高等线性代数

Advanced Linear Algebra
PHYS6653P
2021 学年第一学期

笔记

陈稼霖
github.com/Chen-Jialin
2021 年 9 月 –

目录

Chapter 0

代数学基础

0.1 常用符号

- $\forall$: 对所有 (for all).
- $\exists$: 存在 (there exists).
- $\exists!$: 存在且唯一 (there exists exactly one).
- s.t.: 使得 (such that).
- $\mathbb{N}$: 自然数.
- $\mathbb{Z}$: 整数.
- $\mathbb{Q}$: 有理数.
- $\mathbb{R}$: 实数.
- $\mathbb{C}$: 复数.

0.2 集合

定义 0.1 集合(Set): 略.

元素与集合之间的关系: 对元素 a 和集合 S,

- $a \in S$ 或
- $a \notin S$.

集合中元素之间的关系: $\forall a, b \in S$,

- $a = b$ 或
- $a \neq b$.

集合与集合之间的关系: 对集合 A, B 和全集 I,

(1) **交集**: $A \cap B = \{a \mid a \in A \text{ 且 } a \in B\}$.

(2) **并集**: $A \cup B = \{a \mid a \in A \text{ 或 } a \in B\}$.

(3) **差**: $B - A = \{a \mid a \in B \text{ 且 } a \notin A\}$.

(4) **补集**: $A' = I - A = \{a \mid a \in I \text{ 且 } a \notin A\}$.

(5) **包含**: $A \subseteq B$, 称 A 包含于 B, 或称 B 包含 A, 或称 B 是 A 的子集
$\iff A \cup B = A \iff A \cup B = B$.

证: $\underline{A \subseteq B \implies A \cap B = A}$: $\because A \subseteq B, \therefore \forall a \in A, a \in B \implies A \subseteq A \cap B$.
$\forall a \in A \cup B$, 由交集定义, $a \in A \implies A \cap B \subseteq A$.
故 $A \cap B = A$.

$\underline{A \subseteq B \impliedby A \cap B = A}$: $\because A \cap B = A, \therefore \forall a \in A, a \in B \implies A \subseteq B$.

$\underline{A \subseteq B \implies A \cup B = B}$: $\because A \subseteq B, \forall a \in A, a \in B, \therefore \forall a \in A \cup B, a \in B \implies A \cup B \subseteq B$.
$\because A \subseteq B, \forall a \in A$, 由并集定义, $a \in A \cup B \implies B \subseteq A \cup B$.
故 $A \cup B = B$.

$\underline{A \subseteq B \impliedby A \cup B = B}$: $\forall a \in A$, 由并集定义, $a \in A \cup B$, 又 $\because A \cup B = B, \therefore a \in B \implies A \subseteq B$.

综上, 得证. □

常用公式:

(1) $A \cap (\cup_i B_i) = \cup_i (A \cap B_i)$.

证: $\forall a \in A(\cup_i B_i) \iff a \in A \text{ 且 } a \in \cup_i B_i$
$\iff a \in A \text{ 且 } \exists k, \text{s.t. } a \in B_k$
$\iff \exists k, \text{s.t. } a \in A \cap B_k \subseteq \cup_i (A \cap B_i)$
$\iff a \in \cup_i (A \cap B_i)$, 故 $A \cap (\cup_i B_i) \subseteq \cup_i (A \cap B_i)$.

$\forall a \in \cup_i (A \cap B_i) \iff \exists k, \text{s.t. } a \in A \cap B_k$
$\iff \exists k, \text{s.t. } a \in A \text{ 且 } a \in B_k$
$\iff a \in A \text{ 且 } \exists k, \text{s.t. } a \in B_k$
$\iff a \in A \text{ 且 } a \in \cup_i B_i$
$\iff a \in A \cap (\cup_i B_i)$, 故 $\cup_i (A \cap B_i) \subseteq A \cap (\cup_i B_i)$.

综上, 得证. □

(2) $A \cup (\cap_i B_i) = \cap_i (A \cup B_i)$.

证: $\forall a \in A \cup (\cap_i B_i) \iff a \in A \text{ 或 } a \in \cap_i B_i$
$\iff a \in A \text{ 或 } \forall i, \text{s.t. } a \in B_i$
$\iff \forall i, a \in A \text{ 或 } a \in B_k$
$\iff \forall i, a \in A \cup B_k$
$\iff \cap_i (A \cup B_i)$, 故 $A \cup (\cap_i B_i) \subseteq \cap_i (A \cup B_i)$.

$\forall a \in \cap_i (A \cup B_i) \iff \forall i, a \in A \cup B_i$
$\iff \forall i, a \in A \text{ 或 } a \in B_i$
$\iff a \in A \text{ 或 } \forall i, a \in B_i$

$\Longleftrightarrow a \in A$ 或 $a \in \cup_i B_i$

$\Longleftrightarrow a \in A \cap (\cup_i B_i)$, 故 $\cap_i (A \cup B_i) \subseteq A \cap (\cup_i B_i)$.

综上, 得证. □

(3) $(\cup_i A_i)' = \cap_i A_i'$.

证: $\forall a \in (\cup_i A_i)' \Longleftrightarrow a \in I$ 且 $a \notin \cup_i A_i$

$\Longleftrightarrow a \in I$ 且 $\forall i, a \notin A_i$

$\Longleftrightarrow \forall i, a \in I$ 且 $a \notin A_i$

$\Longleftrightarrow \forall i, a \in A_i'$

$\Longleftrightarrow a \in \cap_i A_i'$, 故 $(\cup_i A_i)' \subseteq \cap_i A_i'$.

$\forall a \in \cap_i A_i' \Longleftrightarrow \forall i, a \in I$ 且 $a \notin A_i$

$\Longleftrightarrow a \in I$ 且 $\forall i, a \notin A_i$

$\Longleftrightarrow a \in I$ 且 $a \notin \cup_i A_i'$

$\Longleftrightarrow a \in (\cup_i A_i)'$, 故 $\cap_i A_i' \in (\cup_i A_i)'$.

综上, 得证. □

(4) $(\cap_i A_i)' = \cup_i A_i'$.

证: $\forall a \in (\cap_i A_i)' \Longleftrightarrow a \in I$ 且 $a \notin \cap_i A_i$

$\Longleftrightarrow a \in I$ 且 $\exists k$, s.t. $a \notin A_k$

$\Longleftrightarrow \exists k$, s.t. $a \in I$ 且 $a \notin A_k$

$\Longleftrightarrow \exists k$, s.t. $a \in A_k'$

$\Longleftrightarrow a \in \cup_i A_i'$, 故 $(\cap_i A_i)' \subseteq \cup_i A_i'$.

$\forall a \in \cup_i A_i' \Longleftrightarrow \exists k$, s.t. $a \in A_k'$

$\Longleftrightarrow \exists k$, s.t. $a \in I$ 且 $a \notin A_k$

$\Longleftrightarrow a \in I$ 且 $\exists k$, s.t. $a \notin A_k$

$\Longleftrightarrow a \in I$ 且 $a \notin \cap_i A_i$

$\Longleftrightarrow a \in (\cap_i A_i)'$, 故 $\cup_i A_i' \subseteq (\cap_i A_i)'$.

综上, 得证. □

0.3 映射

定义 0.2 **映射:** $\forall a \in S_1, \exists! b \in S_2$, s.t. $b = f(a)$, 记作 $f : S_1 \to S_2, a \mapsto b$, 其中称 S_1 为**定义域**, S_2 为**值域**, b 为 a 的**像**, a 为 b 的**原像**.

例 0.1 **恒等映射:** $1_S : S \to S, a \mapsto 1_S(a) = a$. □

定义 0.3 **映射相等:** 映射 $f : S_1 \to S_2, g : S_1 \to S_3, \forall a \in S_1, f(a) = g(a)$, 则称 f 与 g **相等**, 记作 $f = g$.

$\forall a \in S_1, \{f(a)\} \subseteq S_2$ 且 $|\{f(a)\}| = 1$.

定义 0.4 原像集: $f^{-1}(b) \equiv \{a \in S_1 \mid f(a) = b\}$.

$f^{-1}(b) \subseteq S_1$, $f^{-1}(b)$ 可能 $= \emptyset$.

定义 0.5 像集: $\operatorname{Im} f = f(S_1) \equiv \{b \in S_2 \mid b = f(a) \forall a \in S_1\}$.

$\operatorname{Im} f \subseteq S_2$.

基本性质:

(1) $A \subseteq S_1 \Longrightarrow A \subseteq f^{-1}(f(A))$.

证: $\forall a \in A, \because A \subseteq S_1, \therefore a \in S_1$.
又 $\because f(a) \in f(A), \therefore a \in f^{-1}(f(A))$, 故 $A \subseteq f^{-1}(f(A))$. □

若 $\exists a \in S_1 - A$, s.t. $f(a) \in f(A)$, 则 $A \subsetneq f^{-1}(f(A))$.

(2) $B \subseteq S_2 \Longrightarrow B \supseteq f(f^{-1}(B))$.

证: $\because f^{-1}(B) = \{a \in S_1 \mid f(a) \in B\}, \therefore \forall a \in f^{-1}(B), f(a) \in B \Longrightarrow f(f^{-1}(B)) \subseteq B$. □

若 $\exists b \in B$, s.t. $\forall a \in S_1$, $f(a) \neq b$ (即 B 中有元素在 S_1 中无原像), 则 $B \supsetneq f(f^{-1}(B))$.

若 $\forall b \in B, \exists a \in A$, s.t. $f(a) = b$, 则 $B = f(f^{-1}(B))$.

(3) $f^{-1}(\cup_i B_i) = \cup_i f^{-1}(B_i)$.

证: $\forall a \in f^{-1}(\cup_i B_i), \exists k$, s.t. $f(a) \in B_k$
$\Longleftrightarrow \exists k$, s.t. $a \in f^{-1}(B_k)$
$\Longleftrightarrow a \in \cup_i f^{-1}(B_i)$, 故 $f^{-1}(\cup_i B_i) \subseteq \cup_i f^{-1}(B_i)$.

$\forall a \in \cup_i f^{-1}(B_i), \exists k$, s.t. $a \in f^{-1}(B_k)$
$\Longleftrightarrow \exists k$, s.t. $f(a) \in B_k$
$\Longleftrightarrow f(a) \in \cup_i B_i$
$\Longleftrightarrow a \in f^{-1}(\cup_i B_i)$, 故 $\cup_i f^{-1}(B_i) \subseteq f^{-1}(\cup_i B_i)$.

综上, 得证. □

(4) $f^{-1}(\cap_i B_i) = \cap_i f^{-1}(B_i)$.

证: $\forall a \in f^{-1}(\cap_i B_i), \exists k$, s.t. $f(a) \in B_k$
$\Longleftrightarrow \exists k$, s.t. $a \in f^{-1}(B_k)$
$\Longleftrightarrow a \in \cup_i f^{-1}(B_k)$, 故 $f^{-1}(\cap_i B_i) \subseteq \cap_i f^{-1}(B_i)$.

$\forall a \in \cap_i f^{-1}(B_i), \forall i$, s.t. $a \in f^{-1}(B_i)$
$\Longleftrightarrow \forall i$, s.t. $f(a) \in B_i$
$\Longleftrightarrow f(a) \in \cap_i B_i$
$\Longleftrightarrow a \in f^{-1}(\cap_i B_i)$, 故 $\cap_i f^{-1}(B_i) \subseteq f^{-1}(\cap_i B_i)$.

综上, 得证. □

定义 0.6 <u>映射的复合</u>: 映射 $f: S_1 \to S_2$, $g: S_2 \to S_3$, 则称映射 $g \circ f: S_1 \to S_2$, $a \mapsto g \circ f(a) \equiv g(f(a))$ 为 f 和 g 的**复合**.

定理 0.1 <u>映射复合的结合律</u>: $h \circ (g \circ f) = (h \circ g) \circ f$.

故连续复合 $f_1 \circ f_2 \circ \cdots \circ f_n$ 无需括号.

定义 0.7 <u>交换图</u>: $f: S_1 \to S_1$, $h: S_2 \to S_3$, $g: S_1 \to S_3$, 若 $g = f \circ h$, 则称该图**交换**.

$$
\begin{tikzcd}
 & S_3 & \\
S_1 \arrow[ur, "h"] \arrow[rr, "f"] & & S_2 \arrow[ul, "g"']
\end{tikzcd}
$$

$f: S_1 \to S_2$, $g: S_2 \to S_4$, $h: S_1 \to S_3$, $l: S_3 \to S_4$, 若 $g \circ f = l \circ h$, 则称该图**交换**.

$$
\begin{tikzcd}
S_3 \arrow[r, "l"] & S_4 \\
S_1 \arrow[u, "h"] \arrow[r, "f"] & S_2 \arrow[u, "g"]
\end{tikzcd}
$$

定义 0.8 <u>单射(Injective 或One-to-one)</u>: 映射 $f: S_1 \to S_2$, $\forall a, b \in S_1$, 若 $f(a) = f(b) \Longrightarrow a = b$, 则称 f **单射**.

单射的性质:

(1) $c \in S_2$, f 单射, 若 $f^{-1}(c) \neq \emptyset$, 则 $|f^{-1}(c)| = 1$.

(2) f 单射 $\Longleftrightarrow A = f^{-1}(f(A))$.

定义 0.9 <u>满射(Surjective)</u>: 映射 $f: S_1 \to S_2$, 若 $\forall b \in S_2$, $\exists a \in S_1$, s.t. $f(a) = b$ (即 $\operatorname{Im} f = S_2$), 则称 f **满射**.

满射的性质:

(1) f 满射 $\Longleftrightarrow \forall B \subseteq S_2$, $f^{-1}(B) \neq \emptyset$.

(2) f 满射 $\Longleftrightarrow \forall B \subseteq S_2$, $B = f(f^{-1}(B))$.

定义 0.10 <u>双射</u>: 映射 f 单射且满射 $\Longleftrightarrow f$ **双射**.

例 0.2: 恒等映射是双射的. □

常用结论:

(1) f, g 单射 $\Longrightarrow g \circ f$ 单射.

证: $\forall a,b\in S_1$, 若 $g\circ f(a)=g\circ f(b)$, $\because g$ 单射, $\therefore f(a)=f(b)$,
又 $\because f$ 单射, $\therefore a=b$, 故 $g\circ f$ 单射. □

(2) $g\circ f$ 单射 $\Longrightarrow f$ 单射.

证: $\forall a,b\in S_1$, 若 $f(a)=f(b)$, 则 $g\circ f(a)=g\circ f(b)$,
又 $\because g\circ f$ 单射, $\therefore a=b$, 故 f 单射. □

例 0.3 $g\circ f$ 单射, 而g 非单射的例子: 集合 $S_1=\{0\}$, $S_2=\{0,1\}$, $S_3=\{0\}$,
映射 $f:S_1\to S_2$, $f(a)=0\forall a\in S_1$, 单射,
$g:S_2\to S_3$, $g(b)=0\forall S_2$, 非单射, $g\circ f:S_1\to S_3$, $g(a)=0$, 单射. □

(3) f,g 满射 $\Longrightarrow g\circ f$ 满射.

证: $\forall c\in S_3$, $\because g$ 满射, $\therefore \exists b\in S_2$, s.t. $g(b)=c$,
又 $\because f$ 满射, $\therefore \exists a\in S_1$, s.t. $f(a)=b\Longrightarrow g\circ f(a)=c$, 故 $g\circ f$ 满射. □

(4) $g\circ f$ 满射 $\Longrightarrow g$ 满射.

证: $\because g\circ f$ 满射, $\therefore \forall c\in S_3$, $\exists a\in S_1$, s.t. $g\circ f(a)=c$
$\Longrightarrow \exists b=f(a)\in S_2$, s.t. $g(b)=c$, 故 g 满射. □

例 0.4 $g\circ f$ 满射, 而f 非满射的例子: 集合 $S_1=\{0\}$, $S_2=\{0,1\}$, $S_3=\{0\}$,
映射 $f:S_1\to S_2$, $f(a)=0\forall a\in S_1$, 非满射,
$g:S_2\to S_3$, $g(b)=0\forall S_2$, 满射, $g\circ f:S_1\to S_3$, $g(a)=0$, 满射. □

定理 0.2: 映射 $f:S_1\to S_2$ 单射 $\Longleftrightarrow \exists$ 映射 $g:S_2\to S_1$, s.t. $g\circ f=1_{S_1}$, 这样的 g 称为 f 的左逆.

证: "$\Longrightarrow$": 构造 $g(b)=\begin{cases} a, & a\in f^{-1}(b),\\ \text{任意取一个 } a_0\in S_1, & f^{-1}(b)=\emptyset,\end{cases}$,
$\forall a\in S_1$, 记 $b=f(a)$, $\because f$ 单射且 $a\in f^{-1}(b)\neq\emptyset$, $\therefore |f^{-1}(b)|=1$,
$\Longrightarrow g\circ f(a)=a\Longrightarrow g\circ f=1_{S_1}$.

"$\Longleftarrow$": $\forall a,b\in S_1$, 若 $f(a)=f(b)$, 则 $a=1_{S_1}=g\circ f(a)=g\circ f(b)=1_{S_1}(b)=b$, 故 f 单射. □

由于当 $f^{-1}(b)=\emptyset$ 时, $g(b)$ 的取值具有任意性, 故若左逆存在, 则不唯一.

定理 0.3: 映射 $f:S_1\to S_2$ 满射 $\Longleftrightarrow \exists$ 映射 $h:S_2\to S_1$, s.t. $f\circ h=1_{S_2}$, 这样的 h 称为 f 的右逆.

证: "$\Longrightarrow$": $\because f$ 满射, $\therefore \forall b\in S_2$, $\exists a\in S_1$, s.t. $f(a)=b$, 故可构造 $h(b)=a\in f^{-1}(b)$,
从而 $f\circ h(b)=b\Longrightarrow f\circ h=1_{S_2}$.

"$\Longleftarrow$": $\forall b\in S_2$, $\exists a=h(b)\in S_1$, s.t. $f\circ h(b)=1_{S_2}(b)=b$, 故 f 满射. □

由于 $|f^{-1}(b)|\geq 1$, $h(b)$ 的取值可能具有任意性, 故若右逆存在, 则不唯一.

定理 0.4: 若映射 f 同时存在左逆和右逆, 则其左逆 $=$ 右逆, 此时称 f 可逆, 且此时 f 双射.

证: 因为 f 同时存在左逆和右逆, 由定理 0.2 和 0.3 得 f 双射.
设左逆 $g: S_2 \to S_1$, s.t. $g \circ f = 1_{S_1}$, 右逆 $h: S_2 \to S_1$, s.t. $f \circ h = 1_{S_2}$.
假设 $g \neq h$, 则 $\exists b \in S_2$, s.t. $g(b) \neq h(b)$,
又 $\because f$ 单射, $\therefore b = 1_{S_2}(b) = f \circ g(b) \neq f \circ h(b)$.
$\because f$ 满射, $\therefore \exists a \in S_1$, s.t. $b = f(a) \Longrightarrow f(a) = b \neq f \circ g \circ f(a) = 1_{S_2}(f(a)) = f(a)$, 这显然是荒谬的, 故假设错误, $g = h$. □

0.4 等价关系和等价类

定义 0.11 **卡氏积:** 集合 S_1 和 S_2 的**卡氏积** $S_1 \times S_2 \equiv \{(a, b) \mid a \in S_1, b \in S_2\}$.
集合 S 的**卡氏积** $S \times S \equiv \{(a, b) \mid a, b \in S\}$.

注意, 一般 $(a, b) \neq (b, a)$.

定义 0.12 **关系:** 卡氏积的子集. $\mathcal{R} \in S \times S$, 称为 S 上的**关系**.

例 0.5: 自然数集 $\mathbb{N}$ 的卡氏积 $\mathbb{N} \times \mathbb{N} = \{(n, m) \mid n, m \in \mathbb{N}\}$.
小于关系: $\mathcal{R}_1 = \{(n, m) \mid n - m < 0\}$. $(1, 2) \in \mathcal{R}_1$, 记作 $1\mathcal{R}_1 2$.
等于关系: $\mathcal{R}_2 = \{(n, m) \mid n - m = 0\}$. $(1, 1) \in \mathcal{R}_2$, 记作 $1\mathcal{R}_2 1$. □

定义 0.13 **图:** 对映射 $f: S_1 \to S_2$, 有关系 $G_f = \{(a, f(a)) \mid a \in S_1\} \subseteq S_1 \times S_2$, 称 G_f 为 f 的**图**.

(第一个坐标在此关系中仅出现一次, 不会重复.)
映射与图一一对应.

定义 0.14 **等价关系:** 关系 $\mathcal{R} \in S \times S$, 若满足
反身性: $\forall a \in S$, $(a, a) \in \mathcal{R}$ (即 $a \sim a \forall a \in S$)

(2) **对称性**: 若 $(a, b) \in \mathcal{R}$, 则 $(b, a) \in \mathcal{R}$ (即$a \sim b \Longleftrightarrow b \sim a$)

(3) **传递性**: 若 $(a, b) \in \mathcal{R}$, $(b, c) \in \mathcal{R}$, 则 $(a, c) \in \mathcal{R}$ (即$a \sim b, b \sim c \Longleftrightarrow a \sim c$)

则称 $\mathcal{R}$ 为 S 上的**等价关系**. 若元素 a, b 具有等价关系, 记作 $a \sim b$.

定义 0.15 **等价类:** 由具有等价关系的元素组成的集合. $\forall a \in S$, $[a] \equiv \{b \in S \mid b \sim a\} \subseteq$ 称为 a 的**等价类**, a 称为该等价类的**代表元**.

$\because a \in [a]$, $\therefore [a]$ 非空.
$c \in S$, 则有且仅有以下两种情况:

(1) $c \in [a] \Longleftrightarrow c \sim a \Longleftrightarrow a \sim c \Longleftrightarrow a \in [c] \Longleftrightarrow [a] = [c]$.

(2) $c \notin [a] \Longleftrightarrow [a] \cap [c] = \emptyset$.

证: 假设 $[a] \cap [b] \neq \emptyset$, 则 $\exists c \in [a] \cap [b]$
$\Longleftrightarrow c \in [a]$ 且 $c \in [b]$, 即 $c \sim a$ 且 $c \sim b$
$\Longrightarrow a \sim b \Longrightarrow [a] = [b]$, 得证. □

等价类的性质

(1) $a \in [b] \iff b \in [a] \iff [a] = [b]$.

(2) $a \notin [b] \iff [a] \cap [b] = \emptyset$.

(3) $\forall a, b \in S$, 要么 $[a] = [b]$, 要么 $[a] \cap [b] = \emptyset$.
(以上三条证明见前文.)

(4) $S = \cup_{i \in K, a_i \in S}[a_i]$, 其中 $[a_i] \cap [a_j] = \emptyset \forall i \neq j$.

证: $S = \cup_a \{a\}$, 合并各等价类, 即得证. □

等价类这一概念可用于将大问题分解为小问题加以解决.

定义 0.16 剖分: 集合 $S \neq \emptyset$, 若 $S = \cup_{i \in K, S_i \subseteq S} S_i$ 且 $S_i \cap S_j = \emptyset \forall i \neq j$, 则称 $\{S_i \subseteq S \mid i \in K\}$ 为 S 的**剖分**.

可由集合的等价类得到它的一个剖分.

定义 0.17 商类: 所有等价类的集合. $\frac{S}{\sim} \equiv \{[a] \mid a \in S\}$. $\pi : S \to \frac{S}{\sim}$, $a \mapsto [a]$ 称为**自然映射**.

自然映射满射, 但未必单射.

定义 0.18 运算: 映射 $* : S \times S \to S$ 称为 S 上的**运算**, 记作 $(S, *)$.

$\forall a, b \in S$, $a * b \in S$.

0.5 群

定义 0.19 群: 若 $(G, *)$ 满足
结合律: $(a * b) * c = a * (b * c)$
(故 $a_1 * a_2 * \cdots * a_n$ 无需括号, 可写为 $\prod_{i=1}^{n} a_i$.)

(2) **有单位元** e: s.t. $e * a = a * e = a$

(3) **有逆元**: $\forall a \in G$, $\exists b$, s.t. $a * b = b * a = e$, 则称 b 为 a 的逆, 记作 $b = a^{-1}$

则称 $(G, *)$ 为**群**.

定理 0.5: 单位元是唯一的.

证: 假设 e_1, e_2 均为单位元, 则 $e_1 * e_2 = e_1 * e_2$, 得证. □

定理 0.6: 每个元素的逆元是唯一的.

证: 假设 b_1 和 b_2 均为 a 的逆元, 则 $b_1 a = b_2 a = e \Longrightarrow b_1 = b_2$, 得证. □

例 0.6: $(\mathbb{Z}, \times)$ 非群, 因 0 无逆元. □

特殊的群:

(1)

例 0.7 循环群: $G = \{a^i \mid i \in \mathbb{Z}\}$. □

(2)

例 0.8 交换群(Abel 群): $\forall a, b \in G$, $a * b = b * a$. □

群的性质:

(1) $c * c = c \Longleftrightarrow c = e$.

(2) $(a^{-1})^{-1} = a$.

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

(4) 左消去律: $a * b = a * c \Longleftrightarrow b = c$,
右消去律: $b * a = c * a \Longleftrightarrow b = c$.

定义 0.20 群的阶: $|G| \equiv$ 群中元素的个数.

定义 0.21 有限群: 若 $|G| < \infty$, 则称 G 为**有限群**.

