高等线性代数 笔记

Advanced Linear Algebra
PHYS6653P
2021 学年第一学期

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

目录

Chapter 1

代数学基础

1.1 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.

1.2 集合

定义 1.1 集合(Set):

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

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

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

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

综上, 得证. □

常用公式:

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

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

$\forall a \in \cup_i (A \cap B_i) \iff \exists k$, s.t. $a \in A \cap B_k$
$\iff \exists k$, s.t. $a \in A$ 且 $a \in B_k$
$\iff a \in A$ 且 $\exists k$, s.t. $a \in B_k$
$\iff a \in A$ 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: $\forall a \in A \cup (\cap_i B_i) \iff a \in A$ 或 $a \in \cap_i B_i$
$\iff a \in A$ 或 $\forall i$, s.t. $a \in B_i$
$\iff \forall i$, $a \in A$ 或 $a \in B_k$
$\iff \forall i$, $a \in A \cup B_k$
$\iff \cap_i (A \cup B_i)$, 故 $A \cup (\cap_i B_i) \subseteq \cap_i (A \cup B_i)$.

$\forall a \in \cap_i (A \cup B_i) \iff \forall i$, $a \in A \cup B_i$
$\iff \forall i$, $a \in A$ 或 $a \in B_i$
$\iff a \in A$ 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. □

1.3 映射

定义 1.2 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 1.1 恒等映射: $1_S : S \to S$, $a \mapsto 1_S(a) = a$. □

定义 1.3 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 1.4 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 1.5 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 $\cap_i f^{-1}(B_i) \subseteq f^{-1}(\cap_i B_i)$.

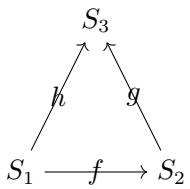
综上, 得证. □

定义 1.6 映射的复合: 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.

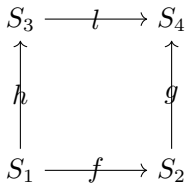
定理 1.1 映射复合的结合律: $h \circ (g \circ f) = (h \circ g) \circ f$.

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

定义 1.7 交换图: $f : S_1 \to S_1$, $h : S_2 \to S_3$, $g : S_1 \to S_3$, 若 $g = f \circ h$, 则称该图交换.



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



定义 1.8 单射(Injective 或One-to-one): 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 1.9 满射(Surjective): 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 1.10 双射: 映射 f 单射且满射 $\Longleftrightarrow f$ 双射.

例 1.2: 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 1.3 $g \circ f$ **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 1.4 $g \circ f$ **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 1.2: 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 1.3: 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 1.4: 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 1.2 和 1.3 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, $g = h$. □

1.4 等价关系和等价类

定义 1.11 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 1.12 关系: 卡氏积的子集. $\mathcal{R} \in S \times S$, 称为 S 上的关系.

例 1.5: 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 1.13 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 1.14 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, 记为 $a \sim b$.

定义 1.15 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 1.16 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 的一个剖分.

可由集合的等价类得到它的一个剖分.

定义 1.17 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 1.18 运算: 映射 $* : S \times S \to S$ 称为 S 上的一个运算, 记为 $(S, *)$.

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

1.5 群

定义 1.19 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, 记为 $b = a^{-1}$

则称 $(G, *)$ 为一个群.

定理 1.5: 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 1.6: 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 1.6: $(\mathbb{Z}, \times)$ 非群, 因 0 无逆元. □

特殊的群:

(1)

例 1.7 循环群: $G = \{a^i \mid i \in \mathbb{Z}\}$. □

(2)

例 1.8 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 1.20 群的阶: $|G| \equiv$ 群中元素的个数.

定义 1.21 有限群: 若 $|G| < \infty$, 则称 G 为有限群.

定义 1.22 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, 记为 $|g|$, 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 1.23 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, 记为 $(H, *) < (G, *)$.

