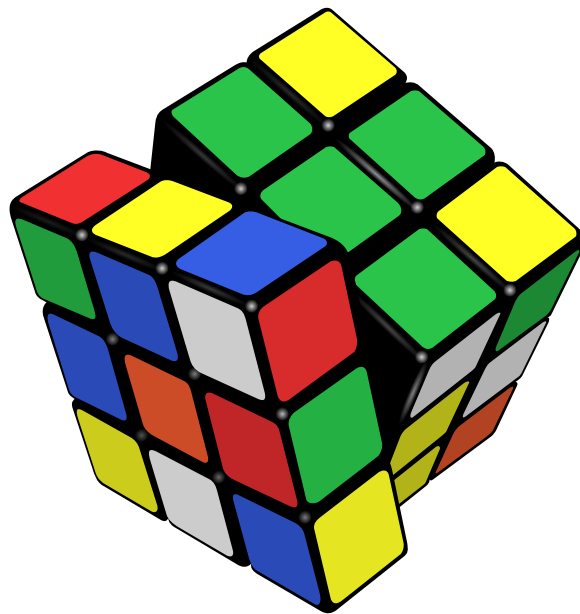


# Algebra

Hoyan Mok<sup>1</sup>

2020 年 10 月 5 日



<sup>1</sup>E-mail: [victoriesmo@hotmail.com](mailto:victoriesmo@hotmail.com)



# 笔记说明

本笔记是笔者学习线性代数时的教材, 主要参考资料是 [2].

笔记假定读者已经熟悉朴素集合论的术语与符号, 并已经学习了以矩阵和行列式运算为主的初级线性代数. 但本笔记力求自足, 将矩阵与行列式运算, 置换和多项式等内容附在附录中, 以资读者在阅读正文时可以随时查阅.

笔记后附有符号列表和索引, 方便读者 (也是方便笔者自己) 查阅.

你可以在<https://github.com/HoyanMok/NotesOnMathematics/tree/master/Algebra>获得本笔记最新的 PDF 与  $\text{\TeX}$  源文档. 封面的来源是[https://commons.wikimedia.org/wiki/File:Rubik%27s\\_cube.svg](https://commons.wikimedia.org/wiki/File:Rubik%27s_cube.svg).

# 目录

笔记说明	i
目录	ii
第一部分 线性代数	1
第一章 群. 环. 域	2
§1 代数运算	2
§2 群	3
§3 环	7
§4 域	12
第二章 线性空间	14
§5 线性空间	14
§6 对偶空间	19
§7 多重线性型	22
§8 二次型	24
第三章 线性算子	25
§9 线性映射	25
§10 线性算子代数	26
§11 不变子空间与特征向量	29
第四章 内积空间	33
第五章 张量	34

目录	iii
附录 A 置换	35
§1 置换群	35
附录 B 矩阵和行列式	38
§2 矩阵	38
§3 行列式	40
附录 C 多项式	42
§4 多项式环	42
§5 整多项式环	43
§6 多项式的根	44
参考文献	45
符号列表	46
索引	48



# 第一部分

## 线性代数

# 第一章 群. 环. 域

## §1 代数运算

**Definition 1.1** (二元运算). 集合的 Cartesian 平方到自身的映射  $*$ :  $X^2 \rightarrow X$  称为其上的一个二元运算. 通常我们记  $*(a, b) := a * b$ . 当  $X$  上定义了二元运算  $*$  后, 称  $*$  定义了  $X$  上的一种代数结构  $(X, *)$ , 也称代数系统.

当指代是明确的时候, 我们将混用集合及其代数结构.

作为习惯, 如果  $\cdot, + \in X^{X^2}$ , 我们记  $ab := a \cdot b$  并称其为  $a$  和  $b$  的积, 称  $a + b$  为  $a$  和  $b$  的和. 这些只是约定.

若  $a * b = b * a$  则称  $*$  或  $(X, *)$  是交换的, 而若  $(a * b) * c = a * (b * c)$  则称  $*$  或  $(X, *)$  为结合的.

若  $\exists e \in X$  满足  $\forall x \in A (e * x = x * e = x)$ , 则称其为  $*$  的一个单位元 (identity), 这时可把  $(X, *)$  记作  $(X, *, e)$ . 可以证明一个代数结构最多只有一个单位元. 乘法单位元通常记为 1, 而加法单位元 (也叫零元) 记为 0.

**Definition 1.2** (半群和么半群). 若  $*$  是结合的, 称  $(X, *)$  是半群 (semigroup); 若  $*$  还有一个单位元, 则称  $(X, *, e)$  是么半群 (monoid).

倘若么半群  $(M, *, e)$  是有限的 (即其元素有限), 称  $\text{card } M$  为有限么半群的阶.

作为重要的例子, 置换么半群定义为  $(X^X, \circ, \text{id}_X)$ , 有么半群结构的  $X^X$  通常记作  $M(X)$ . 半群中, 括号的位置是不重要的 (可用数学归纳法证明). 通常我们记  $x_1 x_2 \cdots x_n$  为:

$$\prod_{i=1}^1 x_i = x_1, \prod_{i=1}^{n+1} x_i = \left( \prod_{i=1}^n x_i \right) x_n; \quad (1-1)$$

同理  $x_1 + x_2 + \cdots + x_n$  为:

$$\sum_{i=1}^1 x_i = x_1, \sum_{i=1}^{n+1} x_i = \left( \sum_{i=1}^n x_i \right) + x_n. \quad (1-2)$$



在半群不交换的场合, 指出递推式右端的顺序是重要的. 这种记法称为**左正规**.

若  $x := x_1 = x_2 = \cdots = x_n$ , 记  $\sum_{i=1}^n x_i = nx$ ,  $\prod_{i=1}^n x_i = x^n$ , 分别表示  $x$  的  $n$  倍和  $x$  的  $n$  次幂. 它们满足:

$$nx + mx = (n + m)x, \quad n(mx) = nm x, \quad n, m \in \mathbb{N}_+; \quad (1-3)$$

$$x^n x^m = x^{n+m}, \quad (x^m)^n = x^{nm}, \quad n, m \in \mathbb{N}_+. \quad (1-4)$$

在么半群中, 还可以令  $x^0 = 1, 0x = 0$ .

若半群  $S$  有子集  $S'$ , 使得  $(S', *)$  是半群, 那么称其为半群  $(S, *)$  的**子半群**. 同理有么半群  $M$  的**子么半群**  $M'$ .

若半群  $(S, *, e)$  的元素  $a$  满足  $\exists a' \in S (aa' = a'a = e)$ , 那么称  $a$  为**可逆的** (invertible),  $a'$  称为其**逆元** (inverse element) 或**逆** (inverse). 通常加法逆元记为  $-a$ , 乘法逆元记为  $a^{-1}$ , 且为可逆元素引入  $na, a^n$  的概念, 其中  $n \in \mathbb{Z}$ . 当  $n$  为负数时,  $na = -(-na), a^n = (a^{-n})^{-1}$ .

因为群未必是 Abelian, 我们可以也用弱化的**左可逆**  $\exists y \text{ s.t. } y * x = 1$  或**右可逆**的概念.

## §2 群

可逆么半群  $G$  称为**群**, 即:

**Definition 2.1** (群). 设有集合  $G$ . 若:

- G1) 定义了二元运算  $\cdot: G^2 \rightarrow G; (x, y) \mapsto xy$ .
- G2) 结合性:  $\forall x, y, z \in G, (xy)z = x(yz)$ .
- G3) 单位元:  $\exists e \in G \forall x \in G, xe = ex = x$ .
- G4) 可逆性:  $\forall x \in G \exists x^{-1} \in G, xx^{-1} = x^{-1}x = e$ .

则称  $(G, \cdot)$  为**群**.

交换群又叫做 **Abelian 群**.

作为重要的例子, 设  $X$  是一个集合,  $S(X) = \{f \in X^X \mid f \text{ 是双射}\}$ . 我们断言,  $(S(X), \circ, \text{id}_X)$  是一个群, 称为**变换群**或**置换群**, 其中  $\circ$  是函数的复合,  $\text{id}_X$  是恒等变换. 当它的阶数  $\text{card } X = n$  是有限的时候, 记  $S_n := S(X)$ .

群也有子群的概念. 设  $(G, \cdot, e)$  是一个群. 当一个集合  $G' \subset G$  满足:

- SG1)  $e \in G'$ ;
- SG2)  $\forall x, y \in G', xy \in G'$ ;
- SG3)  $x \in G' \rightarrow x^{-1} \in G'$ ,

则称  $(G', \cdot, e)$  是一个  $G$  的**子群**. 倘若还有  $G' \neq G$  则称其为一个**真子群**<sup>1</sup>.

<sup>1</sup>[1] 等文献把平凡群  $\{e\}$  也排在真子群的定义外.

**Theorem 2.1.** 非空的  $G'$  是群  $(G, \cdot, 1)$  的子群  $\leftrightarrow \forall x, y \in G' (xy^{-1} \in G')$ .

**Proof.** 根据子群的定义,  $\rightarrow$  是显然的, 下给出  $\leftarrow$  的证明:

$$\text{SG1)} \quad \forall x \in G' (xx^{-1} = 1 \in G');$$

$$\text{SG2)} \quad \forall x, y \in G', x1^{-1}1y^{-1-1} = xy \in G';$$

$$\text{SG3)} \quad \forall x \in G', 1x^{-1} = x^{-1} \in G'.$$

□

这里将不加证明地给出:

**Lemma 1.** 群  $G$  的子群族  $\mathcal{H} = \{H \mid H \text{ 是 } G \text{ 的子群}\}$  的交  $\cap \mathcal{H}$  也是  $G$  的子群.

设  $G$  有子集  $S$ , 我们说群  $(G, \cdot, 1)$  是由  $S$  生成的, 意思是说  $G$  没有包含  $S$  的真子群. 记为  $G = \langle S \rangle$ .