定义 0.22 群元素的阶: $g \in G$, $0 \neq n \in \mathbb{N}$, 若 $g^n = e$, 则称最小的这样的 n 为 g 的**阶**, 记作 $|g|$, 若 n 不存在, 则称 g **无穷阶**.

若 $|G| < \infty$, 则 $\forall g \in G$, $|g| < \infty$.

证: $g \in G$, $g^2 \in G$, $\cdots$, $g^n \in G \Longrightarrow \{g, g^2, \cdots, g^n\} \in G$
$\because |G| < \infty$, $\therefore |\{g, g^2, \cdots, g^n\}| < \infty$
当 $n > |G|$, $\{g, g^2, \cdots, g^n\}$ 中必有元素重复, 故 $\exists n_1 < n_2$, s.t. $g^{n_1} = g^{n_2} \Longrightarrow e = g^{n_1} g^{-n_1} = g^{n_2} g^{-n_1} = g^{n_2 - n_1}$.
最小的这样的 $n_2 - n_1$ 即为 $|g|$, 故 $|g| < \infty$. □

定义 0.23 子群: 对群 $(G, *)$, H 为 G 的非空子集, 若 $(H, *)$ 亦为群, 则称 $(H, *)$ 为 $(G, *)$ 的**子群**, 记作 $(H, *) < (G, *)$.

例 0.9: $(\mathbb{Q}, +)$ 为群, $(\mathbb{Q}^* \equiv \mathbb{Q} - \{0\}, \times)$ 亦为群, 虽然 $\mathbb{Q}^* \subseteq \mathbb{Q}$, 但由于两者运算不同, 故 $(\mathbb{Q}^*, \times)$ 并非 $(\mathbb{Q}, +)$ 的子群. □

定理 0.7: $(H, *) < (G, *) \Longleftrightarrow H \subseteq G, \forall a, b \in H, a * b \in H$ 且 $a^{-1} \in H \Longleftrightarrow H \subseteq G, \forall a, b \in H, a * b^{-1} = H$.

证: $\underline{(H, *) < (G, *) \Longleftrightarrow H \subseteq G, \forall a, b \in H, a * b \in H \text{ 且} a^{-1} \in H}$: 由子群和群的定义即得证.
$\underline{(H, *) < (G, *) \Longleftarrow H \subseteq G, \forall a, b \in H, a * b^{-1} \in H}$: 由子群和群的定义即得证.
$\underline{(H, *) < (G, *) \Longleftarrow H \subseteq G, \forall a, b \in H, a * b^{-1} \in H}$: 取 $b = a$, 得 $a * a^{-1} = e \in H \Longrightarrow H$ 有单位元.
取 $a = e$, 得 $\forall b \in H$, $\exists e * b^{-1} = b^{-1} \in H \Longrightarrow H$ 有逆元.
H 中的运算 $*$ 的结合律继承自 G 中的 $*$ 的结合律.
综上, H 为群. 又 $\because H \subseteq G$, $\therefore H < G$. □

定义 0.24 平凡子群: $(G,*)$ 和 $(\{e\},*)$ 为 $(G,*)$ 的**平凡子群**.

定义 0.25 真子群(非平凡子群): 除平凡子群以外的子群.

定义 0.26 单群: 无真子群的群.

定理 0.8 任意多个子群的交为子群: $(G,*)$ 为群, $(H_i,*) < (G,*)\forall i$, 则 $(\cap_{i\in K}H_i,*) < (G,*)$.

证: $\forall a,b\in\cap_{i\in K}H_i \Longrightarrow \forall i\in K,\ a,b\in H_i$,
$\because (H_i,*) < (G,*)$, $\therefore a*b^{-1}\in H_i\subseteq\cap_{i\in K}H_i \Longrightarrow a*b^{-1}\in\cap_{i\in K}H_i$. □

定理 0.9: $(H,*) < (G,*)$, 则 H 的单位元即为 G 的单位元.

证: 设 G 的单位元为 e.
$\forall a\in H, \because H\in G, \therefore a\in G, e*a=a*e=a \Longrightarrow e$ 为 $(H,*)$ 的单位元,
又 $\because (H,*)$ 的单位元是唯一的, 故得证. □

例 0.10: $(\mathbb{Z},+)$ 为群, $(\mathbb{E}=\langle 2\rangle =\equiv \{vp\},+)$, $(\langle 3\rangle\equiv\{3n\mid n\in\mathbb{Z}\},+) < (\mathbb{Z},+)$. □

定义 0.27 陪集(Coset): 真子群 $H<G, \forall g\in G$, **左陪集** $gH\equiv\{g*h\mid\forall h\in H\}$, **右陪集** $Hg\equiv\{h*g\mid\forall h\in H\}$.

简便起见, 以下讨论针对左陪集, 右陪集同理.

例 0.11: $\mathbb{E}$ 在 $\mathbb{Z}$ 中的陪集: $\forall g,\ n\mathbb{E}=\{n+m\mid m\in\mathbb{E}\}=\begin{cases}\mathbb{E}, & n\text{ 为偶数},\\ 1\mathbb{E}=\mathbb{O}\equiv\{\text{奇数}\}, & n\text{ 为奇数},\end{cases}$ 故 $\mathbb{E}$ 在 $\mathbb{Z}$ 中仅有两个陪集: $\mathbb{E}$ 和 $\mathbb{O}$, 且 $\mathbb{Z}=\mathbb{E}\cup\mathbb{O}$, $\mathbb{E}\cap\mathbb{O}=\emptyset$. □

陪集的性质: 真子群 $H<G, \forall g_1,g_2\in G$,

(1) $g_1H\cap g_2H=\emptyset$ 或 $g_1H=g_2H$.

证: 假设 $g_1H\cap g_2H\neq\emptyset$, 则 $\exists c\in g_1H\cap g_2H$
$\Longleftrightarrow c\in g_1H$ 且 $c\in g_2H$
$\Longleftrightarrow \exists h_1,h_2$, s.t. $c=g_1*h_1=g_2*h_2$
$\Longrightarrow g_2^{-1}g_1=h_2*h_1^{-1}$
又 $\because h_2*h_1^{-1}\in H, \therefore g_2^{-1}*g_1\in H$
$\Longrightarrow (g_2^{-1}*g_1)*H=H$
$\Longrightarrow g_1H=g_2H$. □

(2) $|gH|=|H|$.

证: 要证 $|gH|=|H|$, 只需证 $H\to gH$ 双射.
若 $ga=gb$, 则 $a=b$, 故 $g\to gH$ 单射.
$\forall c\in gH, \exists a=g^{-1}c\in H$ 且 $ga=b$, 故 $H\to gH$ 满射.
综上, $H\to gH$ 双射, 故得证. □

(3) $G = H \cup g_1H \cup g_2H \cup \cdots \cup g_\alpha H$, 其中 $g_iH \cap g_jH = \emptyset \forall i, j$, α 仅为一指标.

证: $G = \cup_{g\in G} gH$, 去除这些并集中的重复集合, 即得证. □

(4) $g_1H = g_2H \iff g_1^{-1} * g_2 \in H$.

证: "$\Longrightarrow$": $g_1H = g_2H \Longrightarrow \forall g_1 * h_1 \in g_1H$, $g_1 * h_1 \in g_2H$
$\Longrightarrow \exists h_2 \in H$, s.t. $g_1 * h_1 = g_2 * h_2$
$\iff g_1^{-1}g_2 = h_1 * h_2^{-1}$
又 $\because h_1 * h_2^{-1} \in H$, $\therefore g_1^{-1} * g_2 \in H$.

"$\Longleftarrow$": $g_1^{-1} * g_2 \in H \Longrightarrow g_1^{-1} * g_2H = H$
$\Longrightarrow g_1H = g_2H$. □

(5)

定理 0.10 拉格朗日(Lagrange) 定理: $|G| < \infty$, 真子集 $H < G$, $|H| \mid |G|$ [a].

[a] $a \mid b$ 表示 b 可被 a 整除.

故若 $|G|$ 为质数, 其子群仅有 $\{e\}$ 和 G 两个, 此时 $\forall g \in G$, $G = \{g, g^2, \cdots, g^{|G|}\}$, 即 G 为有限阶循环交换群.

最小的有限非交换群为 6 阶.

根据 (3), 由陪集可得剖分, 由剖分可得等价关系, 由此我们引入:

(6) $g_1 \sim g_2 \iff g_1^{-1} * g_2 \in H$.

例 0.12: 群 $(\mathbb{Z}, -)$, 可分为两个子群: $(\mathbb{E}, -)$ 和 $(\mathbb{O}, -)$, 其中 $\mathbb{E} \cap \mathbb{O} = \emptyset$, 故由这两个子群可得 $\mathbb{Z}$ 的一个剖分, 这两个子群中的元素各存在等价关系: $n \sim m \iff n - m \in \mathbb{E}$. □

定义 0.28 商群: H 为 G 的正规子群, $\frac{G}{H} = \{[g] \equiv gH \mid g \in G\}$.

问题 0.1: $\frac{G}{H}$ 与 G 和 H 是否或在何种条件下具有相同的代数结构? □

答: $\frac{G}{H}$ 与 G 和 H 具有相同的代数结构, 即 $\forall [g_1], [g_2] \in \frac{G}{H}$, $[g_1] * [g_2] = [g_1 * g_2] \in \frac{G}{H}$,
即存在映射 $\frac{G}{H} * \frac{G}{H} \to \frac{G}{H}$, $([g_1], [g_2]) \mapsto [g_1, g_2])$,
即若 $g_1 \sim g_1'$, $g_2 \sim g_2'$, 则 $g_1 * g_2 \sim g_1' * g_2'$,
即若 $g_1H = g_1'H$, $g_2H = g_2'H$, 则 $(g_1 * g_2)H = (g_1' * g_2')H$.
$\because g_1H = g_1'H$, $\therefore \exists h_1, h_1' \in H$, s.t. $g_1h_1 = g_1'h_1' \iff g_1 = g_1' * h_1' * h_1^{-1}$,
$\because g_2H = g_2'H$, $\therefore \exists h_2, h_2' \in H$, s.t. $g_2h_2 = g_2'h_2' \iff g_2 = g_2' * h_1' * h_2^{-1}$,
从而 $g_1 * g_2 = g_1' * h_1' * h_1^{-1} * g_2' * h_2' * h_2^{-1}$,
若 $\exists h' \in H$, s.t. $(h_1' * h_1^{-1}) * g_2' = g_2' * h'$, 则 $g_1 * g_2 = g_1' * g_2' * h' * h_2' * h_2^{-1} \equiv g_1' * g_2' * h$,
$\Longrightarrow (g_1 * g_2)H = (g_1' * g_2' * h)H = (g_1' * g_2')H$.

故当 $gH = Hg$ 时, $\frac{G}{H}$ 与 G 和 H 具有相同的代数结构. □

定理 0.11 正规子群: 若 $gH = Hg$, 则 $\frac{G}{H}$ 与 G 和 H 具有相同的代数结构, 此时称 H 为 G 的**正规子群**.

定理 0.12: 交换群的任意一个子群为正规子群.

例 0.13: $(\mathbb{Z}, +)$ 的子群均为循环群, $\langle m\rangle \equiv \{mn \mid n \in \mathbb{Z}\}$, $\mathbb{Z}_n \equiv \frac{\mathbb{Z}}{\langle n\rangle}$, $\mathbb{Z}_m$ 有 m 个等价类: $\mathbb{Z}_m = \cap_{i=0}^{m-1}[i]$. □

定义 0.29 群同态: 对群 $(G_1, *)$ 和 $(G_2, \circ)$, 若映射 $f : G_1 \to G_2$ 满足 $f(a * b) = f(a) \circ f(b)$ (即映射后保持代数结构), 则称 f 为 G_1 到 G_2 的**群同态**.

(类似于集合间的映射)

定义 0.30 单同态: 单射的群同态.

定义 0.31 满同态: 满射的群同态.

定义 0.32 同构: 双射的群同态.

定理 0.13: f 为 G_1 到 G_2 的群同态, e_1 和 e_2 分别是 G_1 和 G_2 的单位元, 则 $f(e_1) = e_2$.

证: $f(e_1) = f(e_1 * e_1) = f(e_1) \circ f(e_1) \Longrightarrow f(e_1) = e_2$. □

定理 0.14: f 为 G_1 到 G_2 的群同态, $f(a^{-1}) = [f(a)]^{-1}$.

证: $e_2 = f(e_1) = f(a * a^{-1}) = f(a) \circ f(a^{-1}) \Longrightarrow f(a^{-1}) = [f(a)]^{-1}$. □

定义 0.33 群同态的核(Kernel): 单位元的原像. f 为 G_1 到 G_2 的群同态, e_1 和 e_2 分别是 G_1 和 G_2 的单位元, 则称 $\ker f \equiv f^{-1}(e_2) = \{a \in G_1 \mid f(a) = e_2\}$ 为 f 的**核**.

$\because e_1 \in \ker f$, $\therefore \ker f \neq \emptyset$.

$\ker f \subseteq G_1$.

证: $\forall a, b \in \ker f$, $f(a * b^{-1}) = f(a) \circ f(b) = f(a) \circ [f(b)]^{-1} = e_2 * e_2^{-1} = e_2 \Longrightarrow a * b^{-1} \in \ker f$, 故 $\ker f \subseteq G_1$. □

定义 0.34 群同态的像: f 为 G_1 到 G_2 的群同态, 则称 $\operatorname{Im} f \equiv f(G_1) = \{f(a) \mid a \in G_1\}$ 为 f 的**像**.

$\operatorname{Im} f \in G_2$.

定理 0.15: f 单同态 $\Longleftrightarrow \ker f = \{e_1\}$.

证: "$\Longrightarrow$": $\forall a, b \in \ker f$, $f(a) = f(b) = e_2$,
又 $\because f$ 单同态, $\therefore a = b = e$.

"$\Longrightarrow$": 若 $f(a) = f(b)$, 则 $f(a) \circ [f(b)]^{-1} = e_2$
$\Longrightarrow f(a) \circ f(b^{-1}) = e_2$
$\Longrightarrow f(a * b^{-1}) = e_2$
$\Longrightarrow a * b^{-1} \in \ker f = \{e_1\}$
$\Longrightarrow a = b = e_1$, 故 f 单同态. □

0.6 环

定义 0.35 环: 若 $(R, +, \cdot)$ 满足

$(R, +)$ 为交换群 (单位元记作 0)

(2) **结合律**: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(3) **左分配律**: $a \cdot (b + c) = a \cdot b + a \cdot c$,
右分配律: $(a + b) \cdot c = a \cdot c + b \cdot c$

则称 $(R, +, \cdot)$ 为**环**.

例 0.14: $(\mathbb{Z}, +, \times)$ 为环. □

常用结论:

(1) $0 \cdot a = a \cdot 0 = 0$.

证: $a \cdot 0 = 0 \cdot a = (0 + 0) \cdot a = 0 * a + 0 * a = 0 * a + a * 0 \Longrightarrow 0 \times a = a \cdot 0 = 0$. □

(2) $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$.

证: $(-a) \cdot b + a \cdot b = [a + (-a)] \cdot b = 0 \cdot b = 0 \Longrightarrow (-a) \cdot b = -(a \cdot b)$.
$a \cdot (-b) + a \cdot b = a \cdot [b + (-b)] = a \cdot 0 = 0 \Longrightarrow a \cdot (-b) = -(a \cdot b)$. □

(3) $\left(\sum_i a_i\right) \cdot \left(\sum_j b_j\right) = \sum_{i,j} a_i \cdot b_j$.

证: 由左右分配律即得证. □

特殊的环:

(1)

定义 0.36 交换环: 若 $\forall a, b \in R$, $a \cdot b = b \cdot a$, 则称 R 为**交换环**.

(2)

定义 0.37 有单位元的环: 若 $\exists 1 \in R$, s.t. $\forall a \in R$, $1 \cdot a = a \cdot 1 = a$, 则称 R 为**有单位元的环**, 称 1 为 R 的**单位元**.

例 0.15: $(\mathbb{Z}, +, \cdot)$ 交换且有单位元. □

例 0.16: $(M_{n\times n}, +, \times)$ [1] 非交换, 有单位元 $I_{n\times n}$. □

例 0.17: $(\mathbb{E}, +, \times)$ 交换, 无单位元. □

定义 0.38 零因子: $0 \neq a \in R$, 若 $\exists 0 \neq b \in R$, s.t. $a \cdot b = 0$ 或 $b \cdot a = 0$, 则称 a 为 R 的**零因子**.

[1] $M_{n\times m} \equiv \{(a_{i,j})_{m\times n} \mid a_{i,j} \in \mathbb{R}\}$.

定义 0.39 **整环:** 有单位元, 交换, 无零因子的环.

定义 0.40 **子环:** 非空真子集 $\emptyset \neq R_1 \subseteq R$, 若 $(R_1, +, \cdot)$ 亦为环, 则称 R_1 为 R 的**子环**.

$\because (R_1, +)$ 为交换群, $\therefore (R_1, +) < (R, +)$.

定理 0.16 **子环的判定:** R_1 为 R 的子环 $\iff \forall a, b \in R_1$, $a - b \in R_1$, $a \cdot b \in R_1$.

定理 0.17: R 为有单位元的交换环, 则 R 为整环 $\iff \forall 0 \neq r \in R$, $a, b \in R$, 若 $r \cdot a = r \cdot b$, 则必有 $a = b$.

证: "$\Longrightarrow$": $r \cdot a = r \cdot b \Longleftrightarrow r \cdot (a - b) = r \cdot a - r \cdot b = r \cdot b - r \cdot b = 0$,
$\because r \neq 0$ 且 R 为整环 (无零因子), $\therefore a - b = 0 \Longrightarrow a = b$.

"$\Longleftarrow$": 假设 R 有零因子, $r_0 \cdot a_0 = 0$, 则令 $r = r_0$, $\forall a, b \in R$, 若 $r \cdot a = r \cdot b = 0$, 则 $a - b = 0$ 或 $a - b = a_0$ 或 $a - b = a_0 + a_0, \cdots$, 矛盾, 故假设错误, R 无零因子.
又 $\because R$ 为有单位元的交换环, $\therefore R$ 为整环. □

定义 0.41 **理想:** 非空子集 $I \subseteq R$, 若 $\forall a, b \in I$, $r \in R$, $a - b \in I$, $r \cdot a \in I$, $a \cdot r \in I$, 则称 I 为 R 的**理想**.

定义 0.42 **平凡理想:** $(\{0\}, +, \cdot)$ 和 $(R, +, \cdot)$ 为 $(R, +, \cdot)$ 的**平凡理想**.

定义 0.43 **单环:** 只有平凡理想的环.

定理 0.18: 任意多个理想的交为理想.

证: $\because 0 \in \cap_{i\in K} I_i$, $\cap_{i\in K} I_i = \emptyset$.
$\because \forall a, b \in \cap_{i\in K} I_i$, $\therefore \forall a, b$, $\forall k \in K$, $a, b \in I_k$,
又 $\because \forall k \in K$,$(I_k, +) < (R, +)$, $\therefore \forall k \in K$,$a - b \in I_k \Longrightarrow a - b \in \cap_{i\in K} I_i$.

$\forall k \in K$, $a_k \in I_k$, 又 $\because I_k$ 为理想, $r \cdot a \in I_k$, $a \cdot r \in I_k \Longrightarrow r \cdot a \in I_k$, $a \cdot r \in I_k$.

综上, $\cap_{i\in K} I_k$ 为 R 的理想. □

定理 0.19: 若 $I_1 \subseteq I_2 \subseteq \cdots$ 是 R 中理想的升链, 则 $\cup_i I_i$ 是 R 的理想.

定义 0.44 **生成理想:** R 为交换环, 非空子集 $\emptyset \neq S \in R$, 由 S 生成的理想是 R 中包含 S 的最小理想, 即 R 中包含 S 的所有理想的交, 记作 $\langle S \rangle$.

证: 假设 I_0 是 R 中包含 S 的最小理想, $J = \{I_k \mid k \in K\}$ 是 R 中包含 S 的所有理想的集合.
显然 $I_0 \in J$, 故 $\cap_k I_k \subseteq I_0$.
$\because \cap_{i\in K} I_k$ 为理想, 又 $\because I_0$ 为最小的理想, $\therefore |I_0| \leq |\cap_k I_k|$.
综上, 必有 $I_0 = \cap_k I_k$. □

- 由某个元素 a 生成的理想: $\langle a\rangle = \{r\cdot a \mid r\in R\}$.
- 由多个元素 $\{a_1,\cdots,a_n\}$ 生成的理想: $\langle a_1,\cdots,a_n\rangle = \{\sum_{i=1}^n r_i a_i \mid r_i\in R\}$.
- 由集合 S 生成的理想: $\langle S\rangle = \{\sum_{i=1}^m \mid r_i\in R, a_i\in S, m\in\mathbb{Z}^+\}$.

可用理想得等价关系: I 是 R 的理想, 则 $r_1\sim r_2 \Longleftrightarrow r_1-r_2\in\mathbb{I}$, 从而得到等价关系: $[a]=a+I=\{a+r \mid r\in I\}$.

定义 0.45 商环: $\frac{R}{\sim}\equiv\{[a]\mid a\in R\}$.

$([a],[b])\mapsto[a+b]$ 和 $([a],[b])\mapsto[a\cdot b]$ 都是运算.

证: 要证 $([a],[b])\mapsto[a+b]$ 和 $([a],[b])\mapsto[a\cdot b]$ 都是运算, 即证这些映射与代表元无关,
即证 $a\sim a'$, $b\sim b'$, $[a']+[b']=[a+b]$, $[a']\cdot[b']=[a\cdot b]$.

$\because a\sim a'$, $b\sim b'$, $\therefore a-a'\in I$, $b-b'\in I \Longrightarrow a+b-(a'+b')=(a-a')+(b-b')\in I$
$\Longrightarrow a+b\sim a'+b'$, 故 $([a,b])\mapsto[a+b]$ 与代表无关, 是运算.

$\because a\sim a'$, $b\sim b'$, $\therefore a-a'\in I$, $b-b'\in I$,
设 $a-a'\equiv h_1\in I$, $b-b'\equiv h_2\in I$, 则 $a'\cdot b'=(a+h_1)\cdot(b+h_2)=a'\cdot b'+a'\cdot h_2+h_1\cdot b'+h_1\cdot h_2$,
其中 $\because h_1,h_2\in I\Longrightarrow h_1\cdot h_2\in I$, 而由理想的定义, $a'\cdot h\in I$, $h_1\cdot b'\in I$,
$\Longrightarrow a'\cdot b'=a\cdot b-a'\cdot h_1-h_2\cdot b\in I$, 故 $[a']\cdot[b']=[a'\cdot b']=[a\cdot b]$. □

定义 0.46 环同态: $(R_1,+,*)$ 和 $(R_2,+,\cdot)$ 为环, 映射 $f:R_1\to R_2$ 满足

(1) $f(a+b)=f(a)+f(b)$

(2) $f(a\cdot b)=f(a)\cdot f(b)$

则称 f 为 R_1 到 R_2 的**环同态**.

由环同态的定义, f 必为 $(R_1,+)$ 到 $(R_2,+)$ 的群同态, 故 $f(0)=0$, $f(a^{-1})=[f(a)]^{-1}$.

定义 0.47 核: $\ker f\equiv\{a\in R_1\mid f(a)=0\}$.

定义 0.48 像: $\operatorname{Im} f\equiv\{f(a)\mid a\in R_1\}$.

$\operatorname{Im} f\subseteq R_2$.

定理 0.20: $\ker f$ 为理想.

证: $\forall a,b\in\ker f$, $r\in R_1$, $f(a-b)=f(a+(-b))=f(a)+f(-b)=f(a)-f(b)=0-0=0\Longrightarrow a-b\in\ker f$.
$f(r\cdot a)=f(r)\cdot f(a)=f(r)\cdot 0=0\Longrightarrow r\cdot a\in I$,
同理 $a\cdot r\in I$.

综上, $\ker f$ 为 R_1 的理想. □

定义 0.49 单同态: 单射的环同态.

单同态 $\iff \ker f = \{0\}$.

定义 0.50 满同态: 满射的环同态.

满同态 $\iff \operatorname{Im} f = R_2$.

定义 0.51 同构: 双射的环同态.

定义 0.52 典范同态: I 为 R 的理想, $\pi : R \to \frac{R}{I}$, $a \mapsto [a]$ 称为**典范同态**.

典范同态是满同态.

例 0.18: $(\mathbb{Z}, +, \cdot)$ 为环.
$\langle 2 \rangle = \mathbb{O} \equiv \{2n \mid n \in \mathbb{Z}\}$.
$\langle 3 \rangle \equiv \{3n \mid n \in \mathbb{Z}\}$.
$\langle 2, 3 \rangle \equiv \{2n + 3m \mid n, m \in Z\} = \mathbb{Z}$. $\langle 1 \rangle \equiv \mathbb{Z}$.
$\mathbb{Z}$ 的任何理想均由一个数生成. 更准确地说, 若 I 为 $\mathbb{Z}$ 的理想, 则 $I = \langle n \rangle$, 其中 n 为 I 中最小的正整数. □

(此处其实用到了这样一个定理: 任何一个由自然数组成的集合均存在最小正整数.)

证: 若 $p \in \mathbb{Z}$, $p \in \langle n \rangle$, 我们无妨假设 $p > n$, 设 $p = kn + r$, 其中 $0 \le r < n$.
若 $r \neq 0$, 则 $r = p - kn \in I$, 但 $0 \le r < n$ 而 n 为 $\langle n \rangle$ 中最小的正整数矛盾, 故 $r = 0$, $p = kn$. □

定义 0.53 剩余类环: $\mathbb{Z}_n \equiv \frac{\mathbb{Z}}{\langle n \rangle} = \{[0], [1], \cdots, [n-1]\}$.