例 1.9: $(\mathbb{Q}, +)$ 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 1.7: $(H, *) < (G, *) \Longleftrightarrow H \subseteq G,\ \forall a, b \in H,\ a * b \in H$ 且 $a^{-1} \in H \Longleftrightarrow H \subseteq G,\ \forall a, b \in H,\ a * b^{-1} = H$.

证: $\underline{(H,*)<(G,*) \Longleftrightarrow H\subseteq G,\forall a,b\in H,\ a*b\in H\ 且a^{-1}\in H}$: 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 1.24 <u>平凡子群</u>: $(G,*)$ 和 $(\{e\},*)$ 为 $(G,*)$ 的平凡子群.

定义 1.25 <u>真子群(非平凡子群)</u>: 除平凡子群以外的子群.

定义 1.26 <u>单群</u>: 无真子群的群.

定理 1.8 <u>任意多个子群的交为子群</u>: $(G,*)$ 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 1.9: $(H,*)<(G,*)$, 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 1.10: $(\mathbb{Z},+)$ 为群, $(\mathbb{E}=\langle 2\rangle=\equiv\{vp\},+),(\langle 3\rangle\equiv\{3n\mid n\in\mathbb{Z}\},+)<(\mathbb{Z},+)$. □

定义 1.27 <u>陪集(Coset)</u>: 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 1.11: $\mathbb{E}$ 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 $c\in g_2H$

$\Longleftrightarrow\exists h_1,h_2,\text{ s.t. }c=g_1*h_1=g_2*h_2$

$\Longrightarrow g_2^{-1}g_1=h_2*h_1^{-1}$

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 1.10 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 1.12: 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 1.28 商群: H 为 G 的正规子群, $\frac{G}{H} = \{[g] \equiv gH \mid g \in G\}$.

问题 1.1: $\frac{G}{H}$ 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 1.11 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 1.12: 交换群的任意一个子群为正规子群.

例 1.13: $(\mathbb{Z}, +)$ 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 1.29 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 1.30 单同态: 单射的群同态.

定义 1.31 满同态: 满射的群同态.

定义 1.32 同构: 双射的群同态.

定理 1.13: 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 1.14: 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 1.33 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 $\operatorname{Ker} f \equiv f^{-1}(e_2) = \{a \in G_1 \mid f(a) = e_2\}$ 为 f 的核.

$\because e_1 \in \operatorname{Ker} f, \therefore \operatorname{Ker} f \neq \emptyset$.
$\operatorname{Ker} f \subseteq G_1$.

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

定义 1.34 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 1.15: f 单同态 $\iff \operatorname{Ker} f = \{e_1\}$.

证: "$\Longrightarrow$": $\forall a, b \in \operatorname{Ker} f$, $f(a) = f(b) = e_2$,
又 $\because f$ 单同态, $\therefore a = b = e$.
"$\Longrightarrow$": 若 $f(a) = f(b)$, 则 $f(a) \circ [f(b)]^{-1} = e_2$
$\Longrightarrow f(a) \circ f(b^{-1}) = e_2$
$\Longrightarrow f(a * b^{-1}) = e_2$
$\Longrightarrow a * b^{-1} \in \operatorname{Ker} f = \{e_1\}$
$\Longrightarrow a = b = e_1$, 故 f 单同态. □

1.6 环

定义 1.35 环: 若 $(R, +, \cdot)$ 满足
$(R, +)$ 为交换群 (单位元记作 0)

(1) **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 1.14: $(\mathbb{Z}, +, \times)$ 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) $(\sum_i a_i) \cdot \left(\sum_j b_j\right) = \sum_{i,j} a_i \cdot b_j$.

证: 由左右分配律即得证. □

特殊的环:

(1)

定义 1.36 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 1.37 有单位元的环: 若 $\exists 1$, 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 1.15: $(\mathbb{Z}, +, \cdot)$ 交换且有单位元. □

例 1.16: $(M_{n\times n}, +, \times)$ [1] 非交换, 有单位元 $I_{n\times n}$. □

例 1.17: $(\mathbb{E}, +, \times)$ 交换, 无单位元. □

定义 1.38 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.

