F \subseteq \Pi$. 再由 Π 是素域知 $\Pi = F \cong \mathbb{Q}$.

由命题 1.12知 $\mathbb{Z}_p$ 和 $\mathbb{Q}$ 都是域, 而由定理 4.4(2)知任意素域都同构于这个两个域, 因此素域 (素体) 一定是域.

□

定理 4.5

设 K 是一个体,p 为素数, 则

(1) K中的素域都与$\mathbb{Z}_p$同构 $\Longleftrightarrow \operatorname{ch} K = p$.

(2) K中的素域都与$\mathbb{Q}$同构 $\Longleftrightarrow \operatorname{ch} K = 0$.

进而 $\operatorname{ch} K$ 只能是 0 或素数.

♡

证明 记 K 的幺元为 e. 由定理 4.3知 K 只包含唯一的素域, 记为 Π. 显然 $\mathbb{Z}e = \{ne | n \in \mathbb{Z}\}$ 为 Π 的可交换子环且有 $\mathbb{Z}$ 到 $\mathbb{Z}e$ 的同态 $\pi : \pi(n) = ne (n \in \mathbb{Z})$. 于是由环的同态基本定理知

$$\mathbb{Z}e \cong \mathbb{Z}/\ker\pi. \tag{4.1}$$

由于 $\mathbb{Z}$ 为 Euclid 环, 进而也是主理想整环, 故有 $p' \in \mathbb{Z}$, 使得 $\ker\pi = \langle p' \rangle$. 因为 Π 为体, 故由命题 1.10(2)知 $\mathbb{Z}e$ 为交换整环, 即 $\mathbb{Z}/\ker\pi = \mathbb{Z}/\langle p' \rangle$ 也是交换整环. 因此由定理 3.33(1)知 $\langle p' \rangle$ 为素理想, 再由定理 3.35知 p' 为 $\mathbb{Z}$ 中的素元素, 进而 p' 只能为素数或零.

(1) 若 $\Pi \cong \mathbb{Z}_p$, 因为在 $\mathbb{Z}_p$ 中有 $p \cdot 1 = 0$, 所以在 Π 中有 $pe = 0$, 因而 $pa = pe \cdot a = 0, \forall a \in K$. 又对 $\forall k \in \mathbb{N} \cap (0, p)$, 在 $\mathbb{Z}_p$ 中有 $k \cdot 1 \neq 0$, 故在 Π 中有 $ke \neq 0$. 因此 $\operatorname{ch} K = p$.

反之, 若 $\operatorname{ch} K = p$, 则 $pa = 0, \forall a \in K$, 则 $pe = 0$. 从而对 $\forall z \in \mathbb{Z}$, 有 $\pi(pz) = pze = z \cdot pe = 0$. 故 $\langle p \rangle = p\mathbb{Z} \subseteq \ker \pi$. 若 $p' \neq p$, 则 $\langle p \rangle \nsubseteq \langle p' \rangle = \ker \pi$ 矛盾! 因此 $p = p'$, 即

$$\ker \pi = \langle p \rangle.$$

又因为 p 为素数, 所以由(4.1)式及命题 1.12知 $\mathbb{Z}e \cong \mathbb{Z}/\langle p \rangle = \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$ 为域, 从而 $\mathbb{Z}e$ 是 Π 的子域, 也是子体. 又 Π 无非平凡子体, 故 $\Pi = \mathbb{Z}e \cong \mathbb{Z}_p$.

(2) 若 $\Pi \cong \mathbb{Q}$. 记 $\mathbb{Z}e$ 的分式域为 F, 又 $\mathbb{Z}e \subset \Pi$, 故由定理 3.2知 $F \subseteq \Pi$. 再由 Π 是素域知 $\Pi = F \cong \mathbb{Q}$. 于是由推论 3.1知 $\mathbb{Z} \cong \mathbb{Z}e$. 因此由 $n \cdot 1 \neq 0, \forall n \in \mathbb{N}$ 知 $ne \neq 0, \forall n \in \mathbb{N}$. 又由命题 1.10(2)知 K 是整环, 故 $\forall a \in K^*, na = ne \cdot a \neq 0$. 因此 $\operatorname{ch} K = 0$.

反之, 若 $\operatorname{ch} K = 0$, 则 $\forall n \in \mathbb{N}, a \in K^*$ 有 $na \neq 0$. 特别地, $\pi(n) = ne \neq 0, \pi(-n) = -ne \neq 0$. 于是 $\ker \pi = \{0\} = \langle 0 \rangle$. 故由(4.1)式知 $\mathbb{Z}e \cong \mathbb{Z}/\langle 0 \rangle = \mathbb{Z}$.