例 0.19: $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$, $[2] \cdot [3] = [6] = [0]$, 故 $\mathbb{Z}_6$ 有零因子. □

0.7 域

定义 0.54 域: 若 $(F, +, \cdot)$ 满足

$(F, +)$ 为交换群 (单位元记作 0)

(2) $(F^*, \cdot)$ 为交换群 (单位元记作 1), 其中 $F^* = F - \{0\}$

(3) **左分配律**: $a \cdot (b + c) = a \cdot b + a \cdot c$,
右分配律: $(a + b) \cdot c = a \cdot c + b \cdot c$

则称 $(F, +, \cdot)$ 为**域**.

由于有 0 和 1 这两个元素, $|F| \ge 2$. 当 $|F| = 2$ 时, $F = \{0, 1\} \approxeq \mathbb{Z}_2 = \frac{\mathbb{Z}}{\langle 2 \rangle}$.

例 0.20: $\mathbb{Z}_2$ 是最小的有限域. $\mathbb{Q}$ 为最小的无限域. □

定义 0.55 <u>**有理数:**</u> $\mathbb{Q}=\left\{\frac{m}{n}\mid n\neq 0,n,m\in\mathbb{Z}\right\}$, 即 $\forall q\in\mathbb{Q}$, $\exists m,n\in\mathbb{Z}$, $n\neq 0$, $q=\frac{m}{n}$.

定义 0.56 <u>**域的特征:**</u> $\operatorname{char}F\equiv$ 使得 $n\cdot 1=\overbrace{1+1+\cdots+1}^{n\text{ 个 }1\text{ 相加}}=0$ 的最小正整数.

例 0.21: $\operatorname{char}\mathbb{Z}_2=2$, $\operatorname{char}\mathbb{Q}=0$. □

$p=\operatorname{char}F$ 必为质数, 否则 $\exists m,n<p$, s.t. $0=p\cdot 1=(n\cdot m)\cdot 1=(m\cdot 1)\cdot(n\cdot 1)\Longrightarrow n\cdot 1=0$ 或 $m\cdot 1=0$ 与域的特征的定义矛盾.

当 p 为质数且 $\operatorname{char}\mathbb{Z}_p=p$ 时, $\mathbb{Z}_p$ 为域.

定义 0.57 <u>**域同态:**</u> $(F_1,+,\cdot)$ 和 $(F_2,+,\cdot)$ 为域, 映射 $f:F_1\to F_2$ 满足

(1) $f(a+b)=f(a)+f(b)$

(2) $f(a\cdot b)=f(a)\cdot f(b)$

则称 f 为 F_1 到 F_2 的**域同态**.

域同态的性质:

(1) $f(0)=0$.

(2) $f(1)=1$ 或 0.

证: $f(1)=f(1\cdot 1)=f(1)\cdot f(1)\Longrightarrow f(1)-f(1)\cdot f(1)=0\Longrightarrow f(1)=0$ 或 1. □

(3) 若 $f(1)=0$, 则 $\forall r\in F_1$, $f(r)=f(r\cdot 1)=f(r)\cdot f(1)=f(r)\cdot 0=0$.

(4) 若 $f(1)=1$, 则 $\ker f=\{0\}$, 此时 f 单射.

证: $\forall r\in F^*$, $r^{-1}\in F^*$, $1=f(1)=f(r\cdot r^{-1})=f(r)\cdot f(r^{-1})\Longrightarrow f(r)\neq 0$, $f(r^{-1})\neq 0$, 故 $\forall r\neq 0$, $f(r)\neq 0$, $\ker f=\{0\}$. □

Chapter 1

向量空间

定义 1.1 **向量空间:** 交换群 $(V,+)$ 和域 F, 数乘映射 $\alpha : F \times V \to V$, 若满足

$\alpha(r, u+v) = \alpha(r,u) + \alpha(r,v)$ (可简写为 $r(u+v) = ru + rv$)

(2) $\alpha(r+t, u) = \alpha(r,u) + \alpha(t,u)$ (可简写为 $(r+t)u = ru + tu$)

(3) $\alpha(r \cdot t, u) = \alpha(r, \alpha(t,u))$ (可简写为 $(rt)u = r(tu)$)

(4) **有单位元**: $\exists 1 \in F$, s.t. $\alpha(1,u) = u$ (可简写为 $1u = u$)

则称 V 是 F 上的**向量空间**.

例 1.1 **直角坐标系:** $(\mathbb{R}, +, \cdot)$ 为域, $(\mathbb{R}^2 \equiv \{(x,y) \mid x, y \in \mathbb{R}\}, +)$ 为交换群, 满足

(1) $r((x_1,y_1)+(x_2,y_2)) = r(x_1+x_2, y_1+y_2) = (rx_1+rx_2, ry_1+ry_2) = (rx_1, ry_1)+(rx_2, ry_2) = r(x_1,y_1)+r(x_2,y_2)$

(2) $(r+t)(x,y) = ((r+t)x, (r+t)y) = (rx+tx, ry+ty) = (rx, ry) + (tx, ty) = r(x,y) + t(x,y)$

(3) $(r \cdot t)(x,y) = (rtx, rty) = r(tx, ty) = r(t(x,y))$

(4) $1(x,y) = (x,y)$

故 $\mathbb{R}^2$ 为 $\mathbb{R}$ 上的向量空间. □

$0v = 0$. (注意两个 0 的区别, 等号左边的 0 为域 F 中的零元, 等号右边的 0 为 V 中的零向量.)

证: $0v = (0+0)v = 0v + 0v \Longrightarrow 0v = 0$. □

$r \in F$, $0 \in V$, 则 $r0 = 0$.

证: $r0 = r(0+0) = r0 + r0 \Longrightarrow r0 = 0$. □

$-1v = -v$.

证: $-1v = -(1v) = -v$. □

例 1.2: $\mathbb{R}^2$ 为 $\mathbb{R}$ 上的向量空间.
$\mathbb{R}^2$ 为 $\mathbb{Q}$ 上的向量空间.
$\because$ 对 $c \in \mathbb{C}$, $v \in \mathbb{R}^2$, $cv \notin \mathbb{R}^2$, $\therefore \mathbb{R}^2$ 不是 $\mathbb{C}$ 上的向量空间. □

例 1.3: $F^n \equiv \{(r_1, \cdots, r_n) \mid r_i \in F\}$, 满足 $(r_1, \cdots, r_n) + (l_1, \cdots, l_n) = (r_1 + l_1, \cdots, r_n + l_n)$, $r(r_1, \cdots, r_n) = (rr_1, \cdots, rr_n)$. F^n 为 F 上的向量空间. □

证: $\because$ $r((r_1, \cdots, r_n) + (l_1, \cdots, l_n)) = r(r_1 + l_1, \cdots, r_n + l_n) = (rr_1 + rl_1, \cdots, rr_n + rl_n) = (rr_1, \cdots, rr_n) + (rl_1, \cdots, rl_n) = r(r_1, \cdots, r_n) + r(l_1, \cdots, l_n)$,
且 $(r + t)(r_1, \cdots, r_n) = ((r + t)r_1, \cdots, (r + t)r_n) = (rr_1 + tr_1, \cdots, rr_n + tr_n) = (rr_1, \cdots, rr_n) + (tr_1, \cdots, tr_n) = r(r_1, \cdots, r_n) + t(r_1, \cdots, r_n)$,
且 $(r \cdot t)(r_1, \cdots, r_n) = (rtr_1, \cdots, rtr_n) = r(tr_1, \cdots, tr_n) = r(t(r_1, \cdots, r_n))$,
且 $1(r_1, \cdots, r_n) = (r_1, \cdots, r_n)$,
$\therefore F^n$ 为 F 上的向量空间. □

定义 1.2 子空间: $\emptyset \neq S \subseteq V$, 若 S 为 V 的子群, 且在相同的数乘下构成 F 上的向量空间, 则称 S 是 V 的子空间.

定理 1.1 子空间的判定(课本定理1.1): S 为 V 的子空间 $\iff \forall a, b \in S$, $r, t \in F$, $ra + tb \in S$ (即线性运算封闭).

证: "$\Longrightarrow$": $ra \in S$, $-tb \in S$, 又 $\because S$ 为 V 的子群, $ra - (-tb) \in S$.

"$\Longrightarrow$": 令 $r = 1$, $t = -1$, 有 $a - b \in S \Longrightarrow S < V$.
令 $t = 0$, 有 $ra \in S$, 故 S 为 V 的子空间.

综上, 得证. □

子空间的交是子空间.

证: 设 $S_1, \cdots, S_n$ 为 V 的子空间, 则 $S_1, \cdots, S_n$ 为 V 的子群 $\Longrightarrow \cap_{i=1}^n S_i$ 为 V 的子群.

$\forall u, v \in \cap_{i=1}^n S_i$, $\forall k$, $u, v \in S_k \Longrightarrow u, v$ 满足与 F 中向量相同的数乘映射.

综上, 得证. □

S, T 是 V 的子空间, $S + V \equiv \{u + v \mid u \in S, v \in T\}$ 为 V 的子空间.

证: $\forall w_1, w_2 \in S + T$, $r, t \in F$,
$w_1 \in S + T \Longrightarrow w_1 = u_1 + v_1$, $u_1 \in S$, $v_1 \in T$,
$w_2 \in S + T \Longrightarrow w_2 = u_2 + v_2$, $u_2 \in S$, $v_2 \in T$.
$rw_1 + tw_2 = r(u_1 + v_1) + t(u_2 + v_2) = (ru_1 + tu_2) + (rv1 + tv_2)$, 其中 $ru_1 + tu_2 \in S$, $rv_1 + tv_2 \in T \Longrightarrow rw_1 + tw_2 \in S + T$,
故 $S + T$ 为 V 的子空间. □

定义 1.3 生成子空间和生成集: $\emptyset \neq S \subseteq V$, S 的**生成子空间**为 $\langle S \rangle \equiv$ 包含 S 的最小子空间 $= \{\sum_{i=1}^n r_i u_i \mid r_i \in F, u_i \in S, r$
其中称 S 为**生成集**.

例 1.4: 向量空间 $\mathbb{R}^2$,
$S_x = \langle\{(1, 0)\}\rangle = \{(x, 0) \mid x \in \mathbb{R}\} = x$ 轴,
$S_y = \langle\{(0, 1)\}\rangle = \{(0, y) \mid y \in \mathbb{R}\} = y$ 轴,
$\langle\{(1, 0), (0, 1)\}\rangle = \langle\{(1, 1), (1, -1)\}\rangle = \mathbb{R}^2$, 故对同一生成子空间, 生成集不唯一. □

定义 1.4 线性无关: 非零元 $u_1, \cdots, u_m$, 若 $r_1u_1 + \cdots + \cdots + r_mu_m = 0 \Longrightarrow r_1 = \cdots = r_m = 0$, 则称 $u_1, \cdots, u_m$ **线性无关**.
若 S 中任意有限个元素线性无关, 则称 S **线性无关**.

例 1.5: $(1,0)$ 与 $(0,1)$ 线性无关. □

证: $r_1(1,0) + r_2(0,1) = (r_1, r_2) = 0 = (0,0) \Longrightarrow r_1 = 0, r_2 = 0$. □

例 1.6: $\mathbb{R}^2$ 上线性无关, 即两非零元夹角非零. □

单个非零元 v 线性无关.

证: $rv = 0$ 且 $v \neq 0 \Longrightarrow r = 0$, 故 v 线性无关. □

定义 1.5 线性相关: $u_1, \cdots, u_m$, 若 $\exists$ 不全为零的 $r_1, \cdots, r_m$, s.t. $r_1u_1 + \cdots + r_mu_m = 0$, 则称 $u_1, \cdots, u_m$ **线性相关**.

若 u, v 线性相关, 则两者共线.

证: $\exists r, t$ 不全为零, s.t. $ru + tv = 0$, 无妨设 $0 \neq r \in F$, 则 $ru = -tv \Longrightarrow r^{-1}ru = -r^{-1}tv \Longrightarrow u = -\frac{u}{r}v$ □

定义 1.6 线性表示: v 可由 $u_1, \cdots, u_n$ **线性表示** $\Longleftrightarrow \exists r_1, \cdots, r_n \in F$, s.t. $v = \sum_{i=1}^{n} r_iu_i$.

定理 1.2 (课本定理1.6): S 线性无关 $\Longleftrightarrow \langle S \rangle$ 中的每个向量可由 S 中元素唯一地线性表示
$\Longleftrightarrow S$ 中任一向量不能由 S 中其余向量线性表示.

证: 设 $S = \{u_1, \cdots, u_m\}$.

第一个 "$\Longrightarrow$": $v \in \langle S \rangle$, 则 v 可由 S 中的元素线性表示, 即 $\exists r_1, \cdots, r_m$, s.t. $v = r_1u_1 + \cdots + r_mu_m$.
要证这种线性表示是唯一的, 假设 v 的另一种线性表示为 $v = r_1'u_1 + \cdots + r_m'u_m$.
$v - v = (r_1 - r_1')u_1 + \cdots + (r_m - r_m')u_m = 0$, 又 $\because S$ 线性无关, 即 $u_1, \cdots, u_m$ 线性无关, $\therefore r_1' = r_1$, $r_m' = r_m$, 故两种线性表示相同.

第一个 "$\Longleftarrow$": $0 \in \langle S \rangle$, 由于 $0u_1 + \cdots + 0u_m =$ 是且是 0 唯一的线性表示, 故 S 线性无关.

第二个 "$\Longrightarrow$": 不妨假设 u_1 可由 $u_2, \cdots, u_m$ 线性表示, 即 $u_1 = t_2u_2 + \cdots + t_mu_m$.
若 $r_1u_1 + \cdots + r_mu_m = 0$, 则 $r_1 = \cdots = r_m = 0$ 或 $r_1 \neq 0$, $r_2 = -r_1t_2, \cdots, r_m = -r_mt_m$, 从而 S 线性相关, 故假设错误, u_1 不可由 $u_2, \cdots, u_m$ 线性表示.

第二个 "$\Longleftarrow$": 假设 S 线性相关, 则 $\exists$ 非零 $r_1, \cdots, r_m$, s.t. $r_1u_1 + \cdots + r_mu_m = 0$, 不妨设 r_1 非零, 则 $u_1 = -\frac{r_2}{r_1}u_2 - \cdots - \frac{r_m}{r_1}u_m$, 即 u_1 可由 S 中其余向量线性表示, 矛盾, 故假设错误, S 线性无关. □

定理 1.3 (课本定理1.7): $\emptyset \neq S \subseteq V$, 下列等价:

(1) S 线性无关, 且 $V = \langle S \rangle$

(2) $\forall v \in V$, 可用 S 中元素唯一地线性表示

(3) S 是 V 的极小生成集 (即 S 去除任意元素都无法生成 V, 或 S 的任意真子集都无法生成 V)

(4) S 是 V 的极大线性无关集 (即 S 增加任意元素都线性相关, $\forall u \in V$ 且 $u \notin S$, $S \cup \{u\}$ 线性相关)

证: 由定理 1.2 证得 (1)(2) 等价.

设 $S = \{u_1, \cdots, u_m\}$.

(1)$\Longrightarrow$(3): 假设 $\exists S' \subsetneq S$, s.t. $V = \langle S' \rangle$, 则 $\forall v \in S - S' \subseteq V$, $v = \sum_{i=1}^m r_i u_i$, 其中 $r_i \in F$, $u_i \in S'$, $m \in \mathbb{N}$, 即 v 可由 S 中的部分向量线性表示, 与 S 线性无关矛盾, 故假设错误, S 是 V 的极小生成集.

(3)$\Longrightarrow$(1): S 为 V 的生成集, 即 $V = \langle S \rangle$.
假设 S 线性相关, 即 $\exists r_1, \cdots, r_m$ 不全为零, s.t. $\sum_{i=1}^m r_i u_i = 0$, 不妨设 $r_1 \neq 0$, 则 $u_1 = -\frac{r_2}{r_1} u_2 + \cdots + \frac{r_m}{r_1} u_m$, 则 $S - \{u_1\}$ 仍可以生成 V, 矛盾, 故假设错误, S 线性无关.

(1)$\Longrightarrow$(4): 假设 S 不是极大线性无关集, 则 $\exists v \in V - S$, s.t. $S \cup \{v\}$ 线性无关.
又 $\because V = \langle S \rangle$, $\therefore v = \sum_{i=1}^m r_i u_i$, 其中 $r_i \in F$, $u_i \in S$, $m \in \mathbb{N}$, 即线性无关集 $S \cup \{v\}$ 中的向量 v 可由其中的部分向量线性表示, 与 $S \supseteq$ 线性无关矛盾, 故假设错误, S 是极大线性无关集.

(4)$\Longrightarrow$(1): $\because S$ 是 V 的极大线性无关集, $\therefore S$ 线性无关.
假设 $V \neq \langle S \rangle$, $\exists v \in V - S$, s.t. v 无法由 S 中的元素线性表示 $\Longrightarrow S \cup \{v\}$ 为线性无关集, 与 S 为最大线性无关集矛盾, 故假设错误, $V = \langle S \rangle$.

综上, 得证. □

定义 1.7 基: 任何生成向量空间 V 的线性无关集. 基的阶数称为 V 的**维数**, 记作 $\dim V$.

定理 1.4 (课本定理1.12): 向量空间的任何基都有相同的阶, 即 $\dim V$ 不依赖于基的选取.

例 1.7: $e_1 = (1, 0, \cdots, 0)$, $e_2 = (0, 1, \cdots, 0)$, $\cdots$, $e_n = (0, 0, \cdots, 1)$ 为 F^n 的一组基. □

证: $r_1 e_1 + \cdots + r_n e_n = (r_1, \cdots, r_n) = 0 \Longrightarrow r_1 = \cdots = r_n = 0$, 故 $e_1, \cdots, e_n$ 线性无关.
又 $\langle \{e_1, \cdots, e_n\} \rangle = \{r_1 e_1 + \cdots + r_n e_n = (r_1, \cdots, r_n) \mid r_i \in F,\ 对\ i = 1, \cdots, n\} = F$, 故得证. □

找基的方法:

(1) 若 $0 \neq u_1 \in V$, 则 $\{u_1\}$ 线性无关.

(2) 若 $u_2 \in V - \langle u_1 \rangle$ 且 u_2 与 u_1 线性无关, 则 $\{u_1, u_2\}$ 线性无关.

(3) 重复以上操作, 直至无法找到新的线性无关元素, 即得到极大线性无关集, 此即向量空间的基.

定理 1.5 (课本定理1.9): 线性无关集 $I \subseteq V$, $S \subseteq V$ 是 V 的生成集, 且 $I \subseteq S$, 则 $\exists V$ 的基 $\mathcal{B}$, s.t. $I \subseteq \mathcal{B} \subseteq S$.

定义 1.8 直和: (1) **外直和**: 若 $V_1, \cdots, V_n$ 是 F 上的向量空间, $V_1 \oplus \cdots \oplus V_n \equiv \{(v_1, \cdots, v_n) \mid v_i \in V_i\}$, 满足

- $(v_1, \cdots, v_n) + (u_1, \cdots, u_n) = (v_1 + u_1, \cdots, v_n + u_n)$
- $r(v_1, \cdots, v_n) = (rv_1, \cdots, rv_n)$

则$V_1 \oplus \cdots \oplus V_n$ 为 F 的向量空间, $V_1 \oplus \cdots \oplus V_n$ 为 $V_1, \cdots, V_n$ 的**外直和**.

(2) **内直和**: V 是 F 上的向量空间, $V_1, \cdots, V_n$ 是 V 的子空间, 若 $V = \sum_{i=1}^n V_i$, 其中 $v_i \in V_i$ 且 $V_i \cap (\cup_{j \neq i} V_j) =$

$\{0\}$, 则称 V 为 $V_1, \cdots, V_m$ 的**内直和**, 记作 $V = \bigoplus_{i=1}^n V_i$, 称 V_i 为**直和项**.

内/外直和的关系: $V = V_1 \oplus \cdots \oplus V_n$, $V_1' = \{(v_1, 0, \cdots, 0) \mid v_i \in V_i\}$, $\cdots$, $V_m' = \{(0, 0, \cdots, v_m) \mid v_m \in V_m\}$ 是 V 的子空间, 则 $V = \bigoplus_{i=1}^n V_i$ 且 $V_i' \cap (\cup_{j\neq i} V_j) = \{0\} \Longrightarrow V_i = \bigoplus_{i=1}^m V_i'$, 故内/外直和是等价的, 以下我们不明确区分内/外直和, 均用内直和.

例 1.8: $\mathbb{R}^2 = S_x \oplus S_y$. □

定理 1.6 (课本定理1.5): $\{V_i \mid i \in J\}$ 是 V 的子空间集合, $V = \sum_{i\in J} V_i$, 则下列等价:

(1) $V = \bigoplus_{i\in J} V_i$

(2) $V_i \cap (\sum_{j\neq i} V_j) \neq \{0\}$

(3) $0 = 0 + \cdots + 0$ 是 0 的唯一分解式

(4) V 中任一向量 v 具有唯一分解式 $v = v_1 + \cdots + v_n$, 分解式中的有限个非零元 $v_i \in V_i$ 组成的集合成为支集

证: (1)$\Longleftrightarrow$(2): 由直积的定义即得证.

(2)$\Longrightarrow$(3): 假设 $0 = s_{i1} + \cdots + s_{in}$ 且 s_{ij} 不全为零, 不妨设 $s_{i1} \neq 0$, 则 $V_{i1} \ni s_{i1} = -s_{i2} - \cdots - s_{ij} \in \sum_{j=2}^n V_{ij}$ $\Longrightarrow s_{i_1} \in V_{i_1} \cap (\cup_{j=2}^n V_{i_j})$, $s_{i_1} \neq 0$ 与 $V_{i_1} \cap (\cup_{j=2}^n V_{i_j}) = \{0\}$ 矛盾, 故假设错误, $0 = 0 + \cdots + 0$ 是 0 的唯一分解式.

(3)$\Longrightarrow$(4): $\forall v \in V$, $v = u_1 + \cdots + u_n$, 其中 $u_i \in V_i$.
假设 $v = w_1 + \cdots + w_m$, 其中 $w_i \in V_i$.
$0 = v - v = u_1 + \cdots + u_n - w_1 - \cdots - w_n$, 将属于相同子空间的元素合并到一起, 得 $0 = (u_{t_1} - w_{t_1}) + \cdots + (u_{t_k} - w_{t_k}) + u_{t_{k+1}} + \cdots + u_{t_n} - w_{t_{k+1}} - w_{t_m}$, 由 (2) 知 $k = n = m$ 且 $v_{t_i} = u_{t_i}$, 故 v 具有唯一分解式 $v = v_1 + \cdots + v_n$.

(4)$\Longrightarrow$(2): 假设 $V_i \cap (\sum_{j\neq i} V_j) \neq \{0\}$, 则 $V_i \cap (\sum_{j\neq i} V_j) \supsetneq \{0\}$, 即 $\exists 0 \neq u \in V_i \cap (\cup_{j\neq i} V_j)$,
不妨设 $u \in V_1$ 且 $u \in V_2$, 则 $v = v_1 + \cdots + v_n = (v_1 + u) + (v_2 - u) + \cdots + v_n$, 其中 $v_i \in V_i$ 且 $v_1 + u \in V_1$,$v_2 - u \in V_2$, v 的分解式不唯一, 矛盾, 故假设错误, $V_i \cap (\sum_{j\neq i} V_j) = \{0\}$.

综上, 得证. □

定理 1.7 (课本定理1.8): $\mathcal{B} = \{v_1, \cdots, v_n\}$ 是向量空间 V 的基 $\Longleftrightarrow V = \langle v_1 \rangle \oplus \cdots \oplus \langle v_n \rangle$.

证: "$\Longrightarrow$": $\because \mathcal{B}$ 为 V 的基, $\therefore V = \langle \mathcal{B} \rangle = \langle v_1, \cdots, v_n \rangle = \{\sum_{i=1}^n r_i v_i \mid r_i \in F\} = \langle v_1 \rangle + \cdots + \langle v_n \rangle$.
$\because \mathcal{B}$ 为 V 的基, $\therefore v_1, \cdots, v_n$ 线性无关 $\Longrightarrow \forall 0 \neq u \in \langle v_i \rangle$, $u = r_i v_i$ 且无法由 $\{v_j \mid j \neq i\}$ 线性表示 $\Longrightarrow u \notin V_i \cap (\cup_{j\neq i} V_j)$,
$0 = 0v_i \in \langle v_i \rangle$ 且 $0 = \sum_{j\neq i} 0v_j \Longrightarrow 0 \in V_i \cap (\cup_{j\neq i} V_j)$
$\Longrightarrow V_i \cap (\cup_{j\neq i} V_j) = \{0\}$.
故 $V = \langle v_1 \rangle \oplus \cdots \oplus \langle v_n \rangle$.