定义 1.39 整环: 有单位元, 交换, 无零因子的环.

定义 1.40 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 1.16 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 1.17: 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: "$\Longrightarrow$": $r \cdot a = r \cdot b \iff r \cdot (a - b) = r \cdot a - r \cdot b = r \cdot b - r \cdot b = 0$,
$\because r \neq 0$ 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 1.41 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 1.42 平凡理想: $(\{0\}, +, \cdot)$ 和 $(R, +, \cdot)$ 为 $(R, +, \cdot)$ 的平凡理想.

定义 1.43 单环: 只有平凡理想的环.

定理 1.18: 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. □

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

定理 1.19: 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 1.44 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 1.45 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 1.46 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 1.47 核: $\operatorname{Ker} f \equiv \{a \in R_1 \mid f(a) = 0\}$.

定义 1.48 像: $\operatorname{Im} f \equiv \{f(a) \mid a \in R_1\}$.

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

定理 1.20: $\operatorname{Ker} f$ 为理想.

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

综上, $\operatorname{Ker} f$ 为 R_1 的理想. □

定义 1.49 单同态: 单射的环同态.

单同态 $\Longleftrightarrow \operatorname{Ker} f = \{0\}$.

定义 1.50 满同态: 满射的环同态.

满同态 $\Longleftrightarrow \operatorname{Im} f = R_2$.

定义 1.51 同构: 双射的环同态.

定义 1.52 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 1.18: $(\mathbb{Z}, +, \cdot)$ 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 $0 \leq r < n$.
若 $r \neq 0$, 则 $r = p - kn \in I$, 但 $0 \leq r < n$ 而 n 为 $\langle n \rangle$ 中最小的正整数矛盾, 故 $r = 0$, $p = kn$. □

定义 1.53 剩余类环: $\mathbb{Z}_n \equiv \frac{\mathbb{Z}}{\langle n \rangle} = \{[0], [1], \cdots, [n-1]\}$.

例 1.19: $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$, $[2] \cdot [3] = [6] = [0]$, 故 $\mathbb{Z}_6$ 有零因子. □

1.7 域

定义 1.54 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, $|F|\geq 2$. 当 $|F|=2$ 时, $F=\{0,1\}\cong\mathbb{Z}_2=\frac{\mathbb{Z}}{\langle 2\rangle}$.

例 1.20: $\mathbb{Z}_2$ 是最小的有限域. $\mathbb{Q}$ 为最小的无限域. □

定义 1.55 有理数: $\mathbb{Q}=\left\{\frac{m}{n}\mid n\neq 0,n,m\in\mathbb{Z}\right\}$, 即 $\forall q\in\mathbb{Q},\exists m,n\in\mathbb{Z},n\neq 0,q=\frac{m}{n}$.

定义 1.56 域的特征: $\operatorname{char}F\equiv$ 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 1.21: $\operatorname{char}\mathbb{Z}_2=2,\ \operatorname{char}\mathbb{Q}=0.$ □

$p=\operatorname{char}F$ 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 1.57 域同态: $(F_1,+,\cdot)$ 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 $\operatorname{Ker}f=\{0\}$, 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 $\forall r\neq 0$, $f(r)\neq 0$, $\operatorname{Ker}f=\{0\}$. □

Chapter 2

向量空间

定义 2.1 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 $(r\cdot t)\cdot u=r(tu)$)

(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 2.1 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 2.2: $\mathbb{R}^2$ 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 2.3: $F^n \equiv \{(r_1,\cdots,r_n) \mid r_i \in F\}$, 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 2.2 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 2.1 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 2.3 生成子空间: $\emptyset\neq S\subseteq V$, $\langle S\rangle\equiv$ 包含 S 的最小子空间 $=\{\sum_{i=1}^n r_iu_i \mid r_i\in F, u_i\in S, n\in\mathbb{N}\}$, 其中称 S 为生成集.