**Theorem 2.2.**  $\langle S \rangle = \left\{ \prod_{i=0}^{n-1} s_i \mid \forall i \in n (s_i \in S \vee s_i^{-1} \in S) \right\}$ .

**Proof.** 根据群的定义, 形如  $\prod_{i=0}^{n-1} s_i$  的将构成一个群. 如果存在一个不能写成这种形式的元素, 那么它们将构成一个真子群, 这和  $\langle S \rangle$  的定义相违背.

□

我们把半群的公式 (1-4) 推广到整数次幂, 证明在此忽略了.

**Theorem 2.3.**  $\forall g \in G, \forall n, m \in \mathbb{Z}$ ,

$$g^m g^n = g^{m+n}, \quad (g^m)^n = g^{mn}. \quad (2-1)$$

**Definition 2.2** (循环群). 设  $(G, \cdot, 1)$  是一个乘法群,  $\exists g_0 \in G$ , 使得  $\forall g \in G, \exists n \in \mathbb{Z}, a^n = g$ , 那么我们称它是一个循环群,  $g_0$  是一个生成元 (generator), 并记作  $G = \langle g_0 \rangle$ .

对于群  $G$  中任意元素  $g$ , 我们称  $\text{card}\langle g \rangle$  为元  $g$  的阶数, 或称  $g$  为  $n$  阶元. 而且它将满足:

**Theorem 2.4.** 任意群  $G$  中若有  $q \in \mathbb{Z}$  阶元  $g$ , 则  $\langle g \rangle = \{e, g, \dots, g^{q-1}\}$ , 且:

$$g^n = e \leftrightarrow n = kq, \quad n \in \mathbb{Z}. \quad (2-2)$$

证明利用带余除法和定理 2.3, 证明是显然的. 从该定理, 我们可以论断: 循环群都是 Abelian 群.

**Definition 2.3** (同构). 两个群  $(G, *)$ ,  $(G', \circ)$  如若满足:  $\exists f: G \rightarrow G'$  s.t.

$$\text{i)} \quad \forall a, b \in G, f(a * b) = f(a) \circ f(b);$$

ii)  $f$  是双射,

则称  $f$  是一个**同构映射**或**同构** (isomorphism), 并认为两个群是互**相同构**的 (isomorphic), 记为  $G \simeq G'$ .

同构关系的自反性, 传递性和对称性是平凡的.

**Theorem 2.5.** 设群  $(G, *, 1), (G', \circ, 1')$  被  $f$  见证同构, 那么  $f(1) = 1'$ .

**Proof.**  $\forall g' \in G'$ , 记  $g := f^{-1}(g')$ , 那么  $f(g) \circ f(1) = f(g * 1) = g' = f(1 * g) = f(1) \circ f(g)$ . 从而  $f(1) = 1'$ .  $\square$

**Theorem 2.6.** 设群  $(G, *, 1), (G', \circ, 1')$  被  $f$  见证同构, 那么  $\forall g \in G, f(g^{-1}) = f(g)^{-1}$ .

**Proof.**  $f(g) \circ f(g^{-1}) = f(g * g^{-1}) = f(1) = 1' = f(g^{-1} * g) = f(g^{-1}) \circ f(g)$ .  $\square$

**Theorem 2.7.**

$$\text{card}\langle g_0 \rangle = \text{card}\langle g'_0 \rangle \rightarrow \langle g_0 \rangle \simeq \langle g'_0 \rangle.$$

**Proof.** 倘若  $\text{card}\langle g_0 \rangle = \infty$ , 那么  $\nexists n \in \mathbb{Z} - \{0\}$ , s.t.  $g_0^n = e$ ; 这意味着, 存在这样的双射  $f: \mathbb{Z} \rightarrow \langle g_0 \rangle$ , 满足  $f(n) = g_0^n$ , 见证了  $(\mathbb{Z}, +, 0) \simeq (\langle g_0 \rangle, *, e)$ .

如果阶数是有限的, 只需令  $f: g^k \rightarrow g'^k$ , 其中  $k = 0, 1, \dots, \text{card}\langle g_0 \rangle$ .  $\square$

**Theorem 2.8 (Cayley 定理).** 设  $(G, *, e)$  任意  $n$  阶有限群.  $\exists H \subset S_0$  s.t.  $(H, \circ, \text{id}_X)$  是  $S_n$  的子群且  $G \simeq H$ .

**Proof.** 取  $H := \{L_g \mid g \in G\}$ , 其中  $L_g: G \rightarrow G; g' \mapsto gg'$  可以证明是双射. 那么  $L: G \rightarrow H; g \mapsto L_g$  见证了  $H \simeq G$ .  $\square$

若  $\varphi: G \rightarrow G$  见证了  $G \simeq G$  (如  $\text{id}_G$ ), 那么称  $\varphi$  是群  $G$  的一个**自同构** (automorphism). 所有自同构组成的集合  $\text{Aut}(G)$  和其上的函数复合  $\circ$  构成了  $S(G)$  的一个子群, 称为  $G$  的**自同构群**.

自同构群有一特殊的子群  $\text{Inn}(G) := \{I_a: g \mapsto aga^{-1} \mid a \in G\}$ , 称为**内自同构群** (inner isomorphism), 其元素称为**共轭映射** (conjugation).

**Definition 2.4 (共轭).** 设  $G$  是一个群,  $a, b \in G$ . 如果  $\exists I_g \in \text{Inn}(G)$ , 使得  $I_g(a) = b$ , 那么我们称  $a$  和  $b$  互为**共轭** (conjugate).

我们毫不费力地就能证明共轭关系是等价关系, 而且当  $G$  是 Abelian 群的时候, 其任意元素的共轭都是其自身.

**Definition 2.5** (共轭类). 设  $G$  是一个群. 由共轭规定的等价类称为**共轭类** (Conjugacy class), 记为  $\text{Cl}(g)$ ,  $g$  为其代表元. 称  $\text{card}\{\text{Cl}(g) \mid g \in G\}$  为  $G$  的**类数** (class number). 如果有一个函数  $f$  满足  $g' \in \text{Cl}(g) \rightarrow f(g) = f(g')$ , 那么称  $f$  是一个**类函数** (class function).

**Definition 2.6** (正规子群). 设  $G$  是一个群,  $N$  是其子群. 倘若  $\forall I \in \text{Inn}(G), I(N) = N$ , 即其在共轭映射下不变, 则称其为  $G$  的一个**正规子群** (normal subgroup), 记为  $N \triangleleft G$ .

可以看出 Abelian 群的所有子群都是正规子群. 以下是正规子群的另一种定义方法:

**Theorem 2.9.**

$$N \triangleleft G \leftrightarrow \forall g, h \in G (gh \in N \leftrightarrow hg \in N).$$

**Proof.** 只需注意到  $I_g(gh) = g^{-1}ghg = hg$ . □

**Definition 2.7** (同态). 设有群  $(G, *, e)$  和  $(G', \circ, e')$ , 映射  $f: G \rightarrow G'$  若满足

$$\forall a, b \in G, \quad f(a * b) = f(a) \circ f(b),$$

则称其为群  $(G, *)$  到群  $(G', \circ)$  的一个**同态** (homomorphism), 也叫**态射** (morphism). 类似映射, 可定义**单态射** (monomorphism), **满态射** (epimorphism).

集合  $\ker f := f^{-1}(\{e'\})$  叫做同态  $f$  的**核** (kernel). 群到自身的同态映射称为**自同态** (endomorphism).

同态  $f$  的核是  $G$  的正规子群, 即  $\ker f \triangleleft G$ , 而  $G$  在同态下的像是  $G'$  的子群.

**Theorem 2.10.** 如果同态的核是平凡群 (即,  $\ker f = \{e\}$ ), 那么这个同态是单的.

**Proof.** 如果  $\exists g_1, g_2 \in G$ , s.t.  $f(g_1) = f(g_2)$ , 那么

$$f(g_1 * g_2^{-1}) = f(g_1) \circ f(g_2^{-1}) = f(g_1) \circ f(g_2)^{-1} \circ f(g_2) \circ f(g_2^{-1}) = e' \circ f(e) = e'$$

从而  $g_1 * g_2^{-1} \in \ker f$ , 同理  $g_2^{-1} * g_1 \in \ker f$ , 即  $g_1^{-1} = g_2^{-1}$  或  $g_1 = g_2$ , 即:  $f$  是单的. □

作为例子, 映射

$$f: G \rightarrow \text{Inn}(G); g \mapsto I_g$$

满足同构的条件 i), 因  $f(a) \circ f(b) = I_{ab} = f(ab)$ ; 但它不一定是双射, 因而是一个同态.

**Definition 2.8** (陪集). 设  $(G, *, e)$  是一个群,  $S$  是其子群,  $g \in G$ , 那么我们称  $g * S := \{g * s \mid s \in S\}$  为  $S$  在  $G$  内的**左陪集** (left coset); 同理  $S * g := \{s * g \mid s \in S\}$  为  $S$  在  $G$  内的**右陪集** (right coset). 这里我们称  $g$  是一个代表元. 如果  $g * S = S * g$ , 则称其为**陪集**.