"$\Longleftarrow$": 一方面, $V = \langle v_1 \rangle + \cdots + \langle v_n \rangle = \langle \mathcal{B} \rangle$;
另一方面, 假设 $\{v_1, \cdots, v_n\}$ 线性相关, 则 $\exists$ 不全为零的 $r_1, \cdots, r_n$, s.t. $\sum_i r_i v_i = 0$,
不妨设 $r_i \neq 0$, 则 $r_i v_i = -\sum_{j\neq i} r_j v_j \Longrightarrow 0 \neq r_i v_i \in V_i$ 且 $r_i v_i = -\sum_{j\neq i} r_j v_j \in \cup_{j\neq i} V_j \Longrightarrow r_i v_i \in V_0 \cap (\cup_{j\neq i} V_j) \Longrightarrow V_0 \cap (\cup_{j\neq i} V_j) \neq \{0\}$, 与直和的定义矛盾, 故假设错误, $v_1, \cdots, v_n$ 线性无关.
故 $\mathcal{B} = \{v_1, \cdots, v_n\}$ 是 V 的基. □

定理 1.8 (课本定理1.4): S 为 V 的子空间, 则 $\exists V$ 的子空间 S^c, s.t. $V = S \oplus S^c$, 称 S^c 为 S 的补空间.

证: $\mathcal{B}_1$ 为 S 的基, 则 $\mathcal{B}_1$ 为 V 中的线性无关集,
$\mathcal{B}_1$ 总可以扩张为 (即添加一些元素) 成 V 的基, 即 $\exists \mathcal{B}_2$, s.t. $\mathcal{B}_1 \cap \mathcal{B}_2 = \emptyset$, $\mathcal{B}_1 \cup \mathcal{B}_2$ 线性无关且 $V = \langle \mathcal{B}_1 \rangle + \langle \mathcal{B}_2 \rangle \Longrightarrow V = \langle \mathcal{B}_1 \rangle \oplus \langle \mathcal{B}_2 \rangle$, 故 $S^c = \langle \mathcal{B} \rangle$. □

例 1.9: $\mathbb{R}^2 = S_x \oplus S_y = S_l \oplus S_{l'}$, 其中 S_l 和 $S_{l'}$ 分别为过原点直线 l 和 l' 对应的子空间, l 与 l' 不共线. □

补空间总存在, 但不唯一.

定理 1.9 (课本定理1.13): (1) $\mathcal{B}$ 是 V 的基, 若 $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ 且 $\mathcal{B}_1 \cap \mathcal{B}_2 = \emptyset$, 则 $V = \langle \mathcal{B}_1 \rangle \oplus \langle \mathcal{B}_2 \rangle$.

(2) $V = S \oplus T$, 若 $\mathcal{B}_1$ 是 S 的基, $\mathcal{B}_2$ 是 T 的基, 则 $\mathcal{B}_1 \cap \mathcal{B}_2 = \emptyset$, $\mathcal{B}_1 \cup \mathcal{B}_2$ 是 V 的基.

证: (1) $\because \mathcal{B}$ 是 V 的基, $\therefore \forall u \in V$, $u = \sum_{i=1}^k r_i v_i$, 其中 $r_i \in F$, $v_i \in \mathcal{B}$, $k \in \mathbb{N}$.
$\langle \mathcal{B}_1 \rangle = \{\sum_{i=1}^n r_i v_i \mid r_i \in F, v_i \in \mathcal{B}_1, n \in \mathbb{N}\}$, $\langle \mathcal{B}_2 \rangle = \{\sum_{i=1}^n r_i v_i \mid r_i \in F, v_i \in \mathcal{B}_2, n \in \mathbb{N}\}$.
$u = \sum_{i=1}^t r_i v_i + \sum_{i=t+1}^k r_i v_i$, 其中 $v_1, \cdots, v_t \in \mathcal{B}_1$, $v_{t+1}, \cdots, v_k \in \mathcal{B}_2 \Longrightarrow V = \langle \mathcal{B}_1 \rangle + \langle \mathcal{B}_2 \rangle$.
$\forall u \in \langle \mathcal{B}_1 \rangle \cap \langle \mathcal{B}_2 \rangle$,$u \in \langle \mathcal{B}_1 \rangle \Longrightarrow u = \sum_{i=1}^n r_i v_i$, 其中 $r_i \in F$, $v_i \in \mathcal{B}_1$,
且 $u \in \langle \mathcal{B}_2 \rangle \Longrightarrow u = \sum_{i=1}^n l_i w_i$, 其中 $l_i \in F$, $w_i \in \mathcal{B}_2$
$\Longrightarrow 0 = u - u = \sum r_i v_i - \sum l_i w_i$,
又 $\because \mathcal{B}$ 为基, $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ 且 $\mathcal{B}_1 \cap \mathcal{B}_2 = \emptyset$, $\therefore r_i, w_i$ 线性无关 $\Longrightarrow r_i = l_i = 0$, $\forall i$
$\Longrightarrow u = 0$.
综上, $V = \langle \mathcal{B}_1 \rangle \oplus \langle \mathcal{B}_2 \rangle$.

(2) $V = S \oplus T \Longleftrightarrow V = S + T$ 且 $S \cap T = \{0\}$.
假设 $v \in \mathcal{B}_1 \cap \mathcal{B}_2$, 则 $v \neq 0$, $\langle v \rangle = S \cap T$, 与 $S \cap T = \{0\}$ 矛盾, 故假设错误, $\mathcal{B}_1 \cap \mathcal{B}_2 = \emptyset$.
$\because V = S + T$, $\therefore \forall u \in V$, $u = u_1 + u_2$, 其中 $u_1 \in S$, $u_2 \in T$,
$\because \mathcal{B}_1$ 是 S 的基, $\mathcal{B}_2$ 是 T 的基, $\therefore u_1 = \sum_{i=1}^k r_i v_i$, $u_2 = \sum_{i=k+1}^n$, 其中 $r_i \in F$, 对 $i = 1, \cdots, k$, $v_i \in \mathcal{B}_1$, 对 $i = k+1, \cdots, n$, $v_i \in \mathcal{B}_2$
$\Longrightarrow u = \sum_{i=1}^m r_i v_i$, 其中 $r_i \in F$, $v_i \in \mathcal{B}_1 \cap \mathcal{B}_2$, 即 $V = \langle \mathcal{B}_1 \cup \mathcal{B}_2 \rangle$.
假设 $\mathcal{B}_1 \cup \mathcal{B}_2$ 线性相关, 则 $\exists r_i \in F$ 不全为零, $\sum_{i=1}^n r_i v_i = \sum_{i=1}^k r_i v_i + \sum_{i=k+1}^n r_i v_i = 0$, 其中 $r_i \in F$, 对 $i = 1, \cdots, k$, $v_i \in \mathcal{B}_1$, 对 $i = k+1, \cdots, n$, $v_i \in \mathcal{B}_2$,
$\because \mathcal{B}_1$ 和 $\mathcal{B}_2$ 为基, $\therefore \mathcal{B}_1$ 和 $\mathcal{B}_2$ 线性无关 $\Longrightarrow \sum_{i=1}^k r_i v_i \neq 0$, $\sum_{i=k+1}^n r_i v_i \neq 0$, 与 $0 = 0 + \cdots + 0$ 是 0 的唯一分解式矛盾, 故假设错误, $\mathcal{B}_1 \cup \mathcal{B}_2$ 线性无关 $\Longrightarrow \mathcal{B}_1 \cup \mathcal{B}_2$ 是 V 的基.

□

定理 1.10 (课本定理1.14): S, T 是 V 的子空间, $\dim S + \dim T = \dim(S \cap T) + \dim(S + T)$. 特别地, 若 T 是 S 的补空间, 则 $\dim S + \dim T = \dim(S \oplus T)$.

证: 设 $S \cap T$ 的基为 $\mathcal{A}$,
$\because S \cap T$ 为 S 的子空间, $\therefore$ 可将 $\mathcal{A}$ 扩张成 S 的基 $\mathcal{A} \cup \mathcal{B}$,
$\because S \cap T$ 为 T 的子空间, $\therefore$ 可将 $\mathcal{A}$ 扩张成 T 的基 $\mathcal{A} \cup \mathcal{C}$.

接下来需要用到这样一个事实: $\mathcal{A} \cup \mathcal{B} \cup \mathcal{C}$ 是 $S + T$ 的基. 所以先来证明它:

证: $\forall w \in S+T$, $w=u+v$, 其中 $u\in S$, $v\in T \Longrightarrow u\in\langle\mathcal{A}\cup\mathcal{B}\rangle$, $v\in\langle\mathcal{A}+\mathcal{C}\rangle$, 故 $\langle\mathcal{A}\cup\mathcal{B}\cup\mathcal{C}\rangle=S+T$.

不妨设 $\sum_{i=1}^{n} r_i v_i=0$, 其中 $v_i\in\mathcal{A}\cup\mathcal{B}\cup\mathcal{C}$.

设 $v_1,\cdots,v_k\in\mathcal{A}$, 则 $\sum_{i=1}^{k} r_i v_i+\sum_{i=k+1}^{n} r_i v_i=0$,

令 $x=\sum_{i=1}^{k} r_i v_i$, 则 $x=\sum_{i=1}^{k} r_i v_i\in\langle\mathcal{A}\rangle$ 且 $x=-\sum_{i=k+1}^{n} r_i v_i\in\langle\mathcal{B}\cup\mathcal{C}\rangle\Longrightarrow x\in\langle\mathcal{A}\rangle\cap\langle\mathcal{B}\cup\mathcal{C}\rangle=(S-T)\cap T=\emptyset$.

$\because x\in\langle\mathcal{B}\rangle$, $\therefore x\in\mathcal{S}$, 又 $\because x\in\langle\mathcal{B}\cup\mathcal{C}\rangle$, $\therefore x\in T\Longrightarrow x\in S\cap T=\langle\mathcal{B}\rangle$. $\Longrightarrow x\in\langle\mathcal{A}\rangle\cap\langle\mathcal{B}\rangle\Longrightarrow x=0$.

又 $\because\mathcal{A}$ 和 $\mathcal{B}\cup\mathcal{C}$ 线性独立, 故 $\forall i$, $r_i=0\Longrightarrow\mathcal{A}\cup\mathcal{B}\cup\mathcal{C}$ 线性无关.

综上, $\mathcal{A}\cup\mathcal{B}\cup\mathcal{C}$ 是 $S+T$ 的基. □

故

$$\dim S+\dim T=|\mathcal{A}\cup\mathcal{B}|+|\mathcal{B}\cup\mathcal{C}|=|\mathcal{A}|+|\mathcal{B}|+|\mathcal{B}|+|\mathcal{C}|=|\mathcal{A}|+|\mathcal{B}|+|\mathcal{C}|+\dim(S\cap T)=\dim(S+T)+\dim(S\cap T).$$

□

Chapter 2

线性变换

2.1 线性变换

定义 2.1 **线性变换:** 向量空间之间的映射. F 为域, V, W 为 F 上的向量空间, 映射 $\tau : V \to W$, 若 $\tau(ru+tv) = r\tau(u) + t\tau(v)$, $r, t \in F$, $u, v \in V$, 则称 τ 为 V 到 W 的**线性变换**.

(类似于同态)

取 $r = 1$, $t = 1$, 则 $\tau(u + v) = \tau(u) + \tau(v)$, 故 τ 是 V 到 W 的群同态, 从而 $\tau(0) = 0$, $\tau(-v) = -\tau(v)$.

$\mathcal{L}(V, W) \equiv \{V$ 到 W 的线性变换$\}$, $\mathcal{L}(V) = \mathcal{L}(V, V) = \{V$ 到 V 的线性变换$\} = \{V$ 上的线性算子$\}$.

定义 2.2 **单线性变换:** 单射的线性变换.

定义 2.3 **满线性变换:** 满射的线性变换.

定义 2.4 **同构:** 双射的线性变换. 若两个向量空间 V, W 之间存在同构, 也称这两个向量空间同构, 记作 $V \approx W$.

取 $\tau, \sigma \in \mathcal{L}(V, W)$, $v \overset{\tau}{\mapsto} \tau(v)$, $v \overset{\sigma}{\mapsto} \sigma(v) \Longrightarrow v \overset{\tau+\sigma}{\mapsto} \tau(v) + \sigma(v)$ 也是线性变换, 且 $\tau + \sigma \in \mathcal{L}(V, W)$.

证: 由映射的像的唯一性, 若 $v = u$, 则 $\tau(v) = \tau(u)$, $\sigma(v) = \sigma(u) \Longrightarrow (\tau + \sigma)(v) = \tau(v) + \sigma(v) = \tau(u) + \sigma(u) + (\tau + \sigma)(u)$, 故 $\tau + \sigma$ 是映射.

$(\tau + \sigma)(ru + tv) = \tau(ru + tv) + \sigma(ru + tv) = r\tau(u) + t\tau(v) + r\sigma(u) + t\sigma(v) = r[\tau(u) + \sigma(u)] + t[\tau(v) + \sigma(v)] = r[(\tau + \sigma)(u)] + t[(\tau + \sigma)(v)]$, 故 $\tau + \sigma$ 为 V 到 W 的线性变换. □

由此定义了线性变换之间的加法.

$(\mathcal{L}(V, W), +)$ 为交换群.

证: $(\mathcal{L}(V, W), +)$ 满足

(1) **结合律**: $\forall v \in V$, $[(\tau + \sigma) + \delta](v) = (\tau + \sigma)(v) + \delta(v) = \tau(v) + \sigma(v) + \delta(v) = \tau(v) + (\sigma(v) + \delta(v)) = \tau(v) + (\sigma + \delta)(v) = [\tau + (\sigma + \delta)](v) \Longrightarrow [(\tau + \sigma) + \delta] = [\tau + (\sigma + \delta)]$.

(2) **有单位元** 0: 零映射 $0(v) = 0$, $\forall \tau \in \mathcal{L}(V, W)$, $(0 + \tau)(v) = 0(v) + \tau(v) = 0 + \tau(v) = \tau(v) + 0 = \tau(v) + 0(v) = (\tau + 0)(v)$.

(3) **有逆元**: $\forall \tau \in \mathcal{L}(V, W)$, $\exists -\tau$, s.t. $(-\tau)(v) = -\tau(v) \Longrightarrow [\tau + (-\tau)](v) = \tau(v) - \tau(v) = 0 = 0(v)$.

(4) **交换律**: $\forall v \in V$, $(\tau + \sigma)(v) = \tau(v) + \sigma(v) = \sigma(v) + \tau(v) = [\sigma + \tau](v)$.

故 $\mathcal{L}(V, W)$ 为交换群. □

$\forall r \in F$, $v \in \mathcal{L}(V, W)$, $v \overset{\tau}{\mapsto} \tau(v) \Longrightarrow v \overset{r\tau}{\mapsto} r\tau(v)$ 是线性变换, 且 $r\tau \in \mathcal{L}(V, W)$.

证: 由映射的像的唯一性, $\because v \overset{\tau}{\mapsto} \tau(v)$ 是唯一的, $\therefore v \overset{r\tau}{\mapsto} r\tau(v)$ 是唯一的, 故 $r\tau$ 是映射.
$(r\tau)(v) = r\tau(v) = r[\tau(v)]$, 故 $r\tau$ 为 V 到 W 的线性变换. □

$\mathcal{L}(V, W)$ 是 F 上的向量空间.

证: 前面已证, $(\mathcal{L}(V, W), +)$ 为交换群, 且其满足

(1) $\forall v \in V$, $[(r+t)\tau](v) = (r+t)\tau(v) = r\tau(v) + t\tau(v) = (r\tau + t\tau)(v) \Longrightarrow (r+t)\tau = r\tau + t\tau$

(2) $\forall v \in V$, $[(rt)\tau](v) = (rt)\tau(v) = r[t\tau(v)] = [r(t\tau)](v) \Longrightarrow (rt)\tau = r(t\tau)$

(3) $\forall v \in V$, $[r(\tau + \sigma)](v) = r(\tau + \sigma)(v) = r[\tau(v) + \sigma(v)] = r\tau(v) + r\sigma(v) = (r\tau + r\sigma)(v) \Longrightarrow r(\tau + \sigma) = r\tau + r\sigma$

(4) 恒等映射 $1 : \mathcal{L}(V, W) \to \mathcal{L}(V, W)$, $\tau \overset{1}{\mapsto}$, $\forall v \in V$, $(1\tau)(v) = 1[\tau(v)] = \tau(v) \Longrightarrow 1\tau = \tau$

故得证. □

定理 2.1 (课本定理2.1): (1) $\mathcal{L}(V, W)$ 是 F 上的向量空间.

(2) $\tau \in \mathcal{L}(V, W)$, $\sigma \in \mathcal{L}(W, U)$, 则 $\sigma \circ \tau \in \mathcal{L}(V, U)$.

(3) τ 是 V 到 W 的同构, 则 $\tau^{-1} \in \mathcal{L}(W, V)$.

(4) $\mathcal{L}(V)$ 既是向量空间, 也是环, 且两者的加法运算是相同的, 故 $\mathcal{L}(V)$ 是**代数**.

$\mathcal{L}(V)$ 是环.

证: 前面已证, $(\mathcal{L}(V), +)$ 为交换群, 且满足

(1) **结合律**: $\because$ 映射的复合有结合律, $\therefore \mathcal{L}(V)$ 中元素的复合有结合律

(2) **左右分配律**: $\forall v \in V$, $[(\sigma+\tau)\delta](v) = (\sigma+\tau)[\delta(v)] = \sigma[\delta(v)]+\tau[\delta(v)] = (\sigma\delta)(v)+(\tau\delta)(v) \Longrightarrow (\sigma+\tau)\delta = \sigma\delta+\tau\delta$
$[\sigma(\tau + \delta)](v) = \sigma[(\tau + \delta)(v)] = \sigma[\tau(v) + \delta(v)] = \sigma[\tau(v)] + \sigma[\delta(v)] = \sigma\tau(v) + \sigma\delta(v) \Longrightarrow \sigma(\tau + \delta) = \sigma\tau + \sigma\delta$

故得证. □

定义 2.5 核空间: $\ker \tau \equiv \{v \mid \tau(v) = 0\} \subseteq V$.

定义 2.6 像空间: $\operatorname{Im} \tau \equiv \{\tau(v) \mid v \in V\}$.

定理 2.2 (课本定理2.3): (1) τ 满线性变换 $\iff \operatorname{Im}\tau = W$.

(2) τ 单线性变换 $\iff \ker\tau = \{0\}$.

定理 2.3 (课本定理2.2): $\mathcal{B}$ 是 V 的基, $\tau \in \mathcal{L}(V, W)$, 则 τ 可由 τ 在 $\mathcal{B}$ 上的像唯一确定.

证: 若已知 $\tau(b_i)\forall b_i \in \mathcal{B}$, 则 $\forall v \in V$, $v = \sum_{i=1}^n r_i b_i$, $r_i \in F$, $b_i \in \mathcal{B}$, $n \in \mathbb{Z}^+$
$\implies \tau(v) = \tau\left(\sum_{i=1}^n r_i b_i\right) = \sum_{i=1}^n r_i \tau(b_i)$. □

同构的向量空间有很多性质可以相互传递, 下面我们就来讨论这件事.

定理 2.4 (课本定理2.4): $\tau \in \mathcal{L}(V, W)$ 同构, S 是 V 真子集, 则

(1) $V = \langle S\rangle \iff W = \langle \tau(S)\rangle$.

(2) S 线性无关 $\iff \tau(S)$ 线性无关.

(3) S 是 V 的基 $\iff \tau(S)$ 是 V 的基.

证: (1) "$\implies$": $\because V = \langle S\rangle$, $\therefore \forall v \in V$, $v = \sum_i r_i s_i$,
又 $\because \tau$ 同构, $\therefore \forall w \in W$, $\exists v \in V$, s.t. $w = \tau(v) \implies \tau(v) = \tau\left(\sum_i r_i s_i\right) = \sum_i r_i \tau(s_i)$.
"$\impliedby$": $\because W = \langle \tau(S)\rangle$, $\therefore \forall w \in W$, $w = \sum_i r_i \tau(s_i)$,
又 $\because \tau$ 同构, $\therefore \forall v \in W$, $\exists w \in W$, s.t. $v = \tau^{-1}(w) = \tau^{-1}\left(\sum_i r_i \tau(s_i)\right) = \sum_i r_i \tau^{-1}(\tau(s_i)) = \sum_i r_i \tau(s_i)$.
综上, (1) 得证.

(2) "$\implies$": 假设 $\sum_i r_i \tau(s_i) = 0$, 则 $\tau\left(\sum_i r_i s_i\right) = 0$,
又 $\because \tau$ 同构, $\therefore \ker\tau = \{0\} \implies \sum_i r_i s_i = 0$,
又 $\because S$ 线性无关, $\therefore r_i = 0\forall i \implies \tau(S)$ 线性无关.
"$\impliedby$": 假设 $\sum_i r_i s_i = 0$, 则 $\tau\left(\sum_i r_i s_i\right) = \sum_i r_i \tau(s_i) = 0$,
又 $\because \tau(S)$ 线性无关, $\therefore r_i = 0\forall i \implies S$ 线性无关.
综上, (2) 得证.

(3) (1), (2) $\implies$ (3).

□

定理 2.5 (课本定理2.6): $V \approx W \iff \dim V = \dim W$.

定理 2.6 (课本定理2.7): 若 $\dim V = n$, 则 $V \approx F^n$.

定理 2.7 (课本定理2.8): $\tau \in (L)(V, W)$,

(1) $(\ker\tau)^c \approx \operatorname{Im}\tau$.

(2) $\dim V = \dim\ker\tau + \dim\operatorname{Im}\tau \equiv \operatorname{null}\tau + \operatorname{rk}\tau$, 其中称 $\operatorname{null}\tau \equiv \dim\ker\tau$ 为 τ 的**零度**, $\operatorname{rk}\tau \equiv \dim\operatorname{Im}\tau$ 为 τ 的**秩**.

证: (1) 设映射 $\tau^c : \ker(\tau)^c \to \operatorname{Im}\tau$, $u \mapsto \tau(u)$.

先证 τ^c 是单射: $\ker(\tau^c) = \ker(\tau) \cap \ker(\tau)^c$ (即 $\ker(\tau^c)$ 中的元素同时满足 $\ker(\tau)$ 的条件, 且在定义域 $\ker(\tau)^c$ 中),

又 $\because V = \ker(\tau) \oplus \ker(\tau)^c$, $\therefore \ker(\tau) \cap \ker(\tau)^c = \{0\} \Longrightarrow \ker(\tau^c) = \{0\}$, 故 τ^c 单射.

再证 τ^c 是满射: 一方面, $\operatorname{Im}(\tau^c) \subseteq \operatorname{Im}(\tau)$;

另一方面, $\forall \tau(v)$, $v = u + w$, 其中 $u \in \ker(\tau)$, $w \in \ker(\tau)^c \Longrightarrow \tau(v) = \tau(u+w) = \tau(u) + \tau(w) = 0 + \tau(w) = \tau(w) \in \operatorname{Im}(\tau^c) \Longrightarrow \operatorname{Im}(\tau) \subseteq \operatorname{Im}(\tau^c)$.

故 $\operatorname{Im}(\tau^c) = \operatorname{Im}(\tau)$, 即 τ^c 满射.

综上, (1) 得证.

(2) $\dim V = \dim\ker(\tau) + \dim\ker(\tau)^c = \dim\ker(\tau) + \dim\operatorname{Im}(\tau)$.

□

x 为 n 维向量, $\dim\{x \mid Ax = 0\} = n - \operatorname{rk} A$, 故 $\dim\{x \mid Ax = 0\} = \operatorname{null} A$.

2.2 表示

"表示"其实就是用已知的东西展现未知的东西, 在这里, 我们用已知的矩阵乘法展现未知的线性变换, 这就是线性变换的表示.

F 为域, $F^n = \{(r_1, \cdots, r_n) \mid r_i \in F\}$, 满足 $(r_1, \cdots, r_n) + (l_1, \cdots, l_n) = (r_1 + l_1, \cdots, r_n + l_n)$ 及 $r(r_1, \cdots, r_n) = (rr_1, \cdots, rr_n)$, $\dim F^n = n$, F^n 的标准基为 $\{e_1 = (1, 0, \cdots, 0), e_2 = (0, 1, \cdots, 0), \cdots, e_n = (0, 0, \cdots, 1)\}$; $F^m = \{(r_1, \cdots, r_m) \mid r_i \in F\}$, $\dim F = m$, 标准基为 $\{f_1 = (1, 0, \cdots, 0), f_2 = (0, 1, \cdots, 0), \cdots, f_m = (0, 0, \cdots, 1)\}$. 如何确定/展现 F^n 到 F^m 的线性变换?

根据定理 2.3, 我们只需确定一组基在线性变换下的表现, 就可以确定这一线性变换. 因此, $\forall \tau \in \mathcal{L}(F^n, F^m)$, 若 $\tau(e_i) = (a_{1i}, \cdots, a_{mi}) = \sum_{j=1}^m a_{ji} f_j$.
$\forall (r_1, \cdots, r_n) \in F^n$,

$$\begin{aligned}
\tau((r_1, \cdots, r_n)) =& \tau\left(\sum_{i=1}^n r_i e_i\right) = \sum_{i=1}^n r_i \tau(e_i) = \sum_{i=1}^n r_i \left(\sum_{j=1}^m a_{ji} f_j\right) = \sum_{j=1}^m \left(\sum_{i=1}^n r_i a_{ji}\right) f_j = \left(\sum_{i=1}^n r_i a_{1i}, \cdots, \sum_{i=1}^n r_i a_{mi}\right) \\
=& \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix} = \begin{pmatrix} \tau(e_1) & \tau(e_2) & \cdots & \tau(e_n) \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix} = M_\tau \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix},
\end{aligned}$$

其中 $M_\tau = \begin{pmatrix} \tau(e_1) & \tau(e_2) & \cdots & \tau(e_n) \end{pmatrix}$.
故 $\forall \vec{r} \in F^n$, $\tau(\vec{r}) = M_\tau \vec{r}$.