由定理 4.4知 K 的素域 Π 只可能同构于 $\mathbb{Q}$ 或 $\mathbb{Z}_p$(p 为素数), 因此 $\operatorname{ch} K$ 只能是 0 或素数.

□

推论 4.1

数域的特征都是零.

♡

证明

□

定义 4.3

设 K 为域 F 的扩域, S 为 K 的子集. K 中所有包含 $F \cup S$ 的子域之交, 称为**由 F 与 S 生成的子域**, 也称为 F **上添加 S 所得的域**, 亦称为 S **在 F 上生成的域**, 记为 $F(S)$.

♣

注 显然有 $K = F(K)$.

定理 4.6

设 K 为域 F 的扩域, $S \subseteq K$. 定义 $F[S]$ 为

$$F[S] \triangleq \left\{ \sum_{i_1, i_2, \cdots, i_n \geqslant 0} \alpha_{i_1 i_2 \cdots i_n} a_1^{i_1} a_2^{i_2} \cdots a_n^{i_n} \mid a_j \in S,\ j = 1, 2, \cdots, n,\ n \in \mathbb{N},\ \alpha_{i_1 i_2 \cdots i_n} \in F \right\}.$$

则 $F[S]$ 是 K 的子环, $F[S]$ 的分式域恰为 $F(S)$.

特别当 $S = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ 为有限集时, 分别记

$$F[S] = F[\alpha_1, \alpha_2, \cdots, \alpha_n], \quad F(S) = F(\alpha_1, \alpha_2, \cdots, \alpha_n).$$

♡

证明

□

定理 4.7

设 K 为域 F 的扩域, $S \subseteq K$, 则

(1) $F(S) = \bigcup_{S' \subseteq S} F(S')$, 此处 S' 取遍 S 的所有有限子集.

(2) 若 $S = S_1 \cup S_2$, 则 $F(S) = F(S_1)(S_2)$. 特别地, 若 $a\alpha_1, \alpha_2, \cdots, \alpha_n \in K$, 则 $F(\alpha_1, \alpha_2, \cdots, \alpha_n) = F(\alpha_1)(\alpha_2) \cdots (\alpha_n)$.

♡

证明

(1) 显然对 $\forall S' \subseteq S$, 有 $F(S') \subseteq F(S)$, 因而

$$\bigcup_{S' \subseteq S} F(S') \subseteq F(S).$$

反之, 对 $\forall a \in F(S)$, 由定理 4.6有 $a = \dfrac{f}{g}, f, g \in F[S]$, 由于 f, g 的表达式均为有限和的形式, 因而存在 S 的有限子集 S_0', 使 $f, g \in F[S_0']$. 于是 $a = \dfrac{f}{g} \in F(S_0') \subseteq \bigcup\limits_{S' \subseteq S} F(S')$, 故结论成立.

(2) 由于 $F(S_1 \cup S_2)$ 是 K 中包含 $F, S_1 \cup S_2$ 的最小子域, 而 $F, S_1, S_2 \subseteq F(S_1)(S_2)$, 故有

$$F(S_1 \cup S_2) \subseteq F(S_1)(S_2).$$

反之,$F(S_1)(S_2)$ 是包含 $F(S_1), S_2$ 的最小子域, 而

$$F(S_1) \subseteq F(S_1 \cup S_2), \quad S_2 \subseteq F(S_1 \cup S_2),$$

故 $F(S_1)(S_2) \subseteq F(S_1 \cup S_2)$, 因而结论成立.

□

定义 4.4

设 K 是 F 的扩域. 若 $\exists \alpha \in K$, 使得

$$K = F(\alpha),$$

称 K 是 F 的**单扩域**.

若 α 是 F 上的代数元, 称 $K = F(\alpha)$ 为 F 的**单代数扩域**或**单代数扩张**.

若 α 是 F 上的超越元, 称 $K = F(\alpha)$ 为 F 的**单超越扩域**或**单超越扩张**.

♣

定理 4.8

(1) 设 F 是一个域,α 是 F 上的超越元, 则

(i) F 的单超越扩域 $F(\alpha)$ 就是域 F 上的一元多项式环 $F[\alpha]$ 的分式域, 并且在同构意义下唯一.

(ii) 若 $F[x]$ 是域 F 上的一元多项式环, 则 $F(\alpha)$ 与 $F[x]$ 的分式域同构.