**Theorem 2.11.**

$$N \triangleleft G \leftrightarrow \forall g \in G, g * N = N * g.$$

**Definition 2.9** (商群). 如果  $N \triangleleft G$ , 那么我们记  $G/N := \{g * N \mid g \in G\}$ , 称为  $G$  对  $N$  的商群. 这个群的乘法定义为子群元素的积的集合:

$$(g * N) \cdot (g' * N) := \{s * t \mid s \in g * N, t \in g' * N\} = (g * g') * N$$

, 单位元是  $e * N = N$  自身.

### §3 环

**Definition 3.1** (环). 集合  $R$  非空, 其上定义了加法  $+$  和乘法  $\cdot$ , 且满足:

R1)  $(R, +, 0)$  是 Abelian 群;

R2)  $(R, \cdot)$  是半群;

R3) 乘法对加法有分配律:

$$(a + b)c = ac + bc, \quad c(a + b) = ca + cb$$

对  $\forall a, b, c \in R$  成立.

那么, 我们称  $(R, +, \cdot)$  是一个环 (ring)<sup>2</sup>. 而且称  $(R, +)$  作其加法群, 称  $(R, \cdot)$  为其乘法半群. 倘若  $(R, \cdot)$  还有单位元 1, 那么我们称  $(R, +, \cdot)$  为有单位元的环.

若环  $R$  非空的子集  $L$  满足

$$\forall x, y \in L (x - y \in L \wedge xy \in L),$$

则称  $L$  是  $R$  的一个子环.

若环的乘法半群是交换的, 则称这个环是一个交换环.

作为例子,  $(\mathbb{Z}, +, \cdot)$  是我们熟悉的整数环,  $n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\}$  是它的一个子环 ( $n \in \mathbb{Z}$ ). 交换环  $R$  上的所有  $n$  阶方阵之集合  $M_n(R)$  也是环.

**Definition 3.2** (同态). 设  $R$  和  $R'$  是两个环, 有一个映射  $f$  对加法群和乘法半群都是同态 (保持运算), 即:

$$f(x)f(y) = f(xy), \quad f(x) + f(y) = f(x + y),$$

那么, 我们称其为  $R$  到  $R'$  的一个同态或态射, 集合  $\ker f := \{a \in R \mid f(a) = 0\}$  称为同态的核. 同态  $f$  的核是  $R$  的子环. 类似地我们也有单同态, 满同态和同构的概念. 两个环同构记为  $R \cong R'$ .

---

<sup>2</sup>如果  $(R, \cdot)$  不结合, 通常称非结合环.

设  $(R, +, \cdot)$  是环,  $X$  是一个集合, 在  $R^X$  上定义加法和乘法:

$$f + g: x \mapsto f(x) + g(x); \quad fg: x \mapsto f(x)g(x),$$

就得到了函数环  $(R^X, +, \cdot)$ , 其零元是  $0_X: x \mapsto 0$ . 如果  $R$  有单位元  $1$ , 那么  $R^X$  也有单位元  $1_X: x \mapsto 1, \forall x \in X$ .

作为例子, 考虑到将  $[k]_n \in \mathbb{Z}/\equiv \bmod n$  映射到  $n^{\mathbb{Z}} \ni \bmod n := \{(m, k) \in \mathbb{Z} \times m \mid n \equiv k \bmod n\}$  的同构, 模  $n$  的剩余类环  $(\mathbb{Z}_n, +, \cdot)$  即可看作函数环  $n^{\mathbb{Z}}$  的一个交换子环, 其中  $\mathbb{Z}_n := \{[k]_n \mid k \in n\}$ . 同构关系让我们也能用剩余类的代表元组成的集合  $n$  代替剩余类本身进行运算, 这种情况下,  $n$  称为模  $n$  的剩余类的导出集, 我们能用法表和乘法表给出它的代数结构.

**Definition 3.3** (整环). 环  $R$  中,  $a \in R$ , 如果  $\exists b \in R - \{0\}$  s.t.  $ab = 0$ , 则称  $a$  为环  $R$  的一个零因子; 类似则可定义右零因子<sup>3</sup>. 左零因子和右零因子统称零因子. 零元  $0$  则称为平凡零因子.

若非平凡的交换环  $R$  带单位元  $1 \neq 0$ , 且没有非平凡零因子, 则称  $R$  是一个整环 (entire ring 或 integral domain).

也有将无非平凡左零因子的带单位的非平凡环称为 *domain* 的.

**Theorem 3.1** (消去律). 设  $R$  是带单位元  $1 \neq 0$  的交换环. 环  $R$  是整环  $\leftrightarrow \forall x, y, c \in R, cx = cy \wedge c \neq 0 \rightarrow x = y$ .

**Proof.** 如果  $R$  满足消去律, 那么  $ab = 0 = 0b = a0$  将给出  $a = 0 \vee b = 0$  的论断; 如果  $R$  是整环, 那么  $cx = cy$  即  $c(x - y) = 0$  将得出  $c = 0 \vee x = y$ ; 倘若  $c \neq 0$ , 那么这就是消去律.  $\square$

有单位元的环  $R$  中元素  $x$  的可逆性往往指关于乘法的可逆性.

**Theorem 3.2.** 设  $R$  是带单位元  $1$  的环,  $U(R) := \{x \in R \mid x \text{ 可逆}\}$  是一个乘法群.

**Proof.** 单位元  $1$  当然可逆. 由定义可逆元素的逆也是可逆的. 如果  $x, y \in R$  可逆, 那么

$$(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xx^{-1} = 1 = y^{-1}x^{-1}xy = (xy)^{-1}(xy),$$

即  $xy$  可逆.  $\square$

**Definition 3.4** (除环). 设  $R$  是一个环. 如果  $U(R) = R - \{0\}$ , 那么我们称  $R$  是一个除环 (division ring), 也称斜域或反对称域 (skew field). 除环没有零因子.

接下来我们研究整环的性质, 我们特别关心的是由整数的整除问题抽象而来的整环的整除问题.

---

<sup>3</sup>[1] 中把  $0$  排除在外了.

**Definition 3.5** (正则元). 整环  $R$  的可逆元 ( $U(R)$  之元素) 被称为正则元 (unit<sup>4</sup>).

对于整数环  $\mathbb{Z}$ , 正则元只有单位元 1 和它的相反数  $-1$ .

**Definition 3.6** (整除). 设  $R$  是一个整环,  $a, b \in R$ . 如果  $\exists c \in R, ac = b$ , 那么我们称  $a$  整除 (divides)  $b$ , 或  $b$  被  $a$  整除或  $a$  是  $b$  的一个因子 (divisor), 记为  $a|b$ .

这个定义与我们熟悉的整数环  $\mathbb{Z}$  上的整除关系是一致的.

**Definition 3.7** (相伴元). 设  $R$  是一个整环,  $a, b \in R$ . 若  $a|b$  且  $b|a$ , 那么我们称  $a, b$  互为相伴元 (assosiated elements or assosiates).

**Theorem 3.3.** 设  $R$  是一个整环,  $a, b \in R - \{0\}$ . 若  $a$  与  $b$  相伴, 则它们相差一个可逆元 i.e.  $\exists u \in U(R), au = b$ .

**Proof.** 由它们相伴我们知道  $\exists c, c' \in R$ ,

$$ac = b, \quad bc' = a,$$

在第一式两侧乘  $c'$ , 又由第二式得:  $acc' = bc' = a$ . 由整环的消去律 3.1, 我们知道  $cc' = 1$ . 因为整环是一个交换环, 我们已然确证了  $c' = c^{-1}, c \in U(R)$ .  $\square$

对于整数环  $\mathbb{Z}$  而言,  $a$  和  $b$  相伴意味着  $a = \pm b$ .

**Definition 3.8** (素元). 设  $R$  是一个整环,  $p \in R - \{0\}$ . 如果  $p$  不是正则元 ( $p \notin U(R)$ ), 而且  $\forall a, b \in R - U(R), ab \neq p$ , 那么  $p$  是  $R$  中的一个素元 (prime element) 或称既约元 (irreducible element).

不难验证, 素元的相伴元也是素的.

除环没有素元, 因为除环所有的非零元都是可逆的. 整数环  $\mathbb{Z}$  的素元是素数和它们的相反数 ( $\pm 2, \pm 3, \dots$ ).

**Theorem 3.4** (整除的性质). 设  $R$  是一个整环,  $a, b, c \in R$ .

- 1)  $a|b \wedge b|c \rightarrow a|c$  i.e. 整除关系是传递的.
- 2)  $a|b \wedge a|c \rightarrow a|(b \pm c)$ .
- 3)  $a|b \rightarrow a|bc$ .

**Definition 3.9** (唯一分解整环). 设  $R$  是一个整环. 如果  $\forall a \in R - \{0\}, \exists u \in U(R), \exists (p_i)_{i \in r} \in \{p \in R \mid p \text{ 是素元}\}^{<\infty}$  (i.e. 存在  $r$  个素元) s.t.  $a = u \prod_{i \in r} p_i$  (这个叫做  $a$  的一个素分解,

---

<sup>4</sup>为避免混淆, 通常称单位元 1 为 identity

factorization); 而且如果还  $\exists u' \in U(R)$ ,  $\exists (p'_i)_{i \in r'} \in \{p \in R \mid p \text{ 是素元}\}^{<\infty}$  s.t.  $a = u' \prod_{i \in r'} p'_i$ , 那么  $r = r'$  且  $\exists \pi \in S_r$ ,  $\exists (u_i)_{i \in r} \in (U(R))^r$ ,  $p_i = u_i p'_{\pi(i)}$  (也就是说, 只要不考虑相伴和分解的顺序, 分解是唯一的), 那么, 我们称  $R$  是一个**唯一分解整环** (unique factorization domain, UFD).