综上:

$$\boxed{\mathcal{L}(F^n, F^m) \approx M_{m\times n}(F), \quad \tau \mapsto M_\tau = \begin{pmatrix} \tau(e_1) & \cdots & \tau(e_2) \end{pmatrix}}.$$

$f : \mathcal{L}(F^n, F^m) \to M_{m\times n}(F)$, $\tau \mapsto M_\tau$ 是线性变换.

证: 由上述的 M_τ 构造过程知, $f(\tau) = M_\tau$ 是唯一的, 故 f 是映射.

$$
\begin{aligned}
f(r\tau + t\sigma) =& M_{r\tau+t\sigma} = \begin{pmatrix}(r\tau + t\sigma)(e_1) & \cdots & (r\tau + t\sigma)(e_n)\end{pmatrix} = \begin{pmatrix}r\tau(e_1) + t\sigma(e_1) & \cdots & r\tau(e_n) + t\sigma(e_n)\end{pmatrix} \\
=& r\begin{pmatrix}\tau(e_1) & \cdots & \tau(e_n)\end{pmatrix} + t\begin{pmatrix}\sigma(e_1) & \cdots & \sigma(e_n)\end{pmatrix} = rM_\tau + tM_\sigma = rf(\tau) + tf(\sigma).
\end{aligned}
$$

故 f 是线性的.

综上, $f : \mathcal{L}(F^n) \to M_{m\times n}(F)$, $\tau \mapsto M_\tau$ 是线性变换. □

f 单射.

证: $\ker f \equiv \{\tau \mid f(\tau) = 0\} = \{\tau \mid M_\tau = 0\}$.
$\forall \tau \in \ker f$, $\forall \vec{r} \in F^n$, $\tau(\vec{r}) = M_\tau \vec{r} = \vec{0} \Longrightarrow M_\tau = 0_{m\times n} \Longrightarrow \tau = 0$.
故 $\ker f = \{0\}$ (这里的"0"代表的是零变换) $\Longleftrightarrow$ f 单射. □

f 满射.

证: $\forall A \in M_{m\times n}(F)$, 可由 $\begin{pmatrix}\tau(e_1) & \cdots & \tau(e_n)\end{pmatrix} = M_\tau = A$ 构造 τ, 从而 f 满射. □

综上, f 同构.

取 V 的基 $\mathcal{B} = \{b_1, \cdots, b_n\}$, $\forall v \in V$, $v = \sum_i r_i b_i$.

当 $\mathcal{B}$ 定序, $\phi_\mathcal{B} : V \to F^n$, $v \mapsto \begin{pmatrix}r_1 \\ \vdots \\ r_n\end{pmatrix} \equiv [v]_\mathcal{B}$ 是一个映射.

证: 由于 $\mathcal{B}$ 是 V 的基, 展开式 $v = \sum_i r_i b_i$ 唯一确定, 又 $\because \mathcal{B}$ 定序, 从而映射 $v \mapsto \begin{pmatrix}r_1 \\ \vdots \\ r_n\end{pmatrix}$ 唯一确定, 故 $\phi_\mathcal{B}$ 为映射.

$\forall u, v \in V$, $u = \sum_{i=1}^n w_i b_i$, $v = \sum_{i=1}^n r_i b_i$,

$$
\begin{aligned}
\phi_\mathcal{B}(r\vec{u} + t\vec{v}) =& \phi_\mathcal{B}\left(r\left(\sum_{i=1}^n w_i b_i\right) + t\left(\sum_{i=1}^n r_i b_i\right)\right) = \phi_\mathcal{B}\left(\sum_{i=1}^n (rw_i + tr_i) b_i\right) = \begin{pmatrix}rw_1 + tr_1 \\ \vdots \\ rw_n + tr_n\end{pmatrix} \\
=& r\begin{pmatrix}w_1 \\ \vdots \\ w_n\end{pmatrix} + t\begin{pmatrix}r_1 \\ \vdots \\ r_n\end{pmatrix} = r\phi_\mathcal{B}(u) + t\phi_\mathcal{B}(v),
\end{aligned}
$$

故 ϕ_B 为 V 到 F^n 的线性变换. □

$\phi_\mathcal{B}$ 单射.

证: $\ker \phi_\mathcal{B} = \{v \mid \phi_\mathcal{B}(v) = \begin{pmatrix}0 \\ \vdots \\ 0\end{pmatrix}\}$.

$\phi_\mathcal{B}(v) = \begin{pmatrix}0 \\ \vdots \\ 0\end{pmatrix} \Longrightarrow v = \sum_{i=1}^n 0 b_i = 0$.

故 $\ker \phi_\mathcal{B} = \{0\} \Longleftrightarrow \phi_\mathcal{B}$ 单射. □

$\phi_{\mathcal{B}}$ 满射.

证: $\forall \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} \in F^n$, $\exists v \in V$, s.t. $\sum_{i=1}^{n} r_i b_i \in V$, 故 $\phi_{\mathcal{B}}$ 满射. $\square$

综上, $\phi_{\mathcal{B}}$ 同构.

取 V 的一组定序基 $\mathcal{B} = \{b_1, \cdots, b_n\}$, 另一组定序基 $\mathcal{C} = \{c_1, \cdots, c_n\}$, v 在 $\mathcal{B}$ 下的表象为 $[v]_{\mathcal{B}}$, 在 $\mathcal{C}$ 下的表象为 $[v]_{\mathcal{C}}$, 映射关系见如下的交换图. 如何联系 v 在不同基下的表象, $[v]_{\mathcal{B}}$ 和 $[v]_{\mathcal{C}}$, 从而得到 τ?

$$
\begin{tikzcd}
 & & v \arrow[dddll, mapsto] \arrow[dddrr, mapsto] & & \\
 & & V \arrow[dl, "\phi_{\mathcal{B}}"'] \arrow[dr, "\phi_{\mathcal{C}}"] & & \\
 & F^n \arrow[rr, "\tau = \phi_{\mathcal{C}} \circ \phi_{\mathcal{B}}^{-1}"] & & F^n & \\
 {[v]_{\mathcal{B}}} \arrow[rrrr, mapsto] & & & & {[v]_{\mathcal{C}}}
\end{tikzcd}
$$

$[v]_{\mathcal{C}} = \tau([v]_{\mathcal{B}}) = M_\tau [v]_{\mathcal{B}}$, 其中 $M_\tau = \begin{pmatrix} \tau(e_1) & \cdots & \tau(e_n) \end{pmatrix}$.
$\tau : F^n \to F^n, \quad e_i \mapsto \tau(e_i) = \phi_{\mathcal{C}}(\phi_{\mathcal{B}}^{-1}(e_i)) = \phi_{\mathcal{C}}(b_i)$,
$M_\tau = \begin{pmatrix} [b_1]_{\mathcal{C}} & \cdots & [b_n]_{\mathcal{C}} \end{pmatrix} \equiv M_{\mathcal{BC}}$.

定理 2.8 (课本定理2.12):

$$\boxed{[v]_{\mathcal{C}} = M_{\mathcal{BC}} [v]_{\mathcal{B}}}$$

其中 $[v]_{\mathcal{B}}$ 和 $[v]_{\mathcal{C}}$ 分别是向量 v 在基 $\mathcal{B}$ 和 $\mathcal{C}$ 表象下的坐标表示, $M_{\mathcal{BC}}$ 是在两种坐标表示之间线性变换对应的矩阵.

$$\begin{tikzcd}
b_i \arrow[rrrrr, mapsto] \arrow[ddddd, mapsto] & & & & & \tau(b_i) \arrow[ddddd, mapsto] \\
& v \arrow[rrr, mapsto] \arrow[ddd, mapsto] & & & \tau(v) \arrow[ddd, mapsto] & \\
& & V \arrow[r, "\tau"] \arrow[d, "\phi_{\mathcal{B}}"] & W \arrow[d, "\phi_{\mathcal{C}}"] & & \\
& & F^n \arrow[r, "\tau_A = \phi_{\mathcal{C}} \circ \tau \circ \phi_{\mathcal{B}}^{-1}"] & F^n & & \\
& {[v]_{\mathcal{B}}} \arrow[rrr, mapsto] & & & \tau([v]_{\mathcal{B}}) = [v]_{\mathcal{C}} & \\
e_i \arrow[rrrrr, mapsto] & & & & & \tau_A(e_i) = [\tau(b_i)]_{\mathcal{C}}
\end{tikzcd}$$

$$\begin{aligned}
M_{\tau_A} &= \begin{pmatrix} \tau_A(e_1) & \cdots & \tau(e_n) \end{pmatrix} = \begin{pmatrix} \phi_{\mathcal{C}} \circ \tau \circ \phi_{\mathcal{B}}^{-1}(e_1) & \cdots & \phi_{\mathcal{C}} \circ \tau \circ \phi_{\mathcal{B}}^{-1}(e_n) \end{pmatrix} = \begin{pmatrix} \phi_{\mathcal{C}} \circ \tau(b_1) & \cdots & \phi_{\mathcal{C}} \circ \tau(b_n) \end{pmatrix} \\
&= \begin{pmatrix} [\tau(b_1)]_{\mathcal{C}} & \cdots & [\tau(b_n)]_{\mathcal{C}} \end{pmatrix} \equiv [\tau]_{\mathcal{B}\mathcal{C}}.
\end{aligned}$$

定理 2.9 (课本定理2.14):

$$\boxed{[\tau(v)]_{\mathcal{C}} = [\tau]_{\mathcal{B}\mathcal{C}}[v]_{\mathcal{B}}}$$

其中 $[\tau(v)]_{\mathcal{C}}$ 是 $\tau(v)$ 在基 $\mathcal{C}$ 的表象下的坐标表示, $[\tau]_{\mathcal{B}\mathcal{C}}$ 是从基 $\mathcal{B}$ 的表象到基 $\mathcal{C}$ 的表象的线性变换的矩阵表示, $[v]_{\mathcal{B}}$ 是 v 在基 $\mathcal{B}$ 的表象下的坐标表示.

定理 2.10 (课本定理2.15): $\mathcal{L}(V, W) \to \mathcal{L}(F^n, F^m) \approx M_{m\times n}(F)$, $\tau \mapsto \tau_A \mapsto [\tau]_{\mathcal{B}\mathcal{C}}$.

若我们改变 V 和 W 的基, 那么映射所联系的向量的坐标会如何?

$$\begin{tikzcd}
F^n \arrow[r, "\tau'_A"] & F^n \\
V \arrow[u, "\phi'_{\mathcal{B}}"] \arrow[r, "\tau"] \arrow[d, "\phi_{\mathcal{B}}"] & W \arrow[u, "\phi'_{\mathcal{C}}"] \arrow[d, "\phi_{\mathcal{C}}"] \\
F^n \arrow[r, "\tau_A"] & F^n
\end{tikzcd}$$

$\tau'_A = \phi'_{\mathcal{C}} \phi_{\mathcal{C}}^{-1} \tau_A \phi_{\mathcal{B}} \phi'^{-1}_{\mathcal{B}}$.

定理 2.11 (课本定理2.16):

$$\boxed{[\tau]_{\mathcal{B}'\mathcal{C}'} = M_{\mathcal{C}\mathcal{C}'}[\tau]_{\mathcal{B}\mathcal{C}}M_{\mathcal{B}'\mathcal{B}}}$$

其中 $[\tau]_{\mathcal{B}\mathcal{C}}$ 和 $[\tau]_{\mathcal{B}'\mathcal{C}'}$ 分别是线性变换 τ 在基 $(\mathcal{B},\mathcal{C})$ 和 $(\mathcal{B}',\mathcal{C}')$ 下的表示, 矩阵 $M_{\mathcal{B}'\mathcal{B}}$ 和 $M_{\mathcal{C}\mathcal{C}'}$ 分别对应了从基 $\mathcal{B}$ 到基 $\mathcal{B}'$ 和从基 $\mathcal{C}$ 到基 $\mathcal{C}'$ 的变换矩阵.

$M_{\mathcal{B}\mathcal{B}'}$ 可逆.

证: 设 $\phi_{\mathcal{B}} : V \to F^n$, $v = \sum_{i=1}^n r_i b_i \mapsto [v]_{\mathcal{B}} = \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix}$, $\phi_{\mathcal{B}'} : V \to F^n$, $v = \sum_{i=1}^n r'_i b'_i \mapsto [v]_{\mathcal{B}'} \begin{pmatrix} r'_1 \\ \vdots \\ r'_n \end{pmatrix}$, 即

$$\begin{tikzcd}
 & & v \arrow[dddll, mapsto] \arrow[dddrr, mapsto] & & \\
 & & V \arrow[dl, "\phi_{\mathcal{B}}"'] \arrow[dr, "\phi_{\mathcal{B}'}"] & & \\
 & F^n \arrow[rr, "\tau"] & & F^n & \\
{[v]_{\mathcal{B}}} \arrow[rrrr, mapsto] & & & & {[v]_{\mathcal{B}'}}
\end{tikzcd}$$

$M_{\mathcal{B}\mathcal{B}'} = M_\tau = \begin{pmatrix} [b_1]_{\mathcal{B}'} & \cdots & [b_n]_{\mathcal{B}'} \end{pmatrix}$, s.t. $[v]_{\mathcal{B}'} = M_{\mathcal{B}\mathcal{B}'}[v]_{\mathcal{B}}$.

同理可以构造 $M_{\mathcal{B}\mathcal{B}'} = \begin{pmatrix} [b'_1]_{\mathcal{B}} & \cdots & [b'_n]_{\mathcal{B}} \end{pmatrix}$, s.t. $[v]_{\mathcal{B}} = M_{\mathcal{B}'\mathcal{B}}[v]_{\mathcal{B}'}$.

$\forall [v]_{\mathcal{B}} \in F^n$, $M_{\mathcal{B}\mathcal{B}'}M_{\mathcal{B}'\mathcal{B}}[v]_{\mathcal{B}} = M_{\mathcal{B}\mathcal{B}'}[v]_{\mathcal{B}'} = [v]_{\mathcal{B}} \Longrightarrow M_{\mathcal{B}\mathcal{B}'}M_{\mathcal{B}'\mathcal{B}} = n \times n$ 维的单位矩阵, 即 $M_{\mathcal{B}'\mathcal{B}}$ 是 $M_{\mathcal{B}\mathcal{B}'}$ 的逆, 故 $M_{\mathcal{B}\mathcal{B}'}$ 可逆. □

定理 2.12 (课本定理2.18): $B = PAQ$, 其中 P 和 Q 可逆, 则 B 与 A **等价**.

(因为 B 和 A 是同一线性变换在两组不同的基下的表示.)

定理 2.13 (课本定理2.19): $B = PAP^{-1}$, 其中 P 可逆, 则 B 与 A **相似**.

(因为 B 和 A 是同一线性算子在两组不同的基下的表示.)

Chapter 3

同构定理

定义 3.1 商空间: F 为域, V 是 F 上的向量空间, S 是 V 的子空间, 则称 $\frac{V}{S} \equiv \{[v] \mid v \in V\}$ 是 F 的**商空间**, 其中 $[v] \equiv \{u \in V \mid u - v \in S\} = S + v$.

$\frac{V}{S}$ 是 F 上的向量空间.

证: $[u] + [v] = \{a \in V \mid a - u \in S\} + \{b \in V \mid b - v \in S\} = \{(a+b) \in V \mid a - u \in S, b - v \in S\}$.
$[u + v] = \{w \in V \mid w - (u + v) \in S\}$.
$\forall a + b \in [u] + [v]$, $(a - u) + (b - v) = (a + b) - (u + v) \in S \Longrightarrow (a + b) \in [u + v] \Longrightarrow [u] + [v] \in [u + v]$.
$\forall w \in [u + v]$, $\exists c, d \in S$, s.t. $c + d = w - (u + v) \Longrightarrow w = (c + d) + (u + v) = (c + u) + (d + v)$, 其中 $(c + u) \in [u]$, $(d + v) \in [v] \Longrightarrow w \in [u] + [v]$.
故 $[u] + [v] = [u + v]$.

假设 $u \sim u'$, $v \sim v'$, 即 $[u] = [u']$, $[v] = [v']$.
$\because [u] = [u']$, $\therefore uS = u'S \Longrightarrow \exists s_1, s_1' \in S$, s.t. $u + s_1 = u' + s_1' \Longleftrightarrow v' = u + s_1 - s_1'$,
$\because [v] = [v']$, $\therefore vS = v'S \Longrightarrow \exists s_2, s_2' \in S$, s.t. $v + s_2 = v' + s_2' \Longleftrightarrow v' = v + s_2 - s_2'$,
从而 $u' + v' = u + s_1 - s_1' + v + s_1 - s_1'$, 其中 $\because s_1, s_1', s_1, s_1' \in S$, $s_1 - s_1' \in S$, $s_2 - s_2' \in S$,
$\because V$ 是交换群, $\therefore$, s.t. $s_1 - s_1' + v = v + s_1 - s_1' \Longrightarrow u' + v' = u + v + (s_1 - s_1' + s_2 - s_2')$
$\Longrightarrow (u' + v')S = (u + v + (s_1 - s_1' + s_2 - s_2'))S \Longrightarrow [u' + v'] = [u' + v'] = [u + v]$,
即 $[u] + [v] = [u + v]$ 与代表元选取无关, 故 $[u] + [v] = [u + v]$ 是运算.

$r[u] = r\{v \in V \mid v - u \in S\} = \{rv \mid v \in V, v - u \in S\} = \{rv \in V \mid rv - ru \in S\} = [ru]$.

假设 $u \sim u'$, 即 $[u] = [u']$.
$\because [u] = [u']$, $\therefore uS = u'S \Longrightarrow \exists s, s' \in S$, s.t. $u + s = u' + s' \Longleftrightarrow u' = u + s - s'$,
从而 $ru' = r(u+s-s') = ru+r(s-s')$, 其中 $s-s' \in S \Longrightarrow (ru')S = (ru+r(s-s'))S = (ru)S \Longrightarrow r[u'] = [ru'] = [ru]$,
即 $r[u] = [ru]$ 与代表元选取无关, 故 $r[u] = [ru]$ 是运算.

$(\frac{V}{S}, +)$ 满足

(1) **结合律**: $([v] + [u]) + [w] = [u + v] + [w] = [u + v + w] = [u + (v + w)] = [u] + [v + w] = [u] + ([v] + [w])$

(2) **有单位元** $[0]$: $[0] + [u] = [0 + u] = [u] = [u + 0] = [u] + [0]$

(3) **有逆元**: $\forall v \in V$, $\exists - v$, s.t. $[a] + [-a] = [a + (-a)] = [0] = [(-a) + a] = [-a] + [a]$

且 $[u] + [v] = [u + v] = [v + u] = [v] + [u]$, 即 $(\frac{V}{S}, +)$ 交换, 故 $(\frac{V}{S}, +)$ 是交换群. (总之就是因为 $\frac{V}{S}$ 中的元素 $[v]$ 保持了 V 中的元素 v 的各种运算性质, 所以 $(V, +)$ 是交换群就可以推出 $\frac{V}{S}$ 也是交换群.)

$\frac{V}{S}$ 满足

(1) $r([u+v]) = r([u]+[v]) = r[u]+r[v]$

(2) $(r+t)[u] = [(r+t)u] = [ru+tu] = [ru]+[tu] = r[u]+t[u]$

(3) $(r\cdot t)[u] = [(r\cdot t)u] = [r(tu)] = r[tu] = r(t[u])$

(4) **有单位元** 1: $[1][u] = [1u] = [u]$

故 $\frac{V}{S}$ 是 F 上的向量空间. □

定理 3.1 (课本定理3.2): (1) $\Pi_S : V \to \frac{V}{S}$, $v \mapsto [v]$ 是线性变换.

(2) Π_S 是满线性变换, 即 $\operatorname{Im}\Pi_S = \frac{V}{S}$.

(3) $\ker \Pi_S = S$.

证: (1) 显然 Π_S 是唯一的, 故 Π_S 是映射.
如前所证, V 和 $\frac{V}{S}$ 均为 F 上的向量空间.
$\because [u+v] = \{w \in V \mid w-(u+v) \in S\}$, $r[u] = [ru]$, $\therefore r[u]+t[v] = [ru]+[tv] = [ru+tv]$, 故 Π_S 为线性变换.

(2) $\forall [v] \in \frac{V}{S}$, $\exists v \in V$, s.t. $\Pi_S(v) = [v]$, 即 $\operatorname{Im}\Pi_S = \frac{V}{S}$, 故 Π_S 是满线性变换.

(3) $\ker\Pi_S = \{v \in S \mid \Pi_S(v) = [0]\}$.
$\Pi_S(v) = [v] = S+v = [0] = S \Longrightarrow v \in S \Longrightarrow \ker\Pi_S = S$.

□

定理 3.2 (课本定理3.3): (1) S, T 是子空间, 且 $S \subseteq T$, 则 $\frac{T}{S}$ 是 $\frac{V}{S}$ 的子空间.

(2) 取 X 为 $\frac{V}{S}$ 的子空间, 则 $\exists V$ 的子空间 T, s.t. $\emptyset \neq S \subseteq T$, $\frac{T}{S} = X$.

证: (1) $\frac{T}{S} = \{[u] \mid u \in T\}$, $\frac{V}{S} = \{[v] \mid v \in V\}$.
$\forall [u] \in \frac{T}{S}$, $u \in T$, $\because T$ 是 V 的子空间, $\therefore u \in V \Longrightarrow [u] \in \frac{V}{S}$, 故 $\frac{T}{S} \subseteq \frac{V}{S}$.
$\forall [u_1], [u_2] \in \frac{T}{S}$, $r, t \in F$, $r[u_1]+t[u_2] = [ru_1+tu_2]$, $\because u_1, u_2 \in T$, $\therefore ru_1+tu_2 \in T \Longrightarrow [ru_1+tu_2] \in \frac{T}{S}$, 故 $\frac{T}{S}$ 是线性空间.

综上, 得证.

(2) 取 $T = \cup_{[v]\in X}[v]$.
显然 $T \subseteq V$.
$\forall u, v \in T$, 根据 T 的定义, $[u], [v] \in X$,
$\because X$ 为子空间, $\therefore r[u]+t[v] = [ru+tv] \in X \Longrightarrow ru+tv \in [ru+tv] \subseteq T = \cup_{v\in X}[v] \Longrightarrow ru+tv \in T$.
故 T 为 V 的子空间.

$\because [0] = S$, $\therefore S \subseteq T$.

$\frac{T}{S} = \{[v] = S+v \mid v \in T\}$.
$\forall [v] \in \frac{T}{S}$, $v \in T \Longrightarrow [v] \in X$.
$\forall [v] \in X$, $v \in T \Longrightarrow [v] \in \frac{T}{S}$.
故 $\frac{T}{S} = X$.

综上, 得证.

□

定理 3.3 第一同态基本定理(课本定理3.4): [a] S 是 V 的子空间, $\tau \in \mathcal{L}(V, W)$,

$$\begin{tikzcd}
v \arrow[rrr, mapsto] \arrow[ddd, mapsto] & & & \tau[v] \\
& V \arrow[r, "\tau"] \arrow[d, "\Pi_S"'] & W & \\
& \frac{V}{S} \arrow[ur, dashed, "\tau'"'] & & \\
{[v]} \arrow[uuurrr, dashed, mapsto] & & &
\end{tikzcd}$$

若 $S \subseteq \ker \tau$, 即 $\ker \Pi_S \subseteq \ker \tau$, 则 $\exists! \tau'$, s.t. $\tau = \tau' \circ \Pi_S$, 即 $\forall v \in V$, $\tau(v) = \tau'([v])$, 此时上图可交换.

[a] 该定理回答了 τ' 的存在性 (即 τ' 在什么条件下存在) 的问题. 之所以称"基本", 是因为若将该定理中的向量空间换成其他代数结构, 定理仍然成立.

证: τ' 的唯一性要求, 若 $[u] = [v]$, 则 $\tau'([u]) = \tau'([v])$,
即若 $u \sim v$, 则 $\tau(u) = \tau(v)$,
即若 $u - v \in S$, 则 $\tau(u - v) = 0$,
即 $S \subseteq \ker \tau$. □

此时, $\ker \tau' = \{[v] \in \frac{V}{S} \mid \tau'([v]) = 0\} = \{[v] \in \frac{V}{S} \mid \tau(v) = 0\} = \{[v] \in \frac{V}{S} \mid v \in \ker \tau\} = \{[v] \mid v \in \ker \tau\} = \frac{\ker \tau}{S}$, $\operatorname{Im} \tau' = \{\tau'([v]) \mid [v] \in \frac{V}{S}\} = \{\tau'([v]) \mid v \in V\} = \{\tau(v) \mid v \in V\} = \operatorname{Im} \tau$ ($\because \Pi_S$ 满射, $\therefore \forall [v] \in \frac{V}{S}, \exists v \in V$).

那么, 如果 τ 双射, 即 $\exists \tau^{-1} \in \mathcal{L}(W, V)$, 再加上条件 $\ker \tau \subseteq S$, 即 $\ker \tau = S$, 如何?

$$\begin{tikzcd}
\tau^{-1}(w) \arrow[ddd, mapsto] & & & w \arrow[lll, mapsto] \\
& V \arrow[d, "\Pi_S"'] & W \arrow[l, "\tau^{-1}"'] & \\
& \frac{V}{S} & & \\
{[w]} & & &
\end{tikzcd}$$

此时, $\ker \tau' = \frac{\ker \tau}{S} = \{[v] \mid v \in \ker \tau\} = \{[v] \mid v \in S\} = \{[0]\} \Longrightarrow \tau'$ 单射.