(2) 设 F 是一个域,α 是 F 上的代数元,$F[x]$ 是域 F 上的一元多项式环, 则存在唯一的次数大于等于 1 的首一不可约多项式 $p(x) \in F[x]$ 使得 $p(\alpha) = 0$ 且

$$F(\alpha) \cong F[x]/\langle p(x) \rangle.$$

此时环 $F[\alpha]$ 是一个域, 并且 $F[\alpha] = F(\alpha)$.

♡

证明

(1) (i) 当 α 是 F 上的超越元时, 由定理 4.6知,F 上的一元多项式环 $F[\alpha]$ 的分式域就是 $F(\alpha)$. 若 $F(y)$ 也是 F 的单超越扩域, 则由定理 4.6知,$F[y]$ 的分式域就是 $F(y)$. 由定理 3.37(2)可知 $F[\alpha] \cong F[y]$, 进而由推论 3.1知它们的分式域也同构, 即 $F(\alpha) \cong F(y)$.

(ii) 此时 x 也是 F 的上的超越元, 记 $F(x)$ 也是 F 的单超越扩域, 则定理 4.6知,$F(x)$ 也是 F 上的一元多项式环 $F[x]$ 的分式域. 由定理 3.37(2)可知 $F[\alpha] \cong F[x]$, 进而由推论 3.1知它们的分式域也同构, 即 $F(\alpha) \cong F(x)$.

(2) 从定理 3.37(1)可知当 α 为代数元时, 存在唯一的首一不可约多项式 $p(x) \in F[x]$ 使得 $p(\alpha) = 0$ 且

$$F[\alpha] \cong F[x]/\langle p(x) \rangle.$$

此时环 $F[\alpha]$ 是一个域. 再由定理 3.2知 $F[\alpha]$ 的分式域就是其本身, 故 $F[\alpha] = F(\alpha)$. 因此

$$F(\alpha) \cong F[x]/\langle p(x) \rangle.$$

□

定义 4.5

设 K 是 F 的扩域,$\alpha \in K$,α 是 F 上的代数元.$F[x]$ 中以 α 为根的首一不可约多项式称为 α **在 F 上的不可约多项式**, 记为 $\mathrm{Irr}(\alpha, F)$. 它的次数称为 α **在 F 上的次数**, 记为 $\deg(\alpha, F)$, 即 $\deg(\alpha, F) = \deg(\mathrm{Irr}(\alpha, F))$.

♣

注 由定理 3.37(1)和定理 1.22(3)知若 α 是 F 上的代数元, 则

$$\langle \mathrm{Irr}(\alpha,F)\rangle = \{f(x)\in F[x]|f(\alpha)=0\} = \mathrm{Irr}(\alpha,F)F[x] = \{f(x)\in F[x]|\mathrm{Irr}(\alpha,F)|f(x)\}.$$

定理 4.9

设 $F(\alpha)$ 是 F 的单代数扩张, 又 $\deg(\alpha,F)=n$, 则 $F(\alpha)$ 是 F 上的 n 维线性空间且 $1,\alpha,\alpha^2,\cdots,\alpha^{n-1}$ 是一组基.

♡

证明 根据定理 1.24中域 F 上的线性空间的定义, 可直接验证 $F(\alpha)$ 是 F 上的线性空间. 由定理 4.8(2)知 $F[\alpha]=F(\alpha)$. 设 $F[x]$ 是 F 上的一元多项式环, 则由推论 3.3(2)知 $F[x]$ 与 $F[\alpha]=F(\alpha)$ 之间有满同态 η 满足

$$\eta(f(x)) = f(\alpha),\quad \forall f(x)\in F[x],$$

而

$$\ker\eta = \langle \mathrm{Irr}(\alpha,F)\rangle.$$

对 $\forall f(\alpha)\in R[\alpha]$, 都存在 $f(x)\in R[x]$, 使得 $\eta(f(x))=f(\alpha)$. 又由 $\deg(\alpha,F)=n$, 故 $\exists q(x),r(x)\in F[x]$, 使得

$$f(x) = q(x)\mathrm{Irr}(\alpha,F)+r(x),\quad \deg r(x) < \deg(\alpha,F)=n.$$

(注意 $\deg 0=-\infty$) 因而对上式两边同时作用 η 得 $f(\alpha)=r(\alpha)\in L(1,\alpha,\cdots,\alpha^{n-1})$. 于是 $1,\alpha,\alpha^2,\cdots,\alpha^{n-1}$ 生成 $F(\alpha)$. 又若 $\deg s(x)<\deg(\alpha,F)$, 而 $s(\alpha)=0$, 则 $\eta(s(x))=0$. 故 $\mathrm{Irr}(\alpha,F)|s(x)$, 因而 $s(x)=0$, 即 $1,\alpha,\alpha^2,\cdots,\alpha^{n-1}$ 线性无关, 故 $1,\alpha,\alpha^2,\cdots,\alpha^{n-1}$ 是 $F(\alpha)$ 的一组基, 故 $F(\alpha)$ 的维数为 n.