这里我们没有排斥  $r = 0$  的情况, 也就是: 正则元也有 (平凡的) 素因子分解.

下面的定理给出了一种避开繁琐的 “唯一性” 的描述而定义唯一分解整环的方法:

**Theorem 3.5.** 设  $R$  是一个整环,  $\forall a \in R - \{0\}$ ,  $a$  都有素分解, i.e.  $\exists u \in U(R)$ ,  $\exists (p_i)_{i \in r} \in \{p \in R \mid p \text{ 是素元}\}^{<\infty}$  s.t.  $a = u \prod_{i \in r} p_i$ .

整环  $R$  是唯一分解整环  $\leftrightarrow \forall a, b, p \in R$ ,  $(p \text{ 是素元} \wedge p|ab) \rightarrow (p|a \vee p|b)$ .

**Proof.** 若  $R$  是唯一分解整环,  $ab = pc$ , 那么对  $a, b$  和  $c$  分别进行素分解得:

$$ab = u_{ab} \prod_{i \in r_a} a_i \prod_{j \in r_b} b_j = u_c p \prod_{k \in r_c} c_k,$$

其中  $u_{ab}, u_c \in U(R)$ ,  $a_i, b_j, c_k$  都是素元. 由唯一分解整环的定义,  $\exists p' \in \{a_i\}_{i \in r_a} \cup \{b_j\}_{j \in r_b}$  s.t.  $p'$  与  $p$  相伴, 那么  $p' = u_p p$ , 从而  $a$  或  $b$  必能表成  $p$  的倍 (将与  $p$  相伴的素因子换成  $u_p$  即可).

若  $\forall a, b, p \in R$ ,  $(p \text{ 是素元} \wedge p|ab) \rightarrow (p|a \vee p|b)$ , 我们来证明分解是唯一的. 设存在两种分解  $d = u \prod_{i \in r} p_i = u' \prod_{j \in r'} p'_j$ .

假设  $r \neq r'$ , 不失一般性我们设  $r < r'$ , 那么  $\forall j \in r'$ ,  $p'_j$  都将能整除  $\{p_i\}_{i \in r}$  之一. 由消去律 3.1, 我们将  $p'_j$  消去, 直到所有的  $\{p_i\}_{i \in r}$  都消去了 (因为每次消去两边的素因子个数都减少一个, 这总是能实现的). 假设我们是从  $j = r' - 1$  开始的, 如此我们将得到  $\prod_{j \in r' - r} p'_j \in U(R)$ , 这是荒谬的, 因为这说明  $p'_{j_0}$  有逆  $v \prod_{j \in r' - r; j \neq j_0} p'_j$ ,  $v \in U(R)$ , 这违背了素元没有逆的定义. 所以:  $r = r'$ .

我们使用递归来寻找  $\pi \in S_r$  满足  $p_i = u_{\pi(i)} p'_{\pi(i)}$ :  $r = 1$  的情况是简单的, 而假设  $r = n$  时我们总是可以找到这样的置换,  $r = n + 1$  时, 令  $\pi(n) = \min\{j \in r \mid p_i | p_j\}$  (这不可能是空的), 根据消去律 3.1, 我们得到了  $d = u u_{\pi(n)} \prod_{i \in r - \{\pi(n)\}} p_i = u' \prod_{j \in r' - 1} p'_j$ , 这根据假设已经能够给出所有的  $\pi(j)$ ,  $j \in n$  了.  $\square$

**Definition 3.10** (最大因). 设  $R$  是一个整环,  $a, b \in R$ . 若  $d \in R$  满足 1.  $d|a, d|b$ ; 2.  $\forall c \in R$  ( $c|a \wedge c|b \rightarrow c|d$ ), 则  $d$  被称为  $a, b$  的一个**最大因** (greatest common divisor or highest common factor), 记为  $\gcd(a, b)$ .

因为与  $d$  相伴的数也都是最大因, 因而  $\gcd(a, b)$  并不是一个确定的表述. 在上下文不区分相伴的元素时, 我们将使用这个符号表示任意的最大因.



**Definition 3.11** (最小倍). 设  $R$  是一个整环,  $a, b \in R$ . 若  $m \in R$  满足 1.  $a|m, b|m$ ; 2.  $\forall c \in R(a|c \wedge b|m \rightarrow m|c)$ , 则  $d$  被称为  $a, b$  的一个**最小倍** (least common multiple), 记为  $\text{lcm}(a, b)$ .

**Definition 3.12** (Euclidean 整环). 设  $R$  是一个整环,  $R^* := R - \{0\}$ . 如果  $\exists \delta: R^* \rightarrow \mathbb{N}$  s.t.

E1)  $\forall a, b \in R^*, \delta(ab) \geq \delta(a)$ ;

E2)  $\forall a \in R, \forall b \in R^*, \exists q, r \in R$  s.t.

$$a = qb + r \quad \wedge \quad (\delta(r) < \delta(b) \vee r = 0), \quad (3-1)$$

那么我们称  $R$  是一个 **Euclidean 整环** (Euclidean domain), 这样的函数  $\delta$  被称为 **Euclidean 函数**. 以上的式 (3-1) 中,  $a$  被称为**被除元** (dividend),  $b$  是**除元** (divisor),  $q$  是**商元或商** (quotient) 而  $r$  是**余元** (remiander).

在 Euclidean 整环上, 我们总是可以作辗转相除法找到两个元的最大因. 而且作为其产物我们可以证明<sup>5</sup>:

**Theorem 3.6** (Euclidean 整环上的 Bézout 定理). 设  $R$  是 Euclidean 整环.  $\forall a, b \in R$ , 总是存在最大因  $\text{gcd}(a, b)$  和最小倍  $\text{lcm}(a, b)$ , 而且  $\exists u, v \in R$  s.t.  $\text{gcd}(a, b) = au + bv$ .

**Corollary 1.** 设  $R$  是 Euclidean 整环.  $\text{gcd}(a, b) \in U(R) \leftrightarrow \exists u, v \in R(au + bv = 1)$ .

**Theorem 3.7.** 所有 Euclidean 整环都是唯一分解整环.

**Proof.** 设  $R$  是一个 Euclidean 整环. 我们先证明  $\forall a \in R^*$  都有素分解.

首先, 素元和正则元自身就是一个素分解. 所以现在我们设  $a = bc, b, c \notin U(R)$ . 由 E1),  $\delta(b) \leq \delta(a)$ . 假设  $\delta(b) = \delta(a)$ , 那么由 E2), 我们作带余除法  $b = qa + r$ : 而  $r = 0$  的情况将意味着  $c \in U(R)$ , 因此我们研究  $r \neq 0$  且  $\delta(r) < \delta(a)$  的情况. 考虑  $b - qa = b(1 - qc)$ , 由 E1),  $\delta(r) = \delta(b - qa) \geq \delta(b) = \delta(a)$ , 这与  $\delta(r) < \delta(a)$  矛盾. 所以:  $\delta(b) < \delta(a)$ .

接着我们研究  $A := \{(a_i)_{i \in \mathbb{N}} \in (R - U(R))^{\leq \infty} \mid a = \prod_{i \in \mathbb{N}} a_i\}$ . 首先我们需要证明  $\forall (a_i)_{i \in \mathbb{N}} \in A, \exists N \in \mathbb{N}, n \leq N. \delta(\prod_{i \in \mathbb{N}} a_i) > \delta(\prod_{i \in \mathbb{N}-1} a_i) > \dots > \delta(1)$ , 从而  $\delta(\prod_{i \in \mathbb{N}} a_i) \geq m$ , 从而  $\delta(a) \geq n$ , 即  $A \subset (R - R(R))^{\delta(a)}$ .

这意味着  $N := \max\{n \mid (a_i)_{i \in \mathbb{N}} \in A\}$  是存在的 ( $\mathbb{N}$  的有界子集必有最大值), 我们将说明, 这样的  $(a_i)_{i \in \mathbb{N}}$  就是一个素分解. 假设  $\exists i \in \mathbb{N}, a_i$  不是素元, 那么它将可以写成两个非正则元  $a', a''$  的乘积, 从而  $a = a'a'' \prod_{i \in \mathbb{N}-\{i_0\}} a_i$  意味着  $a$  可以分解成  $N + 1$  非正则元的乘积, 这与  $N$  的定义不合.

---

<sup>5</sup>详见 [1]

接着我们利用定理 3.5. 设  $p \in R$  是一个素元,  $p|bc$  ( $b, c \in R$ ). 因  $\gcd(p, b)|p$ , 它有两种可能性:

- i) 如果  $\gcd(p, b) = up$ ,  $u \in U(R)$ , 从而我们晓得  $up|b$ , 不难证明  $p|b$ ;
- ii) 如果  $\gcd(p, b) = 1$ , 那么  $\exists x, y \in R$ ,  $xp + yb = 1$  (推论 1), 从而  $a = axp + yab$ ,  $p|axp$ ,  $p|yab$  (因  $p|ab$ ) 从而  $p|(axp + yab)$  i.e.  $p|a$ .