由上面关于第一同态定理的延伸讨论我们得到:

定理 3.4 第一同构定理(课本定理3.5): 若 $\ker \tau = S$, 则 τ' 单射, $\frac{V}{\ker \tau} = \frac{V}{S} \approx \operatorname{Im} \tau$.

$$\begin{tikzcd}
v \arrow[rrr, mapsto] \arrow[ddd, mapsto] & & & \tau[v] \\
& V \arrow[r, "\tau"] \arrow[d, "\Pi_S"'] & W & \\
& \frac{V}{S} \arrow[ur, dashed, "\tau'"] & & \\
{[v]} \arrow[uuurrr, dashed, mapsto] & & &
\end{tikzcd}$$

证: $V = \ker\tau \oplus (\ker\tau)^c$, 其中 $(\ker\tau)^c \approx \operatorname{Im}\tau \Longrightarrow \frac{V}{\ker\tau} = (\ker\tau)^c$. □

更一般地, 若 $V = S \oplus T$, 则 $\frac{V}{S} = T$, $\frac{V}{T} \approx S$.

证: $\forall v \in V$, $v = u_S + u_T$, 其中 $u_S \in S$, $u_T \in T$. 令投影映射 $P_T : V \to T$, $v = u_S + u_T \mapsto u_T$.
$\ker P_T = \{v \in V \mid P_T(v) = 0\} = S = [0] = \ker\Pi_S$.
$\exists!\tau'$ 单射, s.t. $P_T = \tau' \circ \Pi_S$.
又 $\operatorname{Im} P_T = T$, 即 P_T 满射, $\therefore \tau'$ 满射 $\Longrightarrow \tau'$ 同构 $\Longrightarrow \frac{V}{S} \approx T$.

$$\begin{tikzcd}
v = u_S + u_T \arrow[rrr, mapsto] \arrow[ddd, mapsto] & & & u_T \\
& V \arrow[r, "P_T"] \arrow[d, "\Pi_S"'] & T & \\
& \frac{V}{S} \arrow[ur, dashed, "\tau'"] & & \\
{[v]} \arrow[uuurrr, dashed, mapsto] & & &
\end{tikzcd}$$

同理可证 $\frac{V}{T} \approx S$. □

定义 3.2 对偶(空间)和线性泛函: $V^* = \mathcal{L}(V, F)$ 是 F 上的向量空间, 称 V^* 为 V 的**对偶(空间)**. 若 $f \in V^*$, 称 f 为**线性泛函**.

(1) $\ker V^*$ 为 F 上的向量空间.

(2) $\dim F = 1$, $\operatorname{Im} f \subseteq F$, $\therefore \dim\operatorname{Im} f \leq 1$, $\dim\ker f \geq \dim V - 1$.

(3) V^* 非空, $\because$ 必有零映射 $0 \in V^*$, $0 : V \to F$, $v \mapsto 0$.

(4) 若 $\dim\operatorname{Im} f = 0$, 则 $\operatorname{Im} f = \{0\}$, f 为零映射.

(5) 若 $\dim\operatorname{Im} f = 1$, 则 $\operatorname{Im} f = \langle r\rangle$, 其中 $0 \neq r \in F \Longrightarrow \operatorname{Im} f = F$,
由反证法易证, 若 $v \in f^{-1}(r) = \{v \in V \mid f(v) = r\}$, 其中 $r \neq 0$, 则 $v \neq 0$, 且必有 $f(\langle v\rangle^c) = \{0\}$.

证明一下 (5) 的末句:

证: 假设 $\exists u \in \langle v\rangle^c$, s.t. $f(u) \neq 0$,
则有 $f\left(\frac{ru}{f(u)}\right) = r \Longrightarrow \frac{ru}{f(u)} \in f^{-1}(r) \Longrightarrow f^{-1} = \langle v\rangle \oplus \langle u\rangle$,
又 $\because u \in \langle v\rangle^c$, $\therefore \dim f^{-1} \geq 2$, 这与 $f^{-1} \subseteq (\ker f)^c$, $\dim(\ker f)^c = \dim \operatorname{Im} f \leq 1$ 矛盾,
故假设错误, $\forall u \in \langle v\rangle^c$, $f(u) = 0 \Longrightarrow f(\langle v\rangle^c) = \{0\}$. □

定理 3.5 (课本定理3.11): (1) 若 $0 \neq v \in V$, $\exists 0 \neq f \in V^*$, s.t. $f(v) \neq 0$.

(2) $v = 0 \Longleftrightarrow \forall f \in V^*$, $f(v) = 0$.

(3) $f \in V^*$, 若 $f(x) \neq 0$, 则 $V = \ker f \oplus \langle x\rangle$, 即 $\operatorname{Im} f \approx \langle x\rangle$.

(4) $0 \neq f, g \in V^*$, $\ker f = \ker g \Longleftrightarrow \exists 0 \neq \lambda \in F$, s.t. $f = \lambda g$.

证: (1) $v \neq 0$, 则 $V = \langle v\rangle \oplus \langle v\rangle^c$, 其中 $\langle v\rangle = \{rv \mid r \in F\}$.
令 $f: V \to F$, $rv + w \mapsto r$, 其中 $rv \in \langle v\rangle$, $w \in \langle v\rangle^c$, 故 $f(v) = 1$, $f \in V^*$.
我们来验证一下: $\forall u_1, u_2 \in V$, $r, t \in F$, u_1 和 u_2 可写成 $u_1 = r_1 v + w_2$, $u_2 = r_2 v + w_2$
$\Longrightarrow f(ru_1 + tu_2) = f(r(r_1 v + w_1) + t(r_2 v + w_2)) = f((rr_1 v + rw_1) + (tr_2 v + tw_2)) = rr_1 + tr_2 = rf(r_1 v + w_1) + tf(r_2 v + w_2) = rf(u_1) + tf(u_2)$.
故得证.

并且需要注意这里的 f 的构造不是唯一的: 我们可以构造 $f: V \to F$, $rv + u \mapsto rt$, 其中 $u \in \langle v\rangle^c$, 如此一来, $f(v) = t$.

(2) "$\Longrightarrow$": 若 $v = 0$, 则 $\forall u \in V$, $f(v) + f(u) = f(v + u) = f(u) \Longrightarrow f(v) = 0$.

"$\Longleftarrow$": 若 $\forall f \in V^*$, $f(v) = 0$, 则假设 $v \neq 0$, 则由 (1), $\exists v \in V^*$, s.t. $f(v) \neq 0$, 矛盾, 故假设错误, $v = 0$.

(3) $f(x) \neq 0 \Longrightarrow \operatorname{Im} f \neq \{0\} \Longrightarrow \dim \operatorname{Im} f \neq 0 \Longrightarrow \dim \operatorname{Im} f \dim(\ker f)^c = 1 \Longrightarrow \dim \ker f = \dim V - \dim(\ker f)^c = \dim V - 1$
$\Longrightarrow \exists v \in V$, s.t. $V = \ker f \oplus (\ker f)^c = \langle v\rangle$,
又 $\because f(x) \neq 0$, $\therefore x \in \langle v\rangle \Longrightarrow \langle x\rangle = \langle w\rangle \Longrightarrow V = \ker f \oplus \langle x\rangle$, 故得证.

(4) "$\Longrightarrow$": 令 $K = \ker f = \ker g$.
$\because \ker f = \ker g$, $\forall x \notin K$, 由 (3) 有, $V = \langle x\rangle \oplus K$.
取 $\lambda = \frac{f(x)}{g(x)}$ 即得.
"$\Longrightarrow$": 若 $\exists \lambda \neq 0$, $f = \lambda g$, 则显然 $\ker f = \ker g$.

□

定义 3.3 对偶基: $\mathcal{B} = \{b_1, \cdots, b_n\}$ 为 V 的基, 则 $\forall i$, $\exists b_i^* \in V$, s.t. $b_i^*(b_i) = 1$, 对 $j \neq i$, $b_i^*(b_j) = 0$, 即 $b_i^*(b_j) = \delta_{ij}$, 从而可以构造出 $\mathcal{B}^* = \{b_1^*, \cdots, b_n^*\} \subseteq V^*$, 称为 $\mathcal{B}$ 的对偶基.

定理 3.6 (课本定理3.12): (1) $\mathcal{B}^* = \{b_1^*, \cdots, b_n^*\}$ 线性无关.

(2) $\dim V < \infty$, 则 $\mathcal{B}^*$ 是 V^* 的基.

证: (1) $\sum_{i=1}^m r_i b_i^* = 0 \Longrightarrow \forall v \in V$, $\left(\sum_{i=1}^m r_i b_i^*\right)(v) = 0(v) = 0$
$\Longrightarrow \sum_{i=1}^m r_i b_i^*(v) = 0$

取 $v=b_j$, 则 $\sum_{i=1}^m r_i b_i^*(b_j)=\sum_{i=1}^m r_i\delta_{ij}=r_j=0$,
对各个 b_j 如法炮制, 从而得到 $r_j=0\forall i$, 故得证.

(2) $\forall f\in V^*, \forall v\in V, \because \mathcal{B}$ 是 V 的基, $\therefore v=\sum_{i=1}^n r_i b_i$
$\Longrightarrow b_j^*(v)=b_j^*\left(\sum_{i=1}^n r_i b_i\right)=\sum_{i=1}^n r_i b_j^*(b_i)=\sum_{i=1}^n r_i\delta_{ij}=r_j$
回代得 $v=\sum_{i=1}^n b_i^*(v)b_i$
$\Longrightarrow f(v)=f\left(\sum_{i=1}^n b_i^*(v)b_i\right)=\sum_{i=1}^n b_i^*(v)f(b_i)=\sum_{i=1}^n f(b_i)b_i^*(v)=\left(\sum_{i=1}^n f(b_i)b_i^*\right)(v)$, 这里 $b_i^*(v), f(b_i)\in F$,
因此可以交换位置, 我们可视 $\{b_i^*(v)\}$ 为基, $f(b_i)$ 为 $f(v)$ 在这组基上的展开系数
$\Longrightarrow f=\sum_{i=1}^n f(b_i)b_i^*$, 即 f 可展开为 $\{\mathcal{B}^*\}$ 的线性表示, 结合 (1) 得证.

□

按照类似上面的方法, $\forall v\in V$, 我们都可构造 $v^*\in V^*$, s.t. $\forall u_1\in\langle v\rangle$, $v^*(u)=1$, $\forall u_2\in\langle v\rangle^c$, $v^*(u_2)=0$,
从而有映射 $V\to V^*$, $v\mapsto v^*$, $0\mapsto 0$ (零映射).
V^* 本身也是向量空间.

定义 3.4 二重对偶(空间): $V^{**}=\mathcal{L}(V^*,F)$ 称为**二重对偶(空间)**, 其中的元素为 $v^{**}: V^*\to F$, $f\to f(v)$.

$V\to V^*\to V^{**}$, $v\mapsto v^*\mapsto v^{**}$, $b_i\mapsto b_i^*\mapsto b_i^{**}$, 满足 $b_i^*(b_j)=\delta_{ij}$, $b_i^{**}(b_j^*)=b_j^*(b_i)$, 两个映射复合得 $\tau: V\to V^{**}$, $v\mapsto v^{**}$.

(1) τ 是映射.

(2) τ 是线性变换.

(3) $\ker\tau=\{v\in V\mid \tau(v)=0\}=\{0\}\Longleftrightarrow\tau$ 单射.

证: (1) 若 $u=v$, 则 $\forall f\in V^*$, $u^{**}(f)=f(u)=f(v)=v^{**}(v)$, 即得证.

(2) $\tau(ru+tv)=(ru+tv)^{**}$,
$\forall f\in V^*$, $(ru+tv)^{**}(f)=f(ru+tv)=rf(u)+tf(v)=ru^{**}(f)+tv^{**}(f)=r\tau(u)(f)+t\tau(v)(f)\Longrightarrow$ $\tau(ru+tv)=r\tau(u)+t\tau(v)$,
结合 (1) 即得证.

(3) $\tau(v)=0\Longrightarrow\forall f\in V^*$, $v^{**}(f)=0\Longrightarrow f(v)=0\Longrightarrow$(定理 3.5 (1)) $v=0$, 即得证.

□

引理 3.1 (课本引理3.13): 若 $\dim V=n<\infty$, 则 $\dim V^*=\dim V^{**}=n$, V^{**} 与 V 同构, 一个线性空间的二重对偶就回到自身, 所以实际上套娃式的 $V^{*\cdots *}$ 是没有意义的, 这里我们就写成 $V^{**}=V$.

定义 3.5 算子伴随: 由线性变换 τ 可引出**算子伴随** $\tau^*: W^*\to V^*$, $g\mapsto g\circ\tau$.

$$\begin{tikzcd}
V \arrow[rr, "\tau"] \arrow[dr, "\tau^* = g \circ \tau"'] & & W \arrow[dl, "g"] \\
& F &
\end{tikzcd}$$

(1) τ^* 是映射.

(2) τ^* 是线性的.

证: (1) 若 $f = g \in W^*$, $v^* * \in \tau^*$, 则 $\tau^*(f) = f \circ \tau = g \circ \tau = \tau^*(g)$, 故得证.

(2) $\tau^*(rg_1 + tg_2) = (rg_1 + tg_2) \circ \tau = rg_1 \circ \tau + tg_2 \circ \tau = r\tau^*(g_1) + t\tau^*(g_2)$, 故得证.

□

定理 3.7 (课本定理3.18): (1) $\tau.\sigma \in \mathcal{L}(V,W)$, $a, b \in F$, 则 $(a\tau + b\sigma)^* = a\tau^* + b\sigma^*$, 即求和与算子伴随可交换.

(2) $\sigma \in \mathcal{L}(V,W)$, $\tau \in \mathcal{L}(W,U)$, 则 $(\tau \circ \sigma)^* = \sigma^* \circ \tau^*$.

(3) $\tau \in \mathcal{L}(V)$ 可逆 $\Longrightarrow (\tau^{-1})^* = (\tau^*)^{-1}$.

证: (1) $\forall f \in W^*$, $(a\tau + b\sigma)^*(f) = f \circ (a\tau + b\sigma) = af \circ \tau + bf \circ \sigma = a\tau^*(f) + b\tau^*(f)$, 即得证.

(2) $\forall f \in V^*$, $(\tau \circ \sigma)^*(f) = f \circ (t \circ \sigma) = f \circ (\tau \circ \sigma) = (f \circ \tau) \circ \sigma = \sigma^*(f \circ \tau) = \sigma^*(\tau^*(f)) = (\sigma^* \circ \tau^*(f)) = (\sigma^* \circ \tau^*)(f) \Longrightarrow (\tau \circ \sigma)^* = \sigma^* \circ \tau^*$.

$$\begin{tikzcd}
V \arrow[rr, "\sigma"] \arrow[dr, "\tau \circ \sigma"'] & & W \arrow[dl, "\tau"] \\
& U &
\end{tikzcd}
\qquad
\begin{tikzcd}
V^* & & W^* \arrow[ll, "\sigma^*"'] \\
& U^* \arrow[ul, "(\tau \circ \sigma)^* = \sigma^* \circ \tau^*?"] \arrow[ur, "\tau^*"'] &
\end{tikzcd}$$

(3) $1^* = (\tau \circ \tau^{-1})^* = (\tau^{-1})^* \circ \tau^* \Longrightarrow (\tau^{-1})^* = (\tau^*)^{-1}$.

□

定理 3.8 (课本定理3.18): $\dim V < \infty$, $\dim W < \infty$, $\tau \in \mathcal{L}(V,W)$, $\tau^* \in \mathcal{L}(V,W)$, $\tau^{**} \in \mathcal{L}(V^{**}, W^{**}) = \mathcal{L}(V,W)$, 则 $\tau^{**} = \tau$.

定理 3.9 (课本定理3.22): $\tau \in \mathcal{L}(V, W)$, 其中 $\dim V < \infty$, $\dim W < \infty$, $\mathcal{B}$ 和 $\mathcal{C}$ 分别是 V 和 W 的定序基, $\mathcal{B}^*$ 和 $\mathcal{C}^*$ 分别是 $\mathcal{B}$ 和 $\mathcal{C}$ 的对偶空间, 则 $[\tau^*]_{\mathcal{C}^*\mathcal{B}^*} = ([\tau]_{\mathcal{B}\mathcal{C}})^T$.

证: 设 $\dim V = n$, $\dim W = m$, V 的定序基 $\mathcal{B} = \{b_1, \cdots, b_n\}$, W 的定序基 $\mathcal{C} = \{c_1, \cdots, c_m\}$, $\tau \in \mathcal{L}(V, W)$ 的矩阵表示为 $[\tau]_{\mathcal{B}\mathcal{C}} = [\alpha_{ij}]_{m\times n}$, $\tau^* \in \mathcal{L}(W^*, V^*)$ 的矩阵表示为 $[\tau^*]_{\mathcal{C}^*\mathcal{B}^*} = [\beta_{ij}]_{n\times m}$,

即 $[\tau]_{\mathcal{B}\mathcal{C}} = \begin{pmatrix} [\tau(b_1)]_{\mathcal{C}} & \cdots & [\tau(b_n)]_{\mathcal{C}} \end{pmatrix}$, 令 $[\tau(b_i)]_{\mathcal{C}} = \begin{pmatrix} \alpha_{1i} \\ \vdots \\ \alpha_{mi} \end{pmatrix}$, $\tau(b_i) = \sum_{k=1}^m \alpha_{ki} c_k$.

$[\tau^*]_{\mathcal{C}^*\mathcal{B}^*} = \begin{pmatrix} [\tau^*(c_1^*)]_{\mathcal{B}^*} & \vdots & [\tau^*(c_n)] \end{pmatrix}$, 其中 $[\tau^*(c_i^*)]_{\mathcal{B}^*} = \begin{pmatrix} \beta_{1i} \\ \vdots \\ \beta_{ni} \end{pmatrix}$, $\tau^*(c_i^*) = \sum_{l=1}^n \beta_{li} b_l^*$.

又 $\because \tau^*(c_i^*) = c_i^* \circ \tau$, 我们将这一复合函数作用在 b_j 上有, $(c_i^* \circ \tau)(b_j) = \left(\sum_{l=1}^n \beta_{li} b_l^*\right)(b_j) = \sum_{l=1}^n \beta_{li} b_l^*(b_j) = \beta_{ji}$ $\Longrightarrow \beta_{ji} = c_i^*(\tau(b_j))$, 代入上面的 $\tau(b_j)$ 的展开式得 $\beta_{ji} = c_i^*\left(\sum_{k=1}^m \alpha_{kj} c_k\right) = \sum_{k=1}^m \alpha_{kj} c_i^*(c_k) = \sum_{k=1}^m \alpha_{kj} \delta_{ik} = \alpha_{ij}$, 故得证. $\square$

Chapter 4

模 I: 基本性质

定义 4.1 模: R 为有单位元交换环, $(M,+)$ 为交换群, 数乘 : $R\times M\to M$, $(r,m)\mapsto m$ 满足

(1) $(r+t)m=rm+tm$

(2) $(rt)m=r(tm)$

(3) $r(m_1+m_2)=rm_1+rm_2$

(4) $1m=m$

则称 M 为 R 上的**模**, 记作 $R-\mathrm{mod}\equiv\{R$ 上的模$\}$.

$\because$ 域是一种特殊的环, $\therefore$ 向量空间是一种特殊的模.

$0m=0$.

证: $0m+0m=(0+0)m=0m\Longrightarrow 0m=0$. □

$r0=0$.

证: $r0+r0=r(0+0)=r0\Longrightarrow r0=0$. □

$(-r)m=r(-m)=-(rm)$.

证: $(-r)m+rm=(-r+r)m=0m=0\Longrightarrow(-r)m=-rm$.
$r(-m)+rm=r(m+(-m))=r0=0\Longrightarrow r(-m)=-rm$. □

$\forall r\in R$, 可构造映射 $\bar r:M\to M$, $m\mapsto rm$. $\bar r$ 是 M 上的群同态, 又称**自同态**, 记作 $\bar r\in\mathrm{End}(M)\equiv\{M$ 上的自同态$\}$, $\mathrm{End}(M)$ 关于同态的加法、复合成环, 其单位元为 M 上的恒等映射, 记作 1_M, 故还可构造映射 $\phi:R\to\mathrm{End}(M)$, $r\mapsto\bar r$.

证: $\bar r(m+n)=r(m+n)=rm+rn=\bar r(m)+\bar r(n)$, 即映射 $\bar r$ 下保持运算结构, 故得证. □

例 4.1: 在交换群 $(G,+)$ 上定义 $1a=a$, $2a=a+a$, $\cdots$, $na=\overbrace{a+\cdots+a}^{n\text{ 个 }a\text{ 相加}}$, $-a=-1a$, $-2a=(-a)+(-a)$, $-na=\overbrace{(-a)+\cdots+(-a)}^{n\text{ 个 }(-a)\text{ 相加}}$, 数乘 $\alpha:\mathbb{Z}\times G\to G$, $(n,a)\mapsto na$, 满足

(1) α 是映射

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

(3) $(nm)a = n(ma)$

(4) $n(a+b) = na + nb$

证: (1) na 的定义依赖于 G 中的运算, 而运算的本质是卡氏积至原集合的映射, 有唯一的结果, 故得证.

(2) $(n+m)a = \overbrace{a+\cdots+a}^{(n+m)\text{ 个 } a \text{ 相加}} = \overbrace{a+\cdots+a}^{n\text{ 个 } a \text{ 相加}} + \overbrace{a+\cdots+a}^{m\text{ 个 } a \text{ 相加}} = na + ma.$

(3) $(nm)a = \overbrace{a+\cdots+a}^{nm\text{ 个 } a \text{ 相加}} = \overbrace{\overbrace{a+\cdots+a}^{m\text{ 个 } a \text{ 相加}} + \cdots + \overbrace{a+\cdots+a}^{m\text{ 个 } a \text{ 相加}}}^{n\text{ 组}} = \overbrace{ma+\cdots+ma}^{n\text{ 个 } ma \text{ 相加}} = n(ma).$

(4) $n(a+b) = \overbrace{(a+b)+\cdots+(a+b)}^{n\text{ 个 }(a+b)\text{ 相加}} = \overbrace{a+\cdots+a}^{n\text{ 个 } a \text{ 相加}} + \overbrace{b+\cdots+b}^{n\text{ 个 } b \text{ 相加}} = na + nb.$

(5) 由定义显然.

□

故 $M \in \mathbb{Z}-\mathrm{mod}$. □

例 4.2: $\forall$ 交换群 $(G,+)$, $G \in \mathbb{Z}-\mathrm{mod}$. □

例 4.3: $R \in R-\mathrm{mod}$, 其中的数乘即 R 中的乘法. □

例 4.4: $\mathbb{Z}_p = \frac{\mathbb{Z}}{p} = \{[0],\cdots,[p-1]\}$, $(\mathbb{Z}_p,+)$ 是交换群, 故 $\mathbb{Z}_p \in \mathbb{Z}-\mathrm{mod}$.

$\mathbb{Z}_6 = \{[0],[1],[2],[3],[4],[5]\}$, $n[k] = \overbrace{[k]+\cdots+[k]}^{n\text{ 个 }[k]\text{ 相加}} = [nk]$,
注意到 $[2] \neq [0]$, $3 \neq 0$, 但 $3[2] = [6] = [0]$, 即非零元素的卡氏积在数乘映射下得到零元素, 这意味着非零的单个元素不再线性无关.

实际上, $\mathbb{Z}_p$ 中无线性无关元素. □

例 4.5: $R^n = \{(r_1,\cdots,r_n) \mid r_i \in R\} \in R-\mathrm{mod}$, 其中 $(r_1,\cdots,r_n)+(l_1,\cdots,l_n) = (r_1+l_1,\cdots,r_n+l_n)$, $r(r_1,\cdots,r_n) = (rr_1,\cdots,rr_n)$. □

定义 4.2 <u>子模</u>: $\emptyset \neq S \subseteq M$, 若在 M 的运算下, S 是 R 上的模, 则称 S 为 M 的子模.

定理 4.1 <u>判定子模的方法(课本定理4.1)</u>: $\emptyset \neq S \subseteq M$ 是 M 的子模 $\Longleftrightarrow \forall u,v \in S, \forall r,t \in R, ru+tv \in S$ (即线性运算封闭).

定理 4.2 <u>(课本定理4.2)</u>: $S,T \subseteq M$ 是 M 的子模, 则 $S \cap T$ 为 M 的子模, $S+T \equiv \{u+v \mid u \in S, v \in T\}$ 为 M 的子模.

定理 4.3: $R \in R-\mathrm{mod}$, R 的子模即 R 上的理想.

证: 设 S 为 R 的子模, 则

(1) $\emptyset \neq S \subseteq R$

(2) $\forall u, v \in S, \forall r, t \in R, ru + tv \in S$. 特别地, 令 $r = 1, t = -1$, 得 $u - v \in S$, 令 $t = 0$, 得 $ru \in S$

故 S 为 R 的理想. □

定义 4.3 **生成子模和生成集:** $\emptyset \neq S \subseteq M \in R-\mathrm{mod}$, S 的**生成子模**为 $\langle\langle S\rangle\rangle \equiv$ 包含 S 的最小子模 $\equiv$ 包含 S 的所有子模的交 $= \{\sum_{i=1}^{n} r_i u_i \mid r_i \in R, u_i \in S, n \in \mathbb{Z}^+\}$, 其中称 S 为**生成集**.