□

定义 4.6

设 K_1,K_2 都是域 F 的扩域. 若有 K_1 到 K_2 上的同构 η, 使 $\eta|_F=\mathrm{id}_F$, 则称 K_1 与 K_2 是 F 的**等价扩张**,η 称为 F **同构**. 特别地, 若 $K_1=K_2$, 则称 η 为 F **自同构**.

♣

命题 4.2

(1) 若 $F(\alpha),F(\beta)$ 都是 F 的单超越扩张, 则 $F(\alpha)$ 与 $F(\beta)$ 是 F 的等价扩张. 这时它们与一元多项式环 $F[x]$ 的分式域都是 F 的等价扩张.

(2) 若 $F(\alpha),F(\beta)$ 都是 F 的单代数扩张且 $\mathrm{Irr}(\alpha,F)=\mathrm{Irr}(\beta,F)$, 则 $F(\alpha)$ 与 $F(\beta)$ 是 F 的等价扩张. 此即, 对 $F[x]$ 中的任一不可约多项式 $p(x)$ 在等价定义下存在唯一单代数扩张. 事实上,$F[x]/\langle p(x)\rangle = F(x+\langle p(x)\rangle)$. 令 $\alpha=x+\langle p(x)\rangle$, 则 $\mathrm{Irr}(\alpha,F)$ 与 $p(x)$ 相伴.

♠

注 注意对 F 的两个等价的单代数扩张 $F(\alpha),F(\beta)$, 不一定有 $\mathrm{Irr}(\alpha,F)=\mathrm{Irr}(\beta,F)$.

证明

(1)

(2) 事实上, 记 $p(x)=\mathrm{Irr}(\alpha,F)=\mathrm{Irr}(\beta,F)$, 则 $F(\alpha),F(\beta)$ 与 $F[x]/\langle p(x)\rangle$ 都是 F 的等价扩张, 故 $F(\alpha)$ 与 $F(\beta)$ 是 F 的等价扩张.

□

例题 4.2 设 $F=\mathbb{R},\alpha=\sqrt{-1},\beta=1+\sqrt{-1}$. 显然 $F(\alpha)=\mathbb{C},F(\beta)=\mathbb{C}$, 故 $F(\alpha)$ 与 $F(\beta)$ 是 F 的等价扩张, 但 $\mathrm{Irr}(\alpha,F)=x^2+1,\mathrm{Irr}(\beta,F)=x^2-2x+2$, 故 $\mathrm{Irr}(\alpha,F)\neq\mathrm{Irr}(\beta,F)$.

证明

□

例题 4.3 定义 $\mathbb{C}$ 到 $\mathbb{C}$ 的映射 τ:

$$\tau(a+b\sqrt{-1}) = a-b\sqrt{-1},\quad \forall a,b\in\mathbb{R},$$

则容易验证 τ 是 $\mathbb{C}$ 的 $\mathbb{R}$ 自同构.

证明

□

定义 4.7

设 K, K_1, K_2 都是域 F 的扩域且

$$K \supseteq K_i \supseteq F, \quad i = 1, 2.$$

若 K_1 与 K_2 是 F 等价扩张, 则称 K_1, K_2 是 K(对 F) **共轭的子域**.

又若 $\alpha, \beta \in K$ 且 $\mathrm{Irr}(\alpha, F) = \mathrm{Irr}(\beta, F)$, 则称 α 与 β 是 (对 F) 的**共轭元素**.

♣

命题 4.3

设 $F(\alpha), F(\beta)$ 都是 F 的单代数扩张, 若 α, β 是共轭元素, 则 $F(\alpha)$ 与 $F(\beta)$ 共轭.

♠

注 从例题 4.2知这个结论反之不成立.

证明 从命题 4.2(2)知 α, β 是共轭元素, 则 $F(\alpha)$ 与 $F(\beta)$ 共轭.

□

参考文献

[1] 孟道骥, 陈良云, 史毅茜, 白瑞蒲. 抽象代数 I——代数学基础[M]. 北京: 科学出版社, 2010.