例 2.4: 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 2.4 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 2.5: $(1,0)$ 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 2.6: $\mathbb{R}^2$ 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 2.5 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 2.6 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 2.2 (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 2.3 (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 2.2 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 2.7 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 2.4 (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 2.7: $e_1 = (1, 0, \cdots, 0)$, $e_2 = (0, 1, \cdots, 0)$, $\cdots$, $e_n = (0, 0, \cdots, 1)$ 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 $\langle \{e_1, \cdots, e_n\} \rangle = \{r_1 e_1 + \cdots + r_n e_n = (r_1, \cdots, r_n) \mid r_i \in F, \text{ 对 } i = 1, \cdots, n\} = F$, 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 2.5 (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 2.8 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 2.8: $\mathbb{R}^2=S_x\oplus S_y$. □

定理 2.6 (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 2.7 (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, $\therefore V=\langle\mathcal{B}\rangle=\langle v_1,\cdots,v_n\rangle=\{\sum_{i=1}^n r_iv_i\mid r_i\in F\}=\langle v_1\rangle+\cdots+\langle v_n\rangle$.
$\because\mathcal{B}$ 为 V 的基, $\therefore v_1,\cdots,v_n$ 线性无关 $\Longrightarrow\forall 0\neq u\in\langle v_i\rangle$, $u=r_iv_i$ 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, (线性无关的证明存疑), $\Longrightarrow v_1,\cdots,v_n$ 线性无关.
故 $\mathcal{B}=\{v_1,\cdots,v_n\}$ 是 V 的基. □

定理 2.8 (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 2.9: $\mathbb{R}^2 = S_x \oplus S_y = S_l \oplus S_{l'}$, 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 2.9 (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 $v_1, \cdots, v_k \in \mathcal{B}_1$, $v_{k+1}, \cdots, v_k \in \mathcal{B}_2 \Longrightarrow V = \langle \mathcal{B}_1 \rangle + \langle \mathcal{B}_2 \rangle$.
$\forall u \in \langle \mathcal{B}_1 \rangle \cap \langle \mathcal{B}_2 \rangle$,$u \in \langle \mathcal{B}_1 \rangle \Longrightarrow u = \sum_{i=1}^{n} r_i v_i$, 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 2.10 (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 3

线性变换

3.1 线性变换

定义 3.1 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 3.2 单线性变换: 单射的线性变换.

定义 3.3 满线性变换: 满射的线性变换.

定义 3.4 同构: 双射的线性变换.

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, $\because v \overset{\tau}{\mapsto} \tau(v)$ 是唯一的, $v \overset{\sigma}{\mapsto} \sigma(v)$ 是唯一的, $\therefore v \overset{\tau+\sigma}{\mapsto} \tau(v) + \sigma(v)$ 是唯一的, 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 3.1 (课本定理2.1): (1) $\mathcal{L}(V,W)$ 是 F 上的向量空间.

(2) $t \in \mathcal{L}(V,W)$, $\sigma \in \mathcal{L}(W,U)$, 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一样的, 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 3.5 核空间: $\operatorname{Ker}\tau \equiv \{v \mid \tau(v) = 0\} \subseteq V$.

定义 3.6 像空间: $\operatorname{Im}\tau \equiv \{\tau(v) \mid v \in V\}$.

定理 3.2 (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 $\iff \operatorname{Ker}\tau = \{0\}$.

定理 3.3 (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 3.4 (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, $\therefore \operatorname{Ker}\tau = \{0\} \implies \sum_i r_i s_i = 0$,
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 3.5 (课本定理2.6): $V \approx W \iff \dim V = \dim W$.

定理 3.6 (课本定理2.7): 若 $\dim V = n$, 则 $V \approx F^n$.

定理 3.7 (课本定理2.8): $\tau \in (L)(V,W)$,

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

(2) $\dim V = \dim \operatorname{Ker}\tau + \dim \operatorname{Im}\tau \equiv \operatorname{null}\tau + \operatorname{rk}\tau$, 其中称 $\operatorname{null}\tau \equiv \dim \operatorname{Ker}\tau$ 为 τ 的零度, $\operatorname{rk}\tau \equiv \dim \operatorname{Im}\tau$ 为 τ 的秩.