$\forall M \in R-\mathrm{mod}$, 都有生成集, $\because M = \langle\langle M\rangle\rangle$.

定义 4.4 **有限生成模:** 生成集由有限个元素构成的生成模.

定义 4.5 **循环模:** 由一个元素生成的模.

例 4.6: $R \in R-\mathrm{mod}$ 是一个循环模, $\because R = \langle\langle 1\rangle\rangle = \{r1 \mid r \in R\}$. □

有限生成模的子模未必是有限生成的, 即有限生成的性质未必会由模遗传至其子模.

例 4.7: 多项式环 $R = F[x_1, \cdots, x_n, \cdots] \equiv \left\{\sum_{k_i=0}^{N} a_{i_1,\cdots,i_n} x_{i_1}^{k_1} \cdots x_{i_n}^{k_n} \mid a_{i_1\cdots i_n} \in F, N_i \in \mathbb{Z}^+\right\}$, $R \in R-\mathrm{mod}$ 且 $R = \langle\langle 1\rangle\rangle$.
假设 S 是有限生成的, $S = \langle\langle f_1, \cdots, f_m\rangle\rangle$, $f_i = \sum_{j_1,\cdots,j_m=0}^{N_i} a_{i_1,\cdots,i_n}^{j_1,\cdots,j_n} x_{i_1}^{j_1} \cdots x_{i_n}^{j_n}$ 是有限个变元的有限次多项式, 故 S 无法生成无限个变元的无限次多项式, 即 S 并非是有限生成的. □

定义 4.6 **线性无关:** $\emptyset \neq S \subseteq M$, 若 $\sum_{i=1}^{n} r_i u_i = 0$ 其中 $u_i \in S$, $r_i \in R \forall i \Longrightarrow r_1 = \cdots = r_n = 0$, 则称 S 线性无关.

在模中, 线性无关元素未必存在, 如例 4.4 中 $\mathbb{Z}_p$ 无线性无关元素.

在向量空间中, 我们有: u, v 线性相关 $\Longleftrightarrow \exists$ 不全为零的 $r, t \in R$, s.t. $ru + tv = 0$, 无妨设 $r \neq 0$, 则 $ru = -tv \Longrightarrow u = -\frac{t}{r} v$.

在模中, 上述说法未必成立: u, v 线性相关 $\Longleftrightarrow \exists$ 不全为零的 r, t, s.t. $ru + tv = 0$, (无妨设 $r \neq 0$,) 则 $ru = -tv$, 但由于未必能找到 r 的逆元, 所以未必有 $u = -\frac{t}{r} v$. 故在模中, 线性相关元素未必能相互表示, 即一个线性相关元素未必能由与其线性相关的元素线性表示.

定义 4.7 **自由模:** $M \in R-\mathrm{mod}$, $M = \langle\langle \mathcal{B}\rangle\rangle$ 且 $\mathcal{B}$ 线性无关, 则称 M 为**自由模**, $\mathcal{B}$ 为 M 的基.

定理 4.4 **(课本定理4.3):** $\emptyset \neq \mathcal{B} \subseteq M$ 是 M 的基, 则 $\forall v \in M$, v 可由 $\mathcal{B}$ 中的元素唯一地线性表示.

定理 4.5 **(课本定理4.4):** $\mathcal{B}$ 是 M 的基 $\Longleftrightarrow \mathcal{B}$ 为 M 的极小生成集且为 M 的极大线性无关集.

例 4.8: $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$, $\mathbb{Z}_6 = \langle\langle [1]\rangle\rangle = \langle\langle [5]\rangle\rangle$,
$\because 0[1] = [0]$, $1[1] = [1]$, $2[1] = [2]$, $3[1] = [3]$, $4[1] = [4]$, $5[1] = [5]$,
$0[5] = [0]$, $1[5] = [5]$, $2[5] = [10] = [4]$, $3[5] = [15] = [3]$, $4[5] = [20] = [2]$, $5[5] = [25] = [1]$.
故 $\mathbb{Z}_6$ 的表示不唯一. □

$M \in R-\text{mod}$, 但 M 的子模未必自由.

例 4.9: $R = \mathbb{Z} \times \mathbb{Z} = \{(n, m) \mid n, m \in \mathbb{Z}\}$, 其中 $(n, m)(k, l) = (nk, ml)$, $(n, m) + (k, l) = (n + k, m + l)$ 是仅为交换环 (而非域), $R \in R-\text{mod}$, $R = \langle\langle(1, 1)\rangle\rangle = \{r(1, 1) \mid r \in R = \mathbb{Z} \times \mathbb{Z}\}$, $\therefore R$ 自由.
但子模 $S = \mathbb{Z} \times \{0\} = \{(n, 0) \mid n \in \mathbb{Z}\}$, $\because \forall n \neq 0$, $(n, 0)(0, 1) = (0, 0)$, $\therefore$ 无线性无关元, 从而非自由. $\square$

定义 4.8 <u>模同态</u>: $M, N \in R-\text{mod}$, 映射 $\tau : M \to N$, 若 $\forall u, v \in M$, $r, t \in R$, $\tau(ru + tv) = r\tau(u) + t\tau(v)$, 则 τ 为 M 到 N 的**模同态**, 记作 $\tau \in \hom(M, N) = \{M \text{ 到 } N \text{ 的模同态}\}$.

取 $r = t = 1$, 则 $\forall u, v \in M$, $\tau(u + v) = \tau(u) + \tau(v)$, 故 τ 为群同态.

定理 4.6 <u>(课本定理4.6)</u>: (1) $\ker \tau \equiv \{v \in M \mid \tau(v) = 0\}$ 是 M 的子模. τ 单射 $\iff \ker \tau = \{0\}$.

(2) $\operatorname{Im} \tau \equiv \{\tau(v) \mid v \in M\}$ 是 N 的子模. τ 满射 $\iff \operatorname{Im} \tau = N$.

定义 4.9 <u>商模</u>: S 是 M 的子模, **商群** $\frac{M}{S} \equiv \{[v] \mid v \in M\}$.

$[u] + [v] = [u + v]$, $r[u] = [ru]$ 是合法运算, $\because$ 结果与代表元选取无关.

$$\begin{tikzcd}
v \arrow[rrrr, mapsto] \arrow[dddd, mapsto] & & & & \tau[v] \\
& M \arrow[rr, "\tau"] \arrow[d, "\Pi_S"] & & N & \\
& \frac{M}{S} \arrow[urr, dashed, "\tau'"] & & & \\
& & & & \\
{[v]} \arrow[uuuurrrr, dashed, mapsto] & & & &
\end{tikzcd}$$

$\Pi_S : M \to \frac{M}{S}$, $v \mapsto [v]$, 且满足

(1) Π_S 满射.

(2) $\ker \Pi_S = S$.

定理 4.7 <u>同态第一基本定理</u>: 若 $S \subseteq \ker \tau$, 则 $\exists! \tau'$, s.t. $\tau = \tau' \circ \Pi_S$.

$\ker \tau' = \frac{\ker \tau}{S}$.

定理 4.8 <u>同构第一基本定理</u>: 若 $S = \ker \tau$, 则 $\tau' = \frac{\ker \tau}{S} = \{[0]\}$, 即 τ' 单射.
$\because \operatorname{Im} \tau' = \operatorname{Im} \tau$, $\therefore$ 若进一步有 τ, 则 τ' 同构.

Chapter 5

模 II: 自由与诺特模

定义 5.1 诺特(Notherian) 模: $M \in R-\mathrm{mod}$, $S_1, \cdots, S_n, \cdots$ 是 M 的子模且 $S_1 \subseteq \cdots \subseteq S_n \subseteq \cdots$, 若 $\exists K \in \mathbb{Z}^+$, s.t. $S_K = S_{K+1} = \cdots$, 则称 M 满足**升链条件 (A.C.C.)**, 称满足 ACC 的模为**诺特模**.

定理 5.1 (课本定理5.7): (1) $M \in R-\mathrm{mod}$ 为诺特模 $\Longleftrightarrow$ M 的子模是有限生成的.

(2) R 是诺特环 $\Longleftrightarrow$ R 的理想都是有限生成的.

证: (1) "$\Longrightarrow$": 设 S 是 M 的子模. 若 $S = \{0\}$, 则 $S = \langle\langle 0 \rangle\rangle$ 显然有限生成,

若 $S \neq \{0\}$, 则 $\exists 0 \neq v_1 \in S$, 令 $S_1 = \langle\langle v_1 \rangle\rangle \subseteq S$,

若 $S_1 = S$, 则 S 有限生成,

若 $S_1 \neq S$, 则 $\exists v_2 \in S - S_1$, 令 $S_2 = \langle\langle v_1, v_2 \rangle\rangle \subseteq S$, 则 $S_1 \subseteq S_2 \subseteq S$,

若 $S_2 = S$, 则 S 有限生成,

若 $S_2 \neq S$, 则 $\exists 0 \neq v_3 \in S - S_2$, 令 $S_3 = \langle\langle v_1, v_2, v_3 \rangle\rangle \subseteq S$, 则 $S_1 \subseteq S_2 \subseteq S_3 \subseteq S$,

若 $S_3 = S$, 则 S 有限生成,

若 $S_3 \neq S$, 则 $\exists 0 \neq v_4 \in S - S_3$, 令 $S_4 = \langle\langle v_1, v_2, v_3, v_4 \rangle\rangle \in S$, 则 $S_1 \subseteq S_2 \subseteq S_3 \subseteq S_3 \subseteq S_4 \subseteq S$,

$\cdots$

以此类推, 得 $S_1 \subseteq S_2 \subseteq \cdots \subseteq S_n \subseteq \cdots$,

$\because S$ 满足 ACC, $\therefore \exists K \in \mathbb{Z}^+$, s.t. $S_K = S_{K+1} = \cdots = S = \langle\langle v_1, \cdots, v_n \rangle\rangle$, 故 S 有限生成.

"$\Longleftarrow$": 取 M 的任一子模升链 $S_1 \subseteq \cdots \subseteq S_n \subseteq \cdots$, 则 $S = \cap_{i \in J} S_i$ 是 M 的子模,

$\because M$ 的子模是有限生成的, $\therefore S$ 必然是有限生成, 故设 $S = \langle\langle v_m, \cdots, v_m \rangle\rangle$,

$\forall K = 1, \cdots, m$, $u_k \in S = \cup_{i \in J} S_i \Longrightarrow \exists i_k \in J$, s.t. $u_k \in S_{i_k}$,

令 $K = \max\{i_1, \cdots, i_m\}$, 则由升链的性质, $u_1, \cdots, u_m \in S_K$

$\Longrightarrow S_K = S$, 故升链必终止于 S_K.

综上, 得证.

$\square$

例 5.1: $\because \mathbb{Z}$ 的任意理想均有单个元素生成, 具体地说, I 是 $\mathbb{Z}$ 的理想, 则 $I = \langle n \rangle$, 其中 n 为 I 中的最小整数, $\therefore \mathbb{Z}$ 是诺特环. $\square$

例 5.2: $F[x] = \{\sum_{i=0}^{n} a_i x^i \mid a_i \in F, n \in \mathbb{Z}\}$, I 是 $F[x]$ 的理想, 则 $I = \langle f(x) \rangle$, 其中 $\deg f(x)$ 是 I 中最小的[1], 故

[1] 多项式间的除法: 若 $\deg g(x) \geq \deg f(x)$, 则 $\exists q(x), r(x) \in F[x]$, s.t. $g(x) = q(x)f(x) + r(x)$ 且 ($r(x) = 0$ 或 $0 < \deg r(x) < \deg f(x)$)

$(F[x], +, \cdot)$ 是诺特环. □

定义 5.2 主理想: 由一个元素生成的诺特环.

定理 5.2 (课本定理5.8): R 为有单位元的交换环,
R 是诺特环 $\iff$ R 上的有限生成模都是诺特模.

上述定理意味着有限生成的性质对诺特环是遗传的.

证: "$\Longleftarrow$": $R \in R-\mathrm{mod}$ 且 $R = \langle\langle 1\rangle\rangle$, 故 R 为诺特环.

"$\Longrightarrow$": 取 R 上的有限生成模 $M = \langle\langle v_1, \cdots, v_n\rangle\rangle \in R-\mathrm{mod}$, $M = \{\sum_{i=1}^n r_i v_i \mid r_i \in R\}$.
定义映射 $\tau : R^n \to M$, $(r_1, \cdots, r_n) \mapsto \sum_{i=1}^n r_i u_i$.

(1) $\because \tau(r(r_1, \cdots, r_n) + t(l_1, \cdots, l_n)) = \tau(rr_1 + tl_1, \cdots, rr_n + tl_n) = \sum_{i=1}^n (rr_i + tl_i)u_i = r\sum_{i=1}^n r_i u_i + t\sum_{i=1}^n l_i u_i = r\tau(r_1, \cdots, r_n) + t\tau(l_1, \cdots, l_n)$, $\therefore \tau$ 是 R^n 到 M 上的模同态.

(2) $\because \forall (r_1, \cdots, r_n)$, $\exists \sum_{i=1}^n r_i u_i$, $\therefore \tau$ 满射.

$\Longrightarrow \tau$ 满同态.

设 S 是 M 的任一子模, 则 $\tau^{-1}(S)$ 是 R^n 的子模, 且 $\because \tau$ 满同态, $\therefore \tau(\tau^{-1}(S)) = S$.

【思路】根据定理 5.2, 要证 M 诺特, 即证 M 的子模 S 有限生成, 于是先证 R^n 的子模有限生成, 从而 R^n 诺特, 进而利用引理 5.1 得 S 有限生成.

数学归纳法: 当 $n = 1$ 时, R 诺特 $\Longrightarrow R^n$ 诺特.
假设当 $n = k$ 时, R^k 诺特, 则当 $n = k + 1$ 时, 要证 R^{k+1} 诺特, 即证 R^{k+1} 的子模有限生成.
取 I 为 R^{n+1} 子模, 取 $I_1 = \{(0, \cdots, 0, a_{k+1}) \mid \exists a_1, \cdots, a_k \in R,\ \text{s.t. } (a_1, \cdots, a_k, a_{k+1}) \in I\}$, $I_2 = \{(a_1, \cdots, a_k, 0) \mid \exists a_k \in R,\ \text{s.t. } (a_1, \cdots, a_k, a_{k+1}) \in I\}$.
$\forall (0, \cdots, 0, a_{k+1}), (0, \cdots, 0, b_{k+1}) \in I_1$, $\exists a_1, \cdots, a_k, b_1, \cdots, b_k \in R$, s.t. $(a_1, \cdots, a_k, a_{k+1}), (b_1, \cdots, b_k, b_{k+1}) \in I$,
$\because I$ 是子模, $\therefore \forall r, t \in R$, $r(a_1, \cdots, a_k, a_{k+1}) + t(b_1, \cdots, b_k, b_{k+1}) = (ra_1 + tb_1, \cdots, ra_k + ta_k) \in I \Longrightarrow r(0, \cdots, 0, a_{k+1}) + t(0, \cdots, 0, b_{k+1}) = (0, \cdots, 0, ra_{k+1} + tb_{k+1}) \in I_2$, 故 I_1 为 R^{k+1} 的子模.
$\forall (a_1, \cdots, a_k, 0), (b_1, \cdots, b_k, 0) \in I_2$, $\exists a_{k+1}, b_{k+1}$, s.t. $(a_1, \cdots, a_k, a_{k+1}), (b_1, \cdots, b_k, b_{k+1}) \in I$
$\therefore I$ 是子模, $\therefore \forall r, t \in R$, $r(a_1, \cdots, a_k, a_{k+1}) + t(b_1, \cdots, b_k, b_{k+1}) = (ra_1 + tb_1, \cdots, ra_k + ta_k) \in I \Longrightarrow r(a_1, \cdots, a_k, 0) + t(b_1, \cdots, b_k, 0) = (ra_1 + tb_1, \cdots, ra_k + tb_k, 0) \in I_2$, 故 I_2 为 R^{k+1} 的子模.
令 $J_1 = \{a_{k+1} \mid (0, \cdots, 0, a_{k+1}) \in I_1\}$, $J_2 = \{(a_1, \cdots, a_k) \mid (a_1, \cdots, a_k) \in I_2\}$, 易证 J_1 是 R 的子模, J_2 是 R^k 的子模.
$\because R, R^k$ 诺特, $\therefore J_1, J_2$ 有限生成, 设 $J_1 = \langle\langle g_1, \cdots, g_m\rangle\rangle$, $J_2 = \langle\langle f_1, \cdots, f_n\rangle\rangle$, 其中 $g_1 \in R$, $f_i \in R^k$.
于是 $\forall i = 1, \cdots, m$, $(0, \cdots, 0, g_i) \in I_1$, 由 I_1 的定义, $\exists g_{i_1}, \cdots, g_{i_k} \in R$, s.t. $\bar{g}_i \equiv (g_{i_1}, \cdots, g_{i_n}, g_i) \in I$,
又有 $\bar{f}_i = (f_i, 0)$,
$\forall r = (r_1, \cdots, r_k, r_{k+1}) \in I$, 则 $(0, \cdots, 0, r_{k+1}) \in I_1$, 即 $r_{k+1} \in J_1 = \langle\langle g_1, \cdots, g_m\rangle\rangle$,
于是 $r_{k+1} = \sum_{i=1}^m \alpha_i g_i$, $(h, 0) \equiv r - \sum_{i=1}^m \alpha_i \bar{g}_i = (*, \cdots, *, 0) \in I$, 从而 $(h, 0) \in I_2$, $h \in J_2$, 设 $h = \sum_{i=1}^n \beta_i f_i$
$\Longrightarrow r = \sum_{i=1}^m \alpha_i \bar{g}_i + \sum_{i=1}^n \beta_i \bar{f}_i$, 故 I 由 $\bar{g}_1, \cdots, \bar{g}_m, \bar{f}_1, \cdots, \bar{f}_n$ 生成 $\Longrightarrow R^{k+1}$ 诺特 $\Longrightarrow R^n$ 诺特 $\forall n \Longrightarrow S = \tau(\tau^{-1}(S))$ 有限生成. □

引理 5.1: $\tau : M \to N$ 满同态, 则 M 有限生成 $\Longrightarrow N$ 有限生成, 即有限生成模的满同态像有限生成.

证: $\because M$ 有限生成, $\therefore$ 设 $M = \langle\langle v_1, \cdots, v_n\rangle\rangle = \{\sum_{i=1}^n r_i v_i \mid r_i \in R\}$,
$\because \tau$ 满同态, $\therefore N = \operatorname{Im}\tau = \{\tau(u) \mid u \in M\} = \{\tau(u) \mid u = \sum_{i=1}^n r_i v_i, r_i \in R\} = \{\tau(\sum_{i=1}^n r_i v_i) \mid r_i \in R\} = \{\sum_{i=1}^n r_i \tau(v_i) \mid r_i \in R\} = \langle\langle \tau(v_1), \cdots, \tau(v_n)\rangle\rangle$, 故 N 有限生成. □

定理 5.3 Hilbert 基本定理(课本定理5.9): R 是诺特环 $\Longrightarrow R[x] \equiv \{\sum_{i=0}^n a_i x^i \mid a_i \in R, n \in \mathbb{Z}^+\}$ 诺特, 其中 $\sum_{i=0}^n a_i x^i + \sum_{j=0}^m b_j x^j = \sum_{k=0}^{\max\{n,m\}} (a_k + b_k) x^k$, $(\sum_{i=0}^n a_i x^i)\left(\sum_{j=0}^m b_j x^j\right) = \sum_{k=0}^{nm}\left(\sum_{i+j=k} a_i b_j\right) x^k$.

证: 设 I 是 $R[x]$ 的理想, $I_k = \{r_k \in R \mid \exists a_0 + a_1 x + \cdots + a_{k-1}x^{k-1} + r_k x^k \in I\}$ 是 R 的理想,
且 $\because \forall f(x) \in I$, $xf(x) \in I$, $\therefore I_0 \subseteq I_1 \subseteq \cdots \subseteq I_K \subseteq \cdots$
又 $\because R$ 诺特, $\therefore \exists K \in \mathbb{Z}^+$, s.t. $I_K = I_{K+1} = \cdots$, 且 R 的理想均有限生成,
故设 $I_0 = \langle r_{01}, r_{02}, \cdots, r_{0t_0}\rangle$, $I_1 = \langle r_{11}, r_{12}, \cdots, r_{1t_1}\rangle$, $\cdots$, $I_K = \langle r_{K1}, r_{K2}, \cdots, r_{Kt_K}\rangle$,
$g_{01} = r_{01} \in I$, $g_{02} = r_{02} \in I$, $\cdots$, $g_{0t_0} = r_{0t_0} \in I$,
$g_{11} = r_{11}x + O(1) \in I$, $g_{12} = r_{12}x + O(1) \in I$, $\cdot$, $g_{1t_1} = r_{1t_1}x + O(1) \in I$,
$\cdots$,
$g_{K1} = r_{K1}x^k + O(x^{k-1}) \in I$, $r_{K2}x^K + O(x^{K-1}) \in I$, $\cdots$, $g_{Kt_K} = r_{Kt_K}x^K + O(x^{K-1}) \in I$,
则 I 由 $\{g_{ij} \mid i = 1, \cdots, K; j = 1, \cdots t_i\}$ 生成,
$\forall f(x) \in I$, 设 $f(x) = \sum_{i=0}^n a_i x^i$,
取 $a_n \in I_n$, 若 $n > K$, 则 $I_n = I_K = \langle r_{K1}, \cdots, r_{Kt_K}\rangle$, 从而 $a_n = \sum_{i=r}^{t_K} \alpha_i r_i$,
$\Longrightarrow f(x) = a_n x^n + O(x^{n-1}) = x^{n-1}\left(\sum_{i=1}^{t_K} \alpha_i g_{Ki}\right) + O(x^{n-K}) = x^{n-K}\left(\sum_{i=1}^{t_K} \alpha_i g_{Ki}\right) + O(x^{K-1}) = \sum_{i=1}^{t_K} \alpha_i r_{Ki} x^n + O(x^{n-1})$,
$f(x) \to f(x) - x^{n-K}\left(\sum_{i=1}^{t_K} \alpha_i g_{Ki}\right) = \beta_{n-1}x^{n-1} + O(x^{n-2})$,
重复以上操作直至多项式的最高次数 $n < K$, 此时, $a^n \in I_n = \langle r_{n1}, \cdots, r_{nt_n}\rangle$, $a_n = \sum_{j=1}^{t_n} \beta_j r_{nj}$, $f(x) - \sum_{j=1}^{t_n} \beta_j g_{nj} =$,
即执行以上操作有限次后, $f(x)$ 完全由 g_{ij} 表示 $\Longrightarrow I$ 有限生成, 故由定理 5.1 得, $R[x]$ 诺特. □

例 5.3: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ 诺特 $\Longrightarrow \mathbb{Z}[x], \mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$ 诺特.
$\mathbb{R}[z] = \{\sum_{i=0}^n a_i x^i \mid a_i \in \mathbb{R}, n \in \mathbb{Z}^+\}$,
方程组 $\begin{cases} f_1(x) = a_{1n}x^n + a_{1,n-1}x^{n-1} + \cdots + a_{11}x + a_{10} = 0, \\ \cdots \\ f_m(x) = a_{mn}x^n + a_{m,n-1}x^{n-1} + \cdots + a_{m1}x + a_{m0} = 0, \end{cases}$ 的解为 $\mathbb{R}$ 的子集合,
令 $h(x) = \sum_{i=1}^m \alpha_i f_i(x)$, 若 $f_i(x) = 0 \forall i$, 则 $h(x) = 0$.
方程组与解集合之间存在的一一对应的关系, 正如 $\mathbb{R}[x]$ 与 $\mathbb{R}$ 之间的对应关系. □

Chapter 6

主理想整环上的模

定义 6.1 **主理想整环(PID):** 每个理想均由一个元素生成的整环.

例 6.1: $\mathbb{Z}$, $\mathbb{C}[x]$ 为 PID. □

PID 必诺特.

$\mathbb{R}$ 为整环, $a, b, r, s \in R$,

(1)

定义 6.2 **整除:** r **整除** $s \Longleftrightarrow s = xr$, $x \in R$, 记作 $r \mid s$.

(2)

定义 6.3 **单位:** R 中的可逆元.

例 6.2: $\mathbb{Z}$ 中的 1 和 -1 互逆, 故 1 和 -1 均为单位, 实际上, $\mathbb{Z}^* \equiv \mathbb{Z} - \{0\}$ 中的元素均为单位. □

(3)

定义 6.4 **素元:** $0 \neq q \in R$, 若 $p \mid ab \Longrightarrow p \mid a$ 或 $p \mid b$, 则称 p 为**素元**.

(4)

定义 6.5 **不可约元:** $0 \neq r \in R$, 若 $r = ab \Longrightarrow a$ 或 b 为单位, 则称 r 为**不可约元**.

(5)

定义 6.6 **互素:** r 与 b **互素** $\Longrightarrow a$ 与 b 无非单位公因子.

注意:

- 单元必素, 必不可约.

  证: 设 $0 \neq r \in R$ 为单位, 则必 $\exists a$ 的逆 a^{-1}.
  若 $r \mid ab$, 则 $(ar^{-1})r = a$, $(br^{-1})r = b \Longrightarrow r$ 为素元.
  若 $r = ab$, 则 $r^{-1}r = r^{-1}(ab) = (r^{-1}a)b = 1$, $r^{-1}a$ 为 b 的逆元, 即 b 可逆 $\Longrightarrow r$ 为不可约元. □

- 对于整环来说, 素元不可约, 反之未必.