□

## §4 域

交换除环  $F$  称为域 (field)<sup>6</sup>. 群  $P^* = U(P)$  称为域的乘法群. 如果  $y \neq 0$ , 那么我们通常记  $x/y = \frac{x}{y} := xy^{-1}$ .

我们可类似环, 定义同构和自同构. 同态的意义不大, 因为如果  $F$  到  $F'$  的同态  $f$  的核  $\ker f \neq \{0\}$ , 那么  $\ker f = F$ . 如果  $F'$  是域  $F$  的子环, 而且也是一个域, 则称其为  $F$  的一个子域, 反之称  $F$  为  $F'$  的一个扩域.

类似群的生成, 包含  $F \cup \{a\}$  的最小  $F$  的扩域, 记为  $F(a)$ . 如有理数域  $\mathbb{Q}$  的扩域  $\mathbb{Q}(\sqrt{2})$ .

**Theorem 4.1.** 有限剩余类环  $\mathbb{Z}_p$  是域, 当且仅当  $p$  是素数.

**Proof.** 记  $\mathbb{Z}_p$  的元素为  $[0], [1], \dots, [p-1]$ . 由素数的定义,  $\forall [k] \in \mathbb{Z}_p^* := \mathbb{Z}_p - \{[0]\}$ ,

$$[k], [2k], \dots, [(p-1)k]$$

都不为  $[0]$ , 而且两两不等. 进而,  $\exists i \in \mathbb{N}_+$  s.t.  $i < p \wedge [ik] = 1$ . 又  $\mathbb{Z}_p$  是交换环, 可知这个  $[i] = [k]^{-1}$ , 即  $\mathbb{Z}_p$  的乘法组成一个群. □

出于  $\mathbb{Z}_p$  的这个性质, 我们也记其为  $\mathbb{F}_p$  或  $\text{GF}(p)$ . 值得一提的是,  $p^n$  元有限域  $\text{GF}(p^n)$  也是存在的.

**Corollary 2 (Fermat 小定理).** 设  $p$  是素数,  $a \in \mathbb{N}$  且  $a \nmid p$ .

$$a^{p-1} \equiv 1 \pmod{p}.$$

**Proof.** 当  $[k] \in \mathbb{Z}_p^*$  时,  $I_{[k]}: \mathbb{Z}_p^* \rightarrow \mathbb{Z}_p^*; [n] \mapsto [kn]$  如定理 4.1 是  $S(\mathbb{Z}_p^*)$  的元素. 从而:

$$\left( \prod_{k=1}^{p-1} [k] \right) [a]^{p-1} = \prod_{k=1}^{p-1} [k].$$

因为域都是整环, 满足消去律 3.1, 从而  $[a]^{p-1} = [1]$ . □

<sup>6</sup>作为总结: 域上定义了加法和乘法, 加法是 Abelian 群, 乘法是 Abelian 么半群, 而且零元以外的元素都关于乘法可逆, 最后, 乘法对加法有分配律.

**Definition 4.1** (素域). 若域  $P$  不含任何非平凡真子域, 则称其为**素域** (prime field).

**Lemma 2.**  $\mathbb{Q}$  和  $\mathbb{Z}_p$  是素域.

**Proof.** 让集合  $\{0, 1\}$  对加法, 减法, 乘法和除法封闭, 我们将得到  $\mathbb{Q}$  或  $\mathbb{Z}_p$  的导出集  $p$ , 取决于 1 在加法群中的阶数.  $\square$

**Theorem 4.2.** 任意非平凡域  $F$  必含且只含一个素子域  $P$ , 而且它将同构于  $\mathbb{Q}$  或  $\mathbb{Z}_p$ , 其中  $p$  是素数.

**Proof.** 若有两个素子域, 它们的交必然也是  $F$  的子域, 根据素域的定义, 这个交不可能是真子域, 从而这两个素域相等. 这就保证了, 如果存在这么一个素子域  $P$ , 它一定是唯一的. 接下来我们研究它的存在性.

定义  $\mathbb{Z}$  到  $F$  的同态  $f(n) = ne$ , 其中  $e$  是  $F$  的单位元. 其核为  $\ker f = m\mathbb{Z}$ , 其中  $m \in \mathbb{N}$ .

如果  $m = 0$ , 那么  $ne \neq o$ , 其中  $o$  是  $F$  的零元, 只要  $n \neq 0$ . 考虑  $f$  在  $\mathbb{Q}$  上的扩张, 可以证明  $P := f(\mathbb{Q}) = \{ne \mid n \in \mathbb{Z}\}$  即构成了与  $\mathbb{Q}$  同构的素子域.

如果  $m \neq 0$ , 那么  $m = p$  是素数. 如果  $m$  不是素数, 假设它有两个 ( $m$  和 1 以外的) 因数  $a, b$ ,  $abe = o$  意味着  $ae = o$  或  $be = o$  (定理 3.1), 将与  $\ker f = m\mathbb{Z}$  矛盾. 考虑  $f$  在  $p$  (作为  $\mathbb{Z}_p$  的导出集) 上的限制,  $P := \{o, e, 2e, \dots, (p-1)e\}$  即构成了与  $\mathbb{Z}_p$  同构的素子域.  $\square$

在刚才的证明中, 我们已经遭遇了:

**Definition 4.2** (特征). 设域  $F$  的单位元和零元分别是  $e, o$ . 若存在  $p \in \mathbb{N}$  使得  $pe = o$ , 则称  $p$  为域的**特征** (characteristic), 记为  $\text{char}(F) = p$ ; 特别地, 定义  $\text{char}(F) = 0$ , 如果不存在这样的  $p$ .

**Definition 4.3** (整环的分式域). 设  $A$  是一个整环. 记  $\sim$  为  $A \times A^*$  上这样的等价关系:  $(a, b) \sim (c, d) \Leftrightarrow ad = bc$ . 从而在  $Q(A) := A \times A^* / \sim$  上我们定义加法  $+$  和乘法  $\cdot$ :

$$[(a, b)] + [(c, d)] = [(ad + bc, bc)], \quad [(a, b)][(c, d)] = [(ac, bd)].$$

如此,  $Q(A)$  被称为整环  $A$  上的一个**分式域** (field of fractions or fraction field).

经过枯燥的验证我们能得到:

**Theorem 4.3.** 分式域是域.

由于  $Q(A)$  的子环  $[a, 1]$  与  $A$  同构, 我们通常也直接说  $A \subset Q(A)$ . 同时, 习惯上我们记  $[a, b] = a/b$ , 甚至  $1/a^n =: a^{-n}$ . 注意,  $a^{-n} \in Q(A)$  而不一定在  $A$  中 (除非  $a \in U(A)$ ).

## 第二章 线性空间

### §5 线性空间

**Definition 5.1** (线性空间). 设  $\mathbb{F}$  是一个域,  $(V, +, \mathbf{0})$  是一个 Abelian 群. 如果定义标量乘积运算:  $\mathbb{F} \times V \rightarrow V; (\lambda, \mathbf{x}) \mapsto \lambda \mathbf{x}$  且满足:

- 1)  $1\mathbf{x} = \mathbf{x}, \forall \mathbf{x} \in V$  (酉性);
- 2)  $(\alpha\beta)\mathbf{x} = \alpha(\beta\mathbf{x}), \forall \alpha, \beta \in \mathbb{F}, \forall \mathbf{x} \in V$ ;
- 3)  $(\alpha + \beta)\mathbf{x} = \alpha\mathbf{x} + \beta\mathbf{x}, \forall \alpha, \beta \in \mathbb{F}, \forall \mathbf{x} \in V$ ;
- 4)  $\lambda(\mathbf{x} + \mathbf{y}) = \lambda\mathbf{x} + \lambda\mathbf{y}$ ,

那么, 我们称  $V$  是  $\mathbb{F}$  上的一个线性空间, 或称向量空间, 其元素称为向量, 相对而言  $\mathbb{F}$  的元素则被称为纯量.

通常我们称  $(\mathbf{x}_i)_{i \in I}$  为向量组,  $I$  是指标集.

**Definition 5.2** (线性组合). 设  $V$  是  $\mathbb{F}$  上的线性空间. 倘若  $\forall i \in n, \lambda_i \in \mathbb{F}, \mathbf{x}_i \in V, n$  是正整数, 那么

$$\sum_{i \in n} \lambda_i \mathbf{x}_i$$

称为向量组  $(\mathbf{x}_i)_{i \in n}$  的一个系数为  $(\lambda_i)_{i \in n}$  的线性组合,  $i \in n$ .

可数向量甚至不可数个向量之和的研究, 将在泛函分析中得到更加细致的讨论.

**Definition 5.3** (线性包络). 设  $V$  是  $\mathbb{F}$  上的线性空间,  $(\mathbf{x}_i)_{i \in n}$  是其中的一个向量组,  $n$  是正整数. 其线性包络 (linear span) 定义为

$$\langle \mathbf{x}_i \rangle_{i \in n} = \left\{ \sum_{i \in n} \lambda_i \mathbf{x}_i \mid (\lambda_i)_{i \in n} \in \mathbb{F}^n \right\}.$$

或者, 设  $M \subset V$ , 那么其线性包络定义为

$$\langle M \rangle = \left\{ \sum_{i \in n} \lambda_i \mathbf{x}_i \mid n \in \mathbb{N}, \forall i \in n (\lambda_i \in \mathbb{F} \wedge \mathbf{x}_i \in M) \right\}.$$

**Definition 5.4** (子空间). 设  $V'$  是  $\mathbb{F}$  上的线性空间  $V$  的加法子群, 且对标量乘积封闭, i.e.  $\forall \mathbf{x} \in V', \forall \lambda \in \mathbb{F}, \lambda \mathbf{x} \in V'$ , 那么, 我们称  $V'$  是  $V$  的一个 (线性) 子空间.