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

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

又 $\because V = \operatorname{Ker}(\tau) \oplus \operatorname{Ker}(\tau)^c$, $\therefore \operatorname{Ker}(\tau) \cap \operatorname{Ker}(\tau)^c = \{0\} \Longrightarrow \operatorname{Ker}(\tau^c) = \{0\}$, 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 $u \in \operatorname{Ker}(\tau)$, $w \in \operatorname{Ker}(\tau)^c \Longrightarrow \tau(v) = \tau(u+w) = \tau(u) + \tau(w) = 0 + \tau(w) = \tau(w) \in \operatorname{Im}(\tau^c) \Longrightarrow \operatorname{Im}(\tau) \subseteq \operatorname{Im}(\tau^c)$.

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

综上, (1) 得证.

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

□

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

3.2 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 3.4, 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.

证: $\{b_1, \cdots, b_n\}$ 为 V 的基, 线性变换 $\tau \in \mathcal{L}(V, W)$, 若已知 $\tau(b_i) \forall i$, 则 $\forall v \in V$, $v = \sum_{i=1}^n r_i b_i \Longrightarrow \tau(v) = \tau\left(\sum_{i=1}^n r_i b_i\right) = \sum_{i=1}^n r_i \tau(b_i)$ 可以确定, 由此 τ 可以确定. □

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.

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

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: $\operatorname{Ker}f\equiv\{\tau\mid f(\tau)=0\}=\{\tau\mid M_\tau=0\}$.

$\forall\tau\in\operatorname{Ker}f,\forall\vec{r}\in F^n,\tau(\vec{r})=M_\tau\vec{r}=\vec{0}\Longrightarrow M_\tau=0_{m\times n}\Longrightarrow\tau=0.$

故 $\operatorname{Ker}f=\{0\}$ (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 $\mathcal{B}=\{b_1,\cdots,b_n\}$, $\forall v\in V$, $v=\sum_i r_ib_i$.

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 $v=\sum_i r_ib_i$ 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.

$\forall u,v\in V$, $u=\sum_{i=1}^n w_ib_i$, $v=\sum_{i=1}^n r_ib_i$,

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

故 ϕ_B 为 V 到 F^n 的线性变换. □

$\phi_\mathcal{B}$ 单射.

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

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

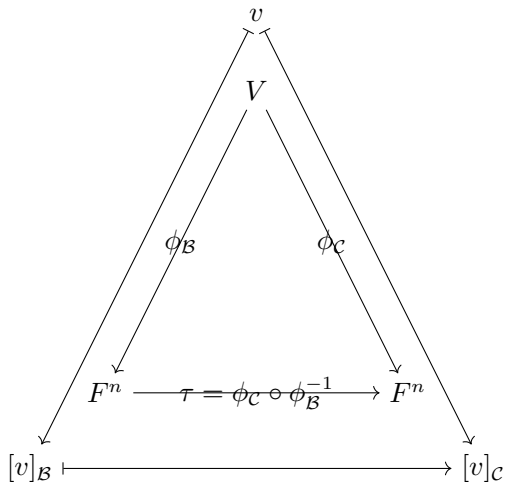
故 $\operatorname{Ker}\phi_\mathcal{B}=\{0\}\Longleftrightarrow\phi_\mathcal{B}$ 单射. □

$\phi_{\mathcal{B}}$ 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. □

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?