  证: 设 p 为素元, 若 $p=ab$, 则 $1p=p=ab \Longrightarrow p \mid ab$.
  $\because p$ 为素元, $\therefore p \mid a$ 或 $p=b$.
  无妨 $p \mid a$, 则 $a=px$, 其中 $x \in R$
  $\Longrightarrow p=ab=pxb \Longrightarrow p(1-xb)=0$,
  $\because p \neq 0$ 且 R 为整环 (R 无零因子), $\therefore 1-xb=0 \Longrightarrow xb=1 \Longrightarrow b$ 为单位, 故 p 为不可约元. □

  例 6.3: (不可约元非素的例子) $R=\{a+b\sqrt{-5} \mid a,b \in \mathbb{Z}\}$ 为整环.
  $9=3^2=(2+\sqrt{-5})(2-\sqrt{-5})$,
  3 不可约 (证略), $3 \mid (2+\sqrt{-5})(2-\sqrt{-5})$, 但 $3 \nmid (2+\sqrt{-5})$, $3 \nmid (2-\sqrt{-5}) \Longrightarrow 3$ 非素. □

- 对于非整环来说, 素元未必不可约.

  例 6.4: $(\mathbb{Z}_6,+,\cdot)$ 非整环, $[2]$ 为素元, 但 $[2]=[2][4]$, $[2]$ 和 $[4]$ 均非单位 $\Longrightarrow [2]$ 可约. □

定理 6.1 (课本定理0.29): R 为 PID, $a,b \in R$,
a 与 b 互素 $\Longleftrightarrow \exists r,t \in R$, s.t. $ra+tb=1$.

证: "$\Longrightarrow$": R 为 PID, 令 $I=\langle a,b\rangle$,
$\because R$ 是主理想, $\therefore I$ 可由一个元素生成, 设 $I=\langle c\rangle$, 其中 $c \in R$,
又 $\because a \in I$, $b \in I$, $\therefore c \mid a$, $c \mid b \Longrightarrow c$ 为 a 和 b 的公因子,
$\because a,b$ 互素, $\therefore c$ 为单位, 即 $\exists c^{-1} \in R$, s.t. $1=c^{-1}c \in I$,
$\because 1 \in I$, $\therefore 1=ra+tb$.
"$\Longleftarrow$": 取 c 为 a 和 b 的公因子,
$\because 1=ra+tb$, $\therefore c \mid 1 \Longrightarrow c$ 可逆, 即 c 为单位. □

有算法可以在给定 a,b 下找到 s,t, 此处不赘述.

定理 6.2 (课本定理0.29): R 是 PID, $\forall 0 \neq r \in R$, $r=up_1\cdots p_n$ 且该分解式唯一, 其中 u 为单位, p_i 是 R 中的不可约元, $n \in \mathbb{Z}^+$.

证: 若 r 不可约, 则直接得证.
若 r 可约, 则设 $r=r_1r_2$, r_1 和 r_2 至少有一个非单位,
无妨 r_1 不是单位, 则 r_1 不可约.
若 r_2 不可约, 则得证,
若 r_2 可约, 则 $\langle r\rangle \subseteq \langle r_2\rangle$,
对 r_2 继续如上分解, 可得 $\langle r\rangle \subseteq \langle r_2\rangle \subseteq \cdots$,
又 $\because R$ 为 PID, $\therefore R$ 诺特, 即 $\exists K \in \mathbb{Z}^+$, s.t. $\langle r_K\rangle=\langle r_{K+1}\rangle=\cdots$,
故重复如上分解操作, 最终可将 r 表为有限个不可约元的乘积. □

定义 6.7 挠元(Torsion): $M \in R-\mathrm{mod}$, $v \in M$, 若 $\exists 0 \neq r \in R$, s.t. $rv=0$, 则称 v 为 M 的挠元.

定义 6.8 挠模: 所有元素均为挠元的模.

定义 6.9 无挠: 若一模无非零挠元, 则称该模**无挠**.

与线性无关类似, 若 $0 \neq v \in M$, $r \in R$, $rv = 0$, 且 M 无挠, 则 $r = 0$.

定义 6.10 挠子模: $M_{\text{tor}} = \{v \in M \mid v \text{ 为挠元}\}$.

$\because 0$ 为 M 的挠元, $0 \in M_{\text{tor}}$, $\therefore M_{\text{tor}} \neq \emptyset$.

M_{tor} 为 M 的子模.

证: $\forall u, v \in M_{\text{tor}}$, $\exists 0 \neq r_1, r_2 \in R$, s.t. $r_1 u = 0$, $r_2 v = 0$,
$\forall s, t \in R$, $(r_1 r_2)(su + tv) = r_2 s(r_1 u) + r_1 t(r_2 v) = r_2 s \cdot 0 + r_1 t \cdot 0 = 0 + 0 = 0$ 且 $r_1 r_2 \neq 0 \Longrightarrow (su + tv) \in M_{\text{tor}}$, 故得证. □

$\frac{M}{M_{\text{tor}}}$ 无挠.

证: 假设 $[0] \neq [v] \in \frac{M}{M_{\text{tor}}}$ 为挠元, 则 $\exists 0 \neq r \in R$, $r[v] = [rv] = [0] = M_{\text{tor}} \Longrightarrow rv \in M_{\text{tor}} \Longrightarrow v = r^{-1}(rv) \in M_{\text{tor}} \Longrightarrow [v] = M_{\text{tor}} = [0]$, 与假设矛盾, 故假设错误, 得证. □

定义 6.11 零化子: $v \in M \in R-\text{mod}$, v 的**零化子** $\text{ann}(v) \equiv \{r \in R \mid rv = 0\} \subseteq R$.
N 是 M 的子模, 则 $\text{ann}(N) = \{r \in R \mid rN \equiv \{rv \mid v \in N\} = \{0\}\} \subseteq R$.

$\text{ann}(v)$ 是 R 的理想.

证: $\forall s, t \in \text{ann}(v)$, $sv = tv = 0 \Longrightarrow sv - tv = (s - t)v = 0 \Longrightarrow s - t \in \text{ann}(v)$,
$\forall r \in R$, $(rs)v = r(sv) = r \cdot 0 = 0 \Longrightarrow rs \in \text{ann}(v)$.
综上, 得证. □

同理, $\text{ann}(N)$ 也是 R 的理想

定义 6.12 阶: 若 R 为 PID, 则 $\text{ann}(v), \text{ann}(N)$ 均为主理想, 其生成元分别称为 v 和 N 的**阶**.

定理 6.3 (课本定理6.5): R 为 PID, $M \in R-\text{mod}$ 自由, 则 M 的子模均自由.

证: (不严谨的证明, 仅针对) M 有限生成 (的特殊情况) 且自由. 设 $M = \langle\langle v_1, \cdots, v_n \rangle\rangle = \{\sum_{i=0}^n r_i v_i \mid r_i \in R\}$, 其中 $\{v_1, \cdots, v_n\}$ 线性无关.

$\forall v \in M$, $v = \sum_{i=1}^n r_i v_i$ 展开唯一, 定序后, $M \longleftrightarrow R^n$, $v \longleftrightarrow \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix}$ 模同构.

设 S 是 R^n 的子模, 取 R 的理想 $I_k = \{r_k \in R \mid \exists a_1, \cdots, a_{k-1} \in R, \text{ s.t. } (a_1, \cdots, a_{k-1}, r_k, 0, \cdots, 0) \in S\}$.
$\because R$ 为 PID, $\therefore I_k$ 由一个元素生成, 设 $I_k = \langle r_k \rangle$, 其中 $r_k \neq 0$, $k = 1, \cdots, n$.
取 $u_k = (a_1^k, \cdots, a_{k-1}^k, r_k, 0, \cdots, 0) \in S$, $S = \langle u_1, \cdots, u_n \rangle$ 生成 (下证) 且显然 $\{u_1, \cdots, u_n\}$ 线性无关.
取 $(b_1, \cdots, b_n) \in S$, 若 $b_n \neq 0$, 则 $b_n \in I_n = \langle r_n \rangle \Longrightarrow \exists x_n \in R$, s.t. $b_n = x_n r_n \Longrightarrow (b_1, \cdots, b_n) - x_n b_n = (\cdots, 0)$, 重复如上操作, 最终可将 $(b_1, \cdots, b_n)$ 用 $\{u_1, \cdots, u_n\}$ 表示.
故得证. □

定理 6.4 (课本定理6.6): R 为 PID, $M \in R-\text{mod}$ 有限生成,
M 自由 $\Longleftrightarrow M$ 无挠.

证: "$\Longrightarrow$": 设 $M = \langle\langle v_1, \cdots, v_n\rangle\rangle$ 且 $\{v_1, \cdots, v_n\}$ 线性无关.
$\forall v \in V$, $v = \sum_{i=1}^{n} r_i v_i$,
若 $rv = 0$, 则 $r\left(\sum_{i=1}^{n} r_i v_i\right) = \sum_{i=1}^{n}(rr_i)v_i = 0$,
$\because \{v_1, \cdots, v_n\}$ 线性无关, $\therefore rr_1 = \cdots = rr_n = 0$,
$\because R$ 为整环 (无零因子), $\therefore$ 若 $r \neq 0$, 则 $r_1 = \cdots = r_n = 0 \Longrightarrow v = 0$, 故 M 无挠.

"$\Longleftarrow$": 取 $M = \langle\langle u_1, \cdots, u_m\rangle\rangle$,
无妨设 $u_1, \cdots, u_k$ 是其中最大的线性无关组, 即 $\forall i = k+1, \cdots, m$, $\{u_1, \cdots, u_k, u_i\}$ 线性相关
$\Longrightarrow \exists$ 不全为零的 $a_{i1}, \cdots, a_{ik}, a_i$, s.t. $a_{i1}u_1 + \cdots + a_{ik}u_k + a_i u_i = 0$,
显然 $a_i \neq 0$ (否则 $a_{i1}u_1 + \cdots + a_{ik}u_k = 0 \Longrightarrow a_{i1} = \cdots = a_{ik} = 0$, 矛盾) $\Longrightarrow a_i u_i = -(a_{i1}u_1 + \cdots + a_{ik}u_k)$.
令 $a = a_{k+1} \cdot \cdots \cdot a_m$, 则 $a \neq 0$,
$aM = \langle\langle au_1, \cdots, au_k, au_{k+1}, \cdots, au_m\rangle\rangle \subseteq \langle\langle u_1, \cdots, u_k\rangle\rangle$,
$\because \{u_1, \cdots, u_k\}$ 线性无关, $\therefore \langle\langle u_1, \cdots, u_k\rangle\rangle$ 是自由模,
$\because R$ 为 PID, 自由具有遗传性, $\therefore aM$ 自由. 构造映射 $\tau: M \to aM$, $v \mapsto av$.

(1) τ 线性.

(2) $\because M$ 无挠且 $a \neq 0$, $\therefore \ker\tau = \{v \in M \mid av = 0\} = \{0\}$.

(3) τ 满射.

故 τ 同构 $\Longrightarrow M$ 也自由.

综上, 得证. □

$\because M$ 自由, $\therefore M = \langle\langle v_1, \cdots, v_n\rangle\rangle$,
又 $\because \{v_1, \cdots, v_n\}$ 线性无关, $\therefore$ 对 $i \neq j$, $\langle\langle v_i\rangle\rangle \cap \langle\langle v_j\rangle\rangle = \{0\} \Longrightarrow M = \langle\langle v_1\rangle\rangle \oplus \cdots \oplus \langle\langle v_n\rangle\rangle$.

定理 6.5 (课本定理6.8): R 是 PID, $M \in R-\text{mod}$ 有限生成, 则 $M = M_{\text{free}} \oplus M_{\text{tor}}$, 其中 $M_{\text{free}} = \frac{M}{M_{\text{tor}}}$.

证: M_{tor} 为挠子模且 $\frac{M}{M_{\text{tor}}}$ 无挠.
$\because \Pi: M \to \frac{M}{M_{\text{tor}}}$, $u \to [u]$ 满同态且 M 有限生成, 由引理 6.1 得 $\frac{M}{M_{\text{tor}}}$ 有限生成.
又 $\because \frac{M}{M_{\text{tor}}}$ 无挠, $\therefore \frac{M}{M_{\text{tor}}}$ 自由.
取 $\frac{M}{M_{\text{tor}}} = \langle\langle [u_1], \cdots, [u_t]\rangle\rangle$, 其中 $\{u_1, \cdots, u_t\}$, 线性无关 (下证),

证: 若 $\sum_{i=1}^{t} r_i u_i = 0$, 则 $\Pi\left(\sum_{i=1}^{t} r_i u_i\right) = \sum_{i=1}^{t} r_i \Pi(u_i) = \sum_{i=1}^{t} r_i [u_i] = 0$,
又 $\because \{[u_1], \cdots, [u_t]\}$ 线性无关, $\therefore r_1 = \cdots = r_t = 0 \Longrightarrow \{u_1, \cdots, u_t\}$ 线性无关. □

故 $\langle\langle u_1, \cdots, u_t\rangle\rangle$ 为自由模, 记作 M_{free}.

确定了 M_{free} 和 M_{tor} 后, 下面来证 $M = M_{\text{free}} \oplus M_{\text{tor}}$:
$\forall v \in M$, $\Pi(v) = [v] \in \frac{M}{M_{\text{tor}}} = \langle\langle [u_1], \cdots, [u_t]\rangle\rangle \Longrightarrow \Pi(v) = [v] = \sum_{i=1}^{t} l_i [u_i]$.
令 $u = \sum_{i=1}^{t} l_i u_i \in M_{\text{free}}$, 则 $\tau(u) = \tau\left(\sum_{i=1}^{t} l_i u_i\right) = \sum_{i=1}^{t} l_i \Pi(u_i) = \sum_{i=1}^{t} l_i [u_i] = \Pi(v)$.
$\Pi(v-u) = \Pi(v) - \Pi(u) = 0 \Longrightarrow v - u \in \ker\Pi = M_{\text{tor}}$,
于是 $v = u + (v-u)$, 其中 $u \in M_{\text{free}}$, $v - u \in M_{\text{tor}} \Longrightarrow M = M_{\text{free}} + M_{\text{tor}}$.

取 $w \in M_{\text{free}} \cap M_{\text{tor}}$, 则 $w \in M_{\text{free}} \iff w = \sum_{i=1}^{t} \alpha_i u_i$,
且 $w \in M_{\text{tor}} \iff \Pi(w) = 0$
$\implies 0 = \Pi(w) = \Pi\left(\sum_{i=1}^{t} \alpha_i u_i\right) = \sum_{i=1}^{t} \alpha_t \Pi(u_i) \implies \alpha_1 = \cdots = \alpha_t = 0 \implies w = 0 \implies M_{\text{free}} \cap M_{\text{tor}} = \{0\}$.
综上, 得证. □

引理 6.1: $\tau : M \to N$ 满同态, 若 M 有限生成, 则 N 有限生成.

证: $\because \tau : M \to N$ 满同态, $\therefore \forall w \in N, \exists u \in M$, s.t. $w = \tau(u)$,
又 $\because M$ 有限生成, 设 $M = \langle\langle v_1, \cdots, v_k \rangle\rangle$, $\therefore u = \sum_{i=1}^{k} r_i u_i \implies \tau(u) = \tau\left(\sum_{i=1}^{k} r_i u_i\right) = \sum_{i=1}^{k} r_i \tau(u_i)$,
故 $N = \langle\langle \tau(u_1), \cdots, \tau(u_k) \rangle\rangle$, 即 N 有限生成. □

至此, $M_{\text{free}} = \langle\langle u_1, \cdots, u_t \rangle\rangle = \langle\langle u_1 \rangle\rangle \oplus \cdots \oplus \langle\langle u_t \rangle\rangle$ 已拆解到位. 那么能否以及如何继续拆解 M_{tor} 呢?

定理 6.6 (课本定理6.10): R 为 PID, $M \in R-\text{mod}$ 为挠模且 $\text{ann}(M) = \langle\langle \mu \rangle\rangle$, 其中 $\mu = up_1 e_1 \cdots p_m^{e_m}$, u 为单位, p_i 均不可约且互不相等, $e_i \in \mathbb{Z}^+$,
则 $M = M_{p_1} \oplus \cdots \oplus M_{p_m}$, 其中 $M_{p_i} = \{v \in M \mid p_i^{e_i} v = 0\}$ 是阶为 $p_i^{e_i}$ (即 $\text{ann}(M_{p_i}) = \langle p_i^{e_i} \rangle$) 的准素子模.

证: 不失一般性, 设 $\mu = pq$, p 与 q 互素, 要证 $M = M_p \oplus M_q$, 其中 $M_p = \{v \mid pv = 0\}$, $M_q = \{v \mid qv = 0\}$.
$\because p$ 与 q 互素, $\therefore \exists r, t \in R$, s.t. $rp + tq = 1$.
$\forall v \in M$, $v = 1v = (rp + tq)v = (rp)v + (tq)v$,
$q(rp)v = (qrp)v = (rpq)v = r(pq)v = r\mu v$,
又 $\because \langle\langle \mu \rangle\rangle$ 为零化子, $\therefore q(rpv) = r\mu v = 0 \implies rpv \in M_q$,
同理, $tqv \in M_p$, 故 $M = M_p + M_q$.
若 $v \in M_p \cap M_q$, 则 $v \in M_p \iff pv = 0$,
且 $v \in M_q \iff qv = 0$
$\implies v = 1v = (rp + tq)v = rpv + tqv = r0 + t0 = 0 + 0 = 0 \implies M_p = M_q = \{0\}$.
$\because M_p = \{v \mid pv = 0\}$, $\therefore \text{ann}(M_p) = \langle p \rangle$, 易推广得 $M_{p_i} = \langle p_i^{e_i} \rangle$.
综上, 得证. □

然后准子模能否进一步分解呢?

定理 6.7 (课本定理6.11): R 为 PID, $M \in R-\text{mod}$ 有限生成, $\text{ann}(M) = \langle p^e \rangle$, 其中 p 不可约, $e \in \mathbb{Z}^+$,
则 $M = \langle\langle v_1 \rangle\rangle \oplus \cdots \oplus \langle\langle v_n \rangle\rangle$, 其中 $\text{ann}(v_i) = \langle p^{e_i} \rangle$, 且 $e = e_1 \geq \cdots \geq e_n$.

证: (存在性证明) 不失一般性, 只需证 M 由两个生成元时, 定理成立, 即可由数学归纳法推广到一般情况.
设 $M = \langle\langle u_1, u_2 \rangle\rangle$ 且 $u_1, u_2 \neq 0$, $\text{ann}(M) = \{r \in R \mid rM = \{0\}\} = \langle p^e \rangle$.
$\because u_1 \in M$, $\therefore p^e u_1 = 0 \implies p^e \in \text{ann}(u_1)$,
同理, $p^e \in \text{ann}(u_2)$.
若 $\text{ann}(u_1) = \langle b_1 \rangle$, 则 $\because p$ 不可约, $\therefore b_1 \mid p^e \implies b_1 = p^{l_1}$, $l_1 \leq e$,
同理, 若 $\text{ann}(u_2) = \langle b_2 \rangle$, 则 $b_2 = p^{l_2}$, $l_2 \leq e$.
假设 $l_1 < e$, $l_2 < e$, 令 $l = \max\{l_1, l_2\}$, 则 $p^e \nmid p^l$ 且 $p^l \in \text{ann}(M)$, 与 $\text{ann}(M) = \langle p^e \rangle$ 矛盾, 故假设错误, l_1, l_2 中至少有一个 $= e$.
无妨设 $l_1 = e$ 即 $\text{ann}(u_1) = \langle p^e \rangle$.
$M = \langle\langle u_1, u_2 \rangle\rangle \implies M = \langle\langle u_1 \rangle\rangle + \langle\langle u_2 \rangle\rangle$,
若 $\langle\langle u_1 \rangle\rangle \cap \langle\langle u_2 \rangle\rangle = \{0\}$, 则 $M = \langle\langle u_1 \rangle\rangle \oplus \langle\langle u_2 \rangle\rangle$, 得证.

若 $\langle\langle u_1\rangle\rangle \cap \langle\langle u_2\rangle\rangle \neq \{0\}$, 则 $\exists 0 \neq r \in R$, s.t. $ru_2 \in \langle\langle u_1\rangle\rangle$.
取 R 的理想 $J = \{r \in R \mid ru_2 \in \langle\langle u_1\rangle\rangle\}$.
$\because R$ 为 PID, $\therefore J$ 由一个元素生成, 设 $J = \langle\langle t\rangle\rangle$.
$\because p^e u_2 = 0 \Longrightarrow p^e \in J$, $\therefore p^e \in J \Longrightarrow t \mid p^e$,
又 $\because p$ 不可约, $\therefore t = p^{e_2}$ 且 $e_2 \leq e$,
又 $\because J = \{r \in R \mid ru_2 \in \langle\langle u_1\rangle\rangle\} = \langle t\rangle$, $\therefore p^{e_2}u_2 \in \langle\langle u_1\rangle\rangle$, 即 $\exists\alpha \in R$, s.t. $p^{e_2}u_2 - \alpha u_1 = 0$
$\Longrightarrow p^{e-e_2}(p^{e_2}u_2 - \alpha u_1) = 0 \Longrightarrow p^e u_2 - p^{e-e_2}\alpha u_1 = 0$,
又 $\because p^e u_2 = 0$, $\therefore p^{e-e_2}\alpha u_1 = 0 \Longrightarrow p^{e-e_2}\alpha \in \operatorname{ann}(u_1)$,
又 $\because \operatorname{ann}(u_1) = \langle p^e\rangle$, $\therefore p^e \mid p^{e-e_2}\alpha \Longrightarrow p^{e_2} \mid \alpha \Longrightarrow \exists\beta \in R$, s.t. $\alpha = \beta p^{e_2}$,
回代到 $p^{e_2}u_2 - \alpha u_1 = 0$ 得 $p^{e_2}u_2 - p^{e_2}\beta u_1 = 0 \Longrightarrow p^{e_2}(u_2 - \beta u_1) = 0$.
令 $w = u_2 - \beta u_1$, 则 $M = \langle\langle u_1, w\rangle\rangle$, 且 $\langle\langle u_1\rangle\rangle \cap \langle\langle w\rangle\rangle = \{0\}$ (下证),

证: 设 $v \in \langle\langle u_1\rangle\rangle \cap \langle\langle w\rangle\rangle$, 则 $v \in \langle\langle u_1\rangle\rangle$,
且 $v \in \langle\langle w\rangle\rangle \Longrightarrow \exists r \in R$, $v = rw$
$\Longrightarrow v = rw = ru_2 - r\beta u_1 \in \langle\langle u_1\rangle\rangle$,
$\because r\beta u_1 \in \langle\langle u_1\rangle\rangle$, $\therefore ru_2 \in \langle\langle u_1\rangle\rangle$, (由 J 的定义) 即 $r = p^{e_2}r_1$,
回代得 $v = rw = p^{e_2}r_1u_2 - p^{e_2}r\beta u_1 = p^{e_2}r_1u_2 - p^{e_2}r_1\beta u_1 = p^{e_2}r_1u_2 - r_1(\beta p^{e_2})u_1 = r_2(p^{e_2}u_2 - \alpha u_1) = r_2 0 = 0 \Longrightarrow$
$\langle\langle u_1\rangle\rangle \cap \langle\langle w\rangle\rangle = \{0\}$. □

故 $M = \langle\langle u_1\rangle\rangle \oplus \langle\langle w\rangle\rangle$, 其中 u_1 的阶为 p^{e_1}, w 的阶为 p^{e_2}, $e_2 \leq e_1 = e$. □

总结定理 6.5, 6.6 和 6.7, 可得:

定理 6.8 (课本定理6.12): R 为 PID, $M \in R-\mathrm{mod}$ 有限生成,
则 $M = M_{\text{free}} \oplus M_{\text{tor}}$, 其中 $M_{\text{free}} = \frac{M}{M_{\text{tor}}}$.
若 $\operatorname{ann}(M_{\text{tor}}) = \langle\mu\rangle$, 其中 $\mu = up_1^{e_1}\cdots p_n^{e_n}$, u 为单位, p_i 不可约且互不相等, $e_i \in \mathbb{Z}^+$,
则 $M_{\text{tor}} = M_{p_1} \oplus \cdots \oplus M_{p_n}$, 其中 $M_{p_i} = \{v \in M_{\text{tor}} \mid p_i(v) = 0\}$ 即 $\operatorname{ann}(M_{p_i}) = \langle p_i^{e_i}\rangle$,
$M_{p_i} = \langle\langle v_i\rangle\rangle \oplus \cdots \langle\langle v_{it_i}\rangle\rangle$, 其中 $\operatorname{ann}(v_{ij}) = \langle p_i^{e_{ij}}\rangle$, $e_i = e_{i1} \geq \cdots \geq e_{it_i}$.

$$\text{故 } M = \overbrace{\left(\bigoplus_{i=1}^{m}\langle\langle u_i\rangle\rangle\right)}^{M_{\text{free}}} \oplus \overbrace{\left[\bigoplus_{i=1}^{n}\overbrace{\left(\bigoplus_{j=1}^{t_i}\langle\langle v_{ij}\rangle\rangle\right)}^{M_{p_i}}\right]}^{M_{\text{tor}}}.$$