显然  $\langle M \rangle$  对  $\forall M \in 2^V$  都是  $V$  的子空间 (而且是包含  $M$  的最小的那个), 从而我们也说这种情况下  $\langle M \rangle$  是  $M$  张出 (span) 或生成的线性空间.

**Definition 5.5** (线性相关). 设  $V$  是  $\mathbb{F}$  上的线性空间, 其中有线性组  $(\mathbf{x}_i)_{i \in n}$ . 若  $\exists (\alpha_i)_{i \in n} \in \mathbb{F}^n$  s.t.  $\exists i \in n (\alpha_i \neq 0)$  且

$$\sum_{i \in n} \alpha_i \mathbf{x}_i = \mathbf{0},$$

那么称向量组  $(\mathbf{x}_i)_{i \in n}$  是线性相关的. 反之则称它们线性无关或线性独立.

**Theorem 5.1.** 向量组  $(\mathbf{x}_i)_{i \in n}$  是线性相关的, 当且仅当  $\exists i \in n$  s.t.

$$\exists (\beta_j)_{j \in n - \{i\}} \in 2^{\mathbb{F}} \quad \text{s.t.} \quad \mathbf{x}_i = \sum_{j \in n - \{i\}} \beta_j \mathbf{x}_j.$$

**Proof.** 证明此定理只需取  $i$  使得见证线性相关的线性组合中  $\mathbf{x}_i$  的系数不为 0 即可.  $\square$

**Definition 5.6** (维数). 设  $V$  是  $\mathbb{F}$  上的线性空间. 若  $\exists n \in \mathbb{N}$ , 满足

$$n = \max\{r \mid \exists (\mathbf{x}_i)_{i \in r} \text{ s.t. 它们是线性独立的}\},$$

那么称  $n$  是  $V$  的维数, 记为  $\dim V = n$ ,  $V$  是  $n$  维线性空间. 倘若不存在这样的  $n$ , 则  $V$  是无穷维线性空间.

特别地,  $\dim\{\mathbf{0}\} = 0$ .

**Definition 5.7** (基底). 设  $V$  是  $\mathbb{F}$  上的  $n$  线性空间,  $(\hat{\mathbf{e}}_i)_{i \in n}$  倘若线性无关, 则称其为  $V$  的一组基底. 特别地, 如果  $\dim V = 0$ , 空集  $\emptyset$  是它的一组基底.

因为基底的顺序并不重要, 有时我们也有基底向量的集合  $\{\hat{\mathbf{e}}_i\}_{i \in n}$  表示它.

**Theorem 5.2** (唯一分解). 设  $V$  是  $\mathbb{F}$  上的  $n$  线性空间,  $(\hat{\mathbf{e}}_i)_{i \in n}$  是其一组基底. 那么  $\forall \mathbf{v} \in V$ ,  $\exists!(v_i)_{i \in n}$  (称为  $\mathbf{v}$  在基底  $(\hat{\mathbf{e}}_i)_{i \in n}$  下的坐标), s.t.

$$\mathbf{v} = \sum_{i \in n} v_i \hat{\mathbf{e}}_i.$$

**Proof.** 唯一性只需要假定有两组分解, 相减并利用基底的线性独立性即可证明. 下面只证存在性: 根据维数的定义,  $(\mathbf{v}, \hat{\mathbf{e}}_0, \dots, \hat{\mathbf{e}}_{n-1})$  线性相关, 从而  $\exists \alpha \in \mathbb{F} \exists (\alpha_i)_{i \in n} \in \mathbb{F}^n$  s.t.  $(\alpha, \alpha_0, \dots, \alpha_{n-1})$  不全为 0 且

$$\alpha \mathbf{v} + \sum_{i \in n} \alpha_i \hat{\mathbf{e}}_i = \mathbf{0},$$

考虑到基底的线性独立性,  $\alpha \neq 0$ , 由域的可逆性, 我们得出了一组线性组合系数  $(-\alpha_i/\alpha)_{i \in n}$ .  $\square$

根据这个定理, 我们断言线性空间  $V$  的基底  $(\hat{e}_i)_{i \in n}$  张出  $V$  本身, i.e.  $V = \langle \hat{e}_i \rangle_{i \in n}$ .

若  $v$  在基底  $\hat{e} = (\hat{e}_i)_{i \in n}$  下的坐标为  $(v_i)_{i \in n}$ , 记之为  $v|_{\hat{e}}$ .

**Corollary 3.** 设  $V'$  是  $V$  的子空间. 如果  $V' \subsetneq V$ , 那么  $\dim V' < \dim V$ .

**Corollary 4.** 如果线性无关的向量组  $(e_j)_{j \in n}$  满足  $\forall j \in n, e_j \in \langle f_i \rangle_{i \in m}$ , 那么  $n \leq m$ .

我们称一个向量组中, 如果存在  $r$  个线性无关的向量, 且所有  $r+1$  个向量都线性相关, 则我们称  $r$  为向量组的秩 (rank), 而那  $r$  个线性无关的向量是最大线性无关组. 我们接下来证明这样的最大线性无关组总是存在, 而且其个数等于向量组张出的线性空间之维数:

**Theorem 5.3.** 设  $(x_j)_{j \in m}$  是线性空间  $V$  的向量组.

$$\dim \langle x_j \rangle_{j \in m} = r \leftrightarrow \exists \{x_{j_k}\}_{k \in r} \in 2^{\{x_j\}_{j \in m}} ((x_{j_k})_{k \in r} \text{ 是最大线性无关组}).$$

**Proof.** 由维数的定义,  $r+1$  个线性无关的向量将不可能张出维数为  $r$  的线性空间. 倘若不存在  $r$  个线性无关向量, 在  $\langle x_j \rangle_{j \in m}$  中取出一组基底共  $r$  个线性无关的向量, 这是违背推论 4 的. 因而, 最大线性无关组总是存在, 而且其个数等于向量组张出的线性空间之维数.  $\square$

**Theorem 5.4 (Steintz 替换).** 设  $V$  是  $\mathbb{F}$  上的  $n$  线性空间,  $(\hat{e}_i)_{i \in n}$  是其一组基底. 任意线性无关组  $(\hat{f}_i)_{i \in s}$ , 都可从基底中取出  $(\hat{e}_{i_k})_{i_k \in n, k \in t}$  使得

$$(\hat{f}_0, \dots, \hat{f}_{s-1}, \hat{e}_{i_0}, \dots, \hat{e}_{i_{t-1}})$$

是  $V$  的一组基底.

**Proof.** 取  $i_0$  使得  $\hat{e}_{i_0} \notin \langle \hat{f}_i \rangle_{i \in s}$ ; 接着取  $i_{k+1}$  使得  $\hat{e}_{i_{k+1}} \notin \langle \hat{f}_0, \dots, \hat{f}_{s-1}, \hat{e}_{i_k} \rangle$ , 直到不能进行下去, 剩下的基底全部都可由前面的向量组线性表出, 令此时  $k = t-1$ . 从而:  $V$  中任何向量都可由基底  $(\hat{e}_i)_{i \in n}$  表出, 从而也就可以由  $(\hat{f}_0, \dots, \hat{f}_{s-1}, \hat{e}_{i_0}, \dots, \hat{e}_{i_{t-1}})$  表出, 从而  $s+t \geq n$ .

另一方面, 不难通过归纳得知,  $(\hat{f}_0, \dots, \hat{f}_{s-1}, \hat{e}_{i_0}, \dots, \hat{e}_{i_{t-1}})$  是线性无关的, 由维数的定义, 我们断言  $t+s \leq n$ . 即  $t+s = n$ , 我们已然得到  $V$  的一组基底了.  $\square$

设  $\mathbb{F}$  上的  $n$  维线性空间有两组基底  $\hat{e} = (\hat{e}_j)_{j \in n}$ ,  $\hat{f} = (\hat{f}_i)_{i \in n}$ , 考虑定理 5.2, 我们写出:

$$\hat{f}_i = \sum_{j \in n} a_{ji} \hat{e}_j, \quad \forall i \in n. \quad (5-1)$$

这里的  $a_{ji}$  决定了矩阵

$$\mathbf{A} = (a_{ij})_{i,j \in n} = \begin{pmatrix} a_{00} & a_{01} & \cdots & a_{0,n-1} \\ a_{10} & a_{11} & \cdots & a_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1,0} & a_{n-1,1} & \cdots & a_{n-1,n-1} \end{pmatrix}. \quad (5-2)$$

矩阵 (5-2) 被称为  $\hat{e}$  到  $\hat{f}$  的一个**转换矩阵**. 值得注意的是下标的位置 (这与有限维向量空间的线性映射的矩阵差了一个转置, 见 §9). 让我们引入矩阵和与积的概念<sup>1</sup>, 用  $\hat{f}$  把  $\hat{e}$  表出, 就可以得到转换矩阵的逆  $\mathbf{A}^{-1}$ . 这两个矩阵之间的关系是  $\mathbf{A}\mathbf{A}^{-1} = \mathbf{A}^{-1}\mathbf{A} = \mathbf{I}$ .