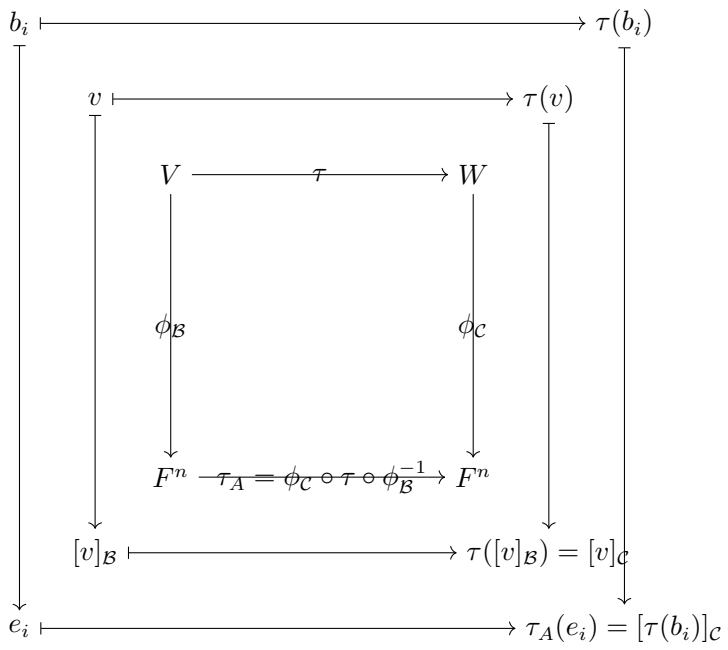


$[v]_{\mathcal{C}} = \tau([v]_{\mathcal{B}}) = M_\tau [v]_{\mathcal{B}}$, 其中 $M_\tau = \begin{pmatrix} \tau(e_1) & \cdots & \tau(e_n) \end{pmatrix}$.
$\tau : F^n \to F^n, \quad e_i \mapsto \tau(e_i) = \phi_{\mathcal{C}}(\phi_{\mathcal{B}}^{-1}(e_i)) = \phi_{\mathcal{C}}(b_i)$,
$M_\tau = \begin{pmatrix}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

定理 3.8 (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.



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

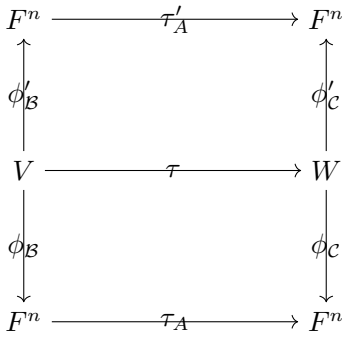
定理 3.9 (课本定理2.14):

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

其中 $[\tau(v)]_{\mathcal{C}}$ 是 $\tau(v)$ 在基 $\mathcal{C}$ 的表象下的坐标表示, $[\tau(v)]_{\mathcal{BC}}$ 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 3.10 (课本定理2.15): $\mathcal{L}(V,W) \to \mathcal{L}(F^n, F^m) \approx M_{m\times n}(F)$, $\tau \mapsto \tau_A \mapsto [\tau]_{\mathcal{BC}}$.

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?



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

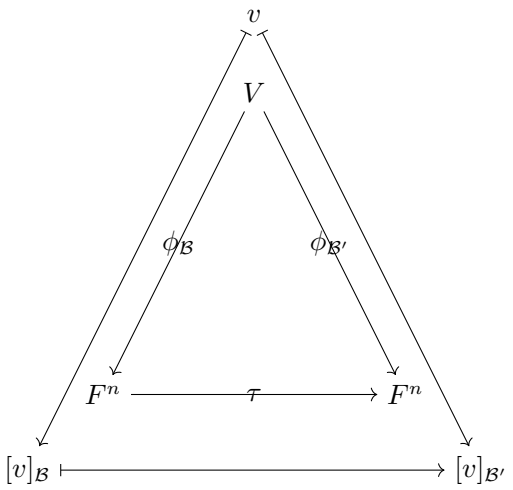
定理 3.11 (课本定理2.16):

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

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



$M_{\mathcal{B}\mathcal{B}'} = M_\tau = \begin{pmatrix} [b_1]_{\mathcal{B}'} & \cdots & [b_n]_{\mathcal{B}'} \end{pmatrix}$, 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 3.12 (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 3.13 (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.)