设  $\mathbf{v} \in V$ ,

$$\mathbf{v} = \sum_{i \in n} v_i \hat{e}_i = \sum_{i \in n} v'_i \hat{f}_i = \sum_{i \in n} v'_i \sum_{j \in n} a_{ji} \hat{e}_j$$

那么,

$$\mathbf{v}|_{\hat{e}} = \left( \sum_{j \in n} a_{ij} v'_j \right)_{i \in n}$$

或  $\mathbf{v}|_{\hat{e}} = \mathbf{A} \mathbf{v}|_{\hat{f}}$ . 同理  $\mathbf{v}|_{\hat{f}} = \mathbf{A}^{-1} \mathbf{v}|_{\hat{e}}$ .

**Definition 5.8** (同构). 如果  $\mathbb{F}$  上的线性空间  $V, W$  之间存在  $f: V \rightarrow W$  s.t.

1)  $f$  是双射;

2)  $\forall \alpha, \beta \in \mathbb{F}, \forall \mathbf{u}, \mathbf{v} \in V, f(\alpha \mathbf{v} + \beta \mathbf{u}) = \alpha f(\mathbf{v}) + \beta f(\mathbf{u})$ ,

那么, 两个线性空间被认为是**同构**的.

我们指出同构关系具有等价关系的性质, 并且将基底映射到基底, 并保持维数, 这里不再一一验证了. 类似地, 我们建立线性空间**同态**的概念, 即保持线性结构的映射, 双同态即是同构. 线性空间  $V$  到  $U$  的同态集记作  $\mathcal{L}(V, U)$ .

**Theorem 5.5.** 所有  $\mathbb{F}$  上的  $n$  维线性空间都同构于 (坐标空间)  $\mathbb{F}^n$ .

**Proof.** 任取  $\mathbb{F}$  上的  $n$  维线性空间  $V$  中的向量  $\mathbf{v}$  和一组基底  $\hat{e}$ , 向量  $\mathbf{v}$  到它的坐标  $\mathbf{v}|_{\hat{e}} \in \mathbb{F}^n$  都是一个同构. □

线性空间的交依然是线性空间, 但是它们的并却不一定.

**Definition 5.9** (子空间的和). 设  $\forall i \in m, U_i$  都是  $V$  的子空间, 定义<sup>2</sup>

$$\sum_{i \in m} U_i := \left\langle \bigcup_{i \in m} U_i \right\rangle = \left\{ \sum_{i \in m} \mathbf{u}_i \mid (\mathbf{u}_i)_{i \in m} \in \prod_{i \in m} U_i \right\}$$

<sup>1</sup>本笔记不想再重复了, 请参见任意一本初等线性代数教材, 或 [1].

<sup>2</sup>这里不用  $+$  表示集合的并.

为  $U$  和  $W$  的和. 若  $\forall i \in m, U_i \cap \sum_{j \in m; j \neq i} U_j = \{\mathbf{0}\}$ , 那么记  $\bigoplus_{i \in m} U_i := \sum_{i \in m} U_i$ , 称为直和.

**Theorem 5.6 (Grassmann 恒等式).**

$$\dim(U + W) = \dim U + \dim W - \dim(U \cap W).$$

**Proof.** 设  $\dim(U \cap W) = m$ , 有基底  $\hat{e} = (\hat{e}_i)_{i \in m}$ ,  $\dim U = k$ ,  $\dim W = \ell$ . 由定理,  $\dim U$  可取基底  $(\hat{e}_0, \dots, \hat{e}_{m-1}; \hat{f}_0, \dots, \hat{f}_{k-m-1})$ ,  $\dim W$  可取基底  $(\hat{e}_0, \dots, \hat{e}_{m-1}; \hat{g}_0, \dots, \hat{g}_{\ell-m-1})$ , 那么

$$U + W = \langle \hat{e}_0, \dots, \hat{e}_{m-1}; \hat{f}_0, \dots, \hat{f}_{k-m-1}; \hat{g}_0, \dots, \hat{g}_{\ell-m-1} \rangle.$$

接下来我们证明向量组

$$\hat{e}_0, \dots, \hat{e}_{m-1}; \hat{f}_0, \dots, \hat{f}_{k-m-1}; \hat{g}_0, \dots, \hat{g}_{\ell-m-1}$$

线性独立. 若存在非平凡的线性组合:

$$\sum_{s \in m} \varepsilon_s \hat{e}_s + \sum_{i \in k-m} \varphi_i \hat{f}_i + \sum_{j \in \ell-m} \gamma_j \hat{g}_j = \mathbf{0},$$

但是前两项是  $U$  中的元素, 第三项是  $W$  中的元素, 这将说明它们都属于  $U \cap W$ , 这意味着第三项可用  $\hat{e}$  表出, 这是一个矛盾.  $\square$

**Corollary 5.**  $U = \sum_{i \in m} U_i$  是直和, 当且仅当:

$$\dim U = \sum_{i \in m} \dim U_i.$$

**Proof.** 利用 Grassmann 恒等式 5.6 和数学归纳法易证.  $\square$

**Theorem 5.7** (向量在直和上分解的唯一性). 设  $U = \sum_{i \in m} U_i$ .  $U = \sum_{i \in m} U_i$  还是直和, 当且仅当:

$$\forall \mathbf{u} \in U \exists! (\mathbf{u}_i)_{i \in m} \in \prod_{i \in m} U_i \left( \mathbf{u} = \sum_{i \in m} \mathbf{u}_i \right).$$

**Proof.**  $\leftarrow$ : 假设  $\exists \mathbf{u} \in U$  s.t.  $\exists i, j \in m (i \neq j \wedge \mathbf{u} \in U_i \cap U_j)$ , 那么  $\mathbf{u}_0$  在其上的分解式不唯一:  $\mathbf{u}_i$  和  $\mathbf{u}_j$  可以其中一个取  $\mathbf{u}$ , 另一个取  $\mathbf{0}$ .

$\rightarrow$ : 这相当于证明  $\sum_{i \in m} \mathbf{u}_i = \mathbf{0} \rightarrow \forall i \in m (\mathbf{u}_i = \mathbf{0})$ , 其逆否命题的成立, 只需要将非零项移至另一侧并用直和的定义即可验证.  $\square$

**Theorem 5.8.** 域  $\mathbb{F}$  上的  $n$  维线性空间  $V$  的任意  $m$  维线性子空间  $U$ , 都能找到  $V$  的线性子空间  $W$  使得  $V = U \oplus W$  (称  $V$  和  $W$  是互补的子空间).



**Proof.** 证明用 Steintz 替换 5.4 即可. □

记  $\text{codim } U = \dim V - \dim U$ .

当  $L$  是  $V$  的一个子空间时, 我们记线性空间作为加法群的陪集  $x + L := \{x + y \mid y \in L\}$ , 并记其代表元为. 考虑到线性空间作为加法群是 Abelian 群, 其所有子群 (子空间蕴含了加法子群) 都是正规子群, 从而:

**Definition 5.10** (商空间). 域  $\mathbb{F}$  上的线性空间  $V$  有子空间  $L$ , 记线性空间作为加法群的商群  $V/L$ , 并在  $\mathbb{F} \times V/L$  上定义标量乘法:

$$\alpha(x + L) := \alpha x + L,$$

那么称  $V/L$  是一个商空间. 不难验证商空间是一个线性空间.

我们记商空间上的同余等价类:

$$x \equiv x' \pmod{L} \leftrightarrow x - x' \in L.$$

**Theorem 5.9.** 设  $V$  的子空间  $U$  和  $W$  互余, 那么

$$f: W \rightarrow V/U; w \mapsto w + U$$

见证了  $W$  和  $V/U$  的同构.

**Proof.** 映射  $f$  对线性结构的保持是平凡的.

设  $v + U \in V/U$ . 因为  $V \oplus U = W$ ,  $\exists u \in U, \exists w \in W$  s.t.  $v = u + w$ . 从而

$$v + U = (u + w) + U = (u + U) + (w + U) = U + (w + U) = w + U = f(w),$$

所以  $f$  是满的. 满射  $f$  的单性由

$$\ker f = \{w \in W \mid f(w) = U\} = \{w \in W \mid w \in U\} = W \cap U = \{0\}$$

保证. □

## §6 对偶空间

**Definition 6.1** (线性型). 设  $V$  是一个域  $\mathbb{F}$  上的线性空间. 同态  $f: V \rightarrow \mathbb{F}$  被称为  $V$  上的一个线性型 (linear form). 在不同的情景, 它也可能被称作线性泛函 (linear functional), 线性函数等.

作为  $n$  维有限维空间的例子, 设有线性型  $\ell$ , 它作用于  $\mathbf{x} \in V$  时, 设基底为  $\hat{e}$ , 那么:

$$\ell: \mathbf{x} \mapsto \ell|_{\hat{e}} \mathbf{x}|_{\hat{e}},$$

其中  $\ell|_{\hat{e}}$  是  $1 \times n$  的行向量. 坐标变换到  $\hat{f}$  时, 设转换矩阵是  $\mathbf{P}$ , 那么:

$$\ell|_{\hat{e}} \mathbf{x}|_{\hat{e}} = \ell|_{\hat{e}} \mathbf{P} \mathbf{x}|_{\hat{f}} = \ell|_{\hat{f}} \mathbf{x}|_{\hat{f}},$$

即:

$$\ell|_{\hat{f}} = \mathbf{P} \ell|_{\hat{e}}. \quad (6-1)$$

定义线性型的线性组合  $\alpha f + \beta g$  为:

$$(\alpha f + \beta g)(\mathbf{x}) := \alpha f(\mathbf{x}) + \beta g(\mathbf{x}), \quad \forall \mathbf{x} \in V \forall \alpha, \beta \in \mathbb{F}.$$

如此我们注意到  $V$  上所有的线性型构成了一个线性空间, 其中零元是  $0_V: \mathbf{x} \mapsto 0$ .

**Definition 6.2** (对偶空间). 线性空间  $V$  上所有的线性型构成线性空间  $V^*$ , 称为  $V$  的**对偶空间** (dual space), 线性组合和零元已定义如前. 通常对偶空间的元素可称为**余向量** (covector), 或**共变向量** (covariant vector, 与此同时,  $V$  的元素对应地称为**反变向量**, contravariant vector).

为区别两种向量, 有用  $x^i$  表示反变向量而用  $\ell_i$  表示共变向量, 并引入 Einstein 求和约定的, 见之后第 5 章.

我们继续以  $n$  维线性空间为例子. 设  $V$  中有基底  $\hat{e} = (\hat{e}_i)_{i \in n}$ , 取  $V^*$  的基底  $\hat{e}^* := (\hat{e}_i^*)_{i \in n}$ , 使得  $\hat{e}_i^*(\hat{e}_j) = \delta_{ij}$ , 其中  $\delta_{ij}$  是 Kronecker 符号, 当且仅当  $i = j$  时取值为 1, 否则为 0.

不难证明它们是线性独立的, 而且能线性表示所有余向量. 这组基底称为**对偶基底**. 而且作为推论:

**Theorem 6.1.** 设  $V$  是有限维线性空间, 那么

$$\dim V^* = \dim V.$$

考虑到  $V^{**} := (V^*)^*$  和  $V$  的维数也当相同, 它们之间应该存在同构关系. 这个同构有一个自然的构造:

**Theorem 6.2** (自然同构). 设  $V$  是  $n$  维线性空间, 映射  $\varepsilon: V \rightarrow V^{**}$  定义如下:

$$\mathbf{x} \mapsto \varepsilon_{\mathbf{x}}; \quad \varepsilon_{\mathbf{x}}: V^* \rightarrow \mathbb{F}; f \mapsto f(\mathbf{x}).$$

映射  $\varepsilon$  是一个同构.

**Proof.** 事实  $\varepsilon \in \mathcal{L}(V, V^{**})$  的验证是枯燥的. 这里我们只证明它是个双射:

选取  $V$  的基底  $\hat{e} = (\hat{e}_i)_{i \in n}$ , 就能立马得出结论  $\hat{\varepsilon} = (\varepsilon_{\hat{e}_i})_{i \in n}$  是  $V^{**}$  的基底.  $\square$

这个同构被称为**自然同构**, 这样得到的  $\hat{e}^* = (e_i^*)_{i \in n}$  被称为  $\hat{e}$  的**对偶基底**.

**Lemma 3.** 设  $L$  是  $n$  维线性空间  $V$  的子空间,  $\hat{f} := (f_i)_{i \in n}$  是对偶空间  $V^*$  的一组基底. 倘若  $(f_i|_L)_{i \in n}$  表示基底各自在  $L$  上的限制, 那么  $L^* = \langle f_i|_L \rangle_{i \in n}$ .

**Proof.** 首先, 显然  $\langle f_i|_L \rangle_{i \in n} \subseteq L^*$ . 设  $r := \dim L$ ,  $\hat{e} := (\hat{e}_i)_{i \in r}$  是  $L$  的基底. 由定理 5.4, 将其扩充至  $V$  的基底  $(\hat{e}_i)_{i \in n}$ .

$\forall f \in L^*$ , 取线性型  $\tilde{f} := \sum_{i \in n} \beta_i f_i \in V^*$  满足  $\forall i' \leq r, \tilde{f}(\hat{e}_{i'}) = 0$ . 显然  $f = \tilde{f}|_L = \sum_{i \in n} \beta_i f_i|_L$ .  $\square$

**Lemma 4.** 设线性空间  $V$  中有线性相关的向量组  $(\mathbf{x}_j)_{j \in m}$ , 而  $\forall i \in m, f_i \in V^*$ . 那么:

$$\det(f_i(\mathbf{x}_j))_{i,j \in m} = 0.$$

**Proof.** 根据定理 5.1,  $\exists j_0 \in m$  使得  $\mathbf{x}_{j_0}$  是其他  $(\mathbf{x}_j)_{j \in m; j \neq j_0}$  的线性组合. 根据行列式的性质, 将  $j_0$  列减去其他各列 ( $j \neq j_0$ ) 乘上线性组合的系数  $\lambda_j$ , 不改变行列式的值, 但该行变成了

$$f_i(\mathbf{x}_{j_0}) - \sum_{j \in m; j \neq j_0} \alpha_j f_i(\mathbf{x}_j) = f_i\left(\mathbf{x}_{j_0} - \sum_{j \in m; j \neq j_0} \alpha_j \mathbf{x}_j\right) = f_i(\mathbf{0}) = 0.$$

这给出了  $\det(f_i(\mathbf{x}_j))_{i,j \in m} = 0$  的证明.  $\square$

**Lemma 5.** 设  $V$  是  $n$  维线性空间, 而  $\hat{f} := (f_i)_{i \in n}$  是对偶空间  $V^*$  的一组基底. 向量组  $(\mathbf{x}_j)_{j \in n}$  线性无关当且仅当

$$\det(f_i(\mathbf{x}_j))_{i,j \in n} \neq 0.$$

**Proof.** 由引理 4, 我们已经证明了行列式非零则线性无关. 反过来, 若线性无关, 取  $\hat{e} = \hat{f}^*$  即  $\hat{f}$  的对偶基底. 考虑到  $\hat{x} = (\mathbf{x}_j)_{j \in n}$  也是一组基底, 那么存在转换矩阵  $\mathbf{P}$ , 而且它的行列式恰是  $\det(f_i(\mathbf{x}_j))_{i,j \in n}$ . 转换矩阵是可逆的, 它的行列式非零.  $\square$

**Theorem 6.3.** 设  $V$  是  $n$  维线性空间, 而  $\hat{f} := (f_i)_{i \in n}$  是对偶空间  $V^*$  的一组基底. 那么  $V$  的子空间  $\langle \mathbf{x}_j \rangle_{j \in m}$  的维数  $r$  等于

$$(f_i(\mathbf{x}_j))_{i \in n, j \in m}$$

的最大非零子式的阶数.

**Proof.** 由引理 4, 阶数比  $r$  大的子式必为 0, 我们只需证明有  $r$  阶非零子式.

取  $(\mathbf{x}_j)_{j \in m}$  中的一组线性无关组  $(\mathbf{x}_{j_k})_{k \in r}$ , 再在  $\hat{f}|_{\langle \mathbf{x}_j \rangle_{j \in m}}$  中取出线性无关组  $(\bar{f}_k)_{k \in r} := (f_{i_k}|_{\langle \mathbf{x}_j \rangle_{j \in m}})_{k \in r}$  (引理 3), 引理 5 告诉我们

$$\det(\bar{f}_i(\mathbf{x}_{j_k}))_{i,k \in r} \neq 0.$$

□

**Corollary 6.** 设  $V$  是  $n$  维线性空间, 有基底  $\hat{e}$ , 向量组  $(\mathbf{x}_j)_{j \in m}$  的维数等于矩阵  $(\mathbf{x}_j|_{\hat{e}})_{j \in m}$  的最大非零子式的阶数. .

**Proof.** 在定理 6.3 中令  $\hat{f} = \hat{e}^*$  即可. □

## §7 多重线性型

**Definition 7.1** (多重线性型). 设  $V_0, V_1, \dots, V_{p-1}, U$  是  $\mathbb{F}$  上的线性空间. 若映射

$$f: \prod_{i \in p} V_i \rightarrow U$$

满足  $\forall i \in p$ ,

$$\forall (\mathbf{a}_j)_{j \in p; j \neq i} \in \prod_{j \in p; j \neq i} V_j, \quad f_i: V_i \rightarrow U; \quad \mathbf{x} \mapsto f(\mathbf{a}_0, \dots, \mathbf{a}_{i-1}, \mathbf{x}, \mathbf{a}_{i+1}, \dots, \mathbf{a}_{p-1}) \in \mathcal{L}(V_i, U),$$

则称  $f$  是  $V_0, \dots, V_{p-1}$  上的**多重线性型**, 或  $p$ -**线性型**. 这些多重线性型的集合记为  $\mathcal{L}(V_0, \dots, V_{p-1}; U)$ .

如  $V_0 = V_1 = \dots = V_{p-1}$ , 那么我们记  $V^p$  上的多重线性型的集合为  $\mathcal{L}_p(V; U)$ . 当  $U = \mathbb{F}$  时, 我们也可省略  $\mathbb{F}$  不写.

**Definition 7.2** (对称与反对称). 若  $V, U$  是  $\mathbb{F}$  上的线性空间,  $f \in \mathcal{L}_p(V, U)$ . 如果  $\forall \pi \in S_p$ ,  $\forall (\mathbf{x}_i)_{i \in p} \in V^p$ ,

$$f(\mathbf{x}_{\pi(i)})_{i \in p} = f(\mathbf{x}_i)_{i \in p},$$

那么我们称  $f$  为**对称的**. 如  $\forall \pi \in S_p$ ,  $\forall (\mathbf{x}_i)_{i \in p} \in V^p$ ,

$$f(\mathbf{x}_{\pi(i)})_{i \in p} = \varepsilon_\pi f(\mathbf{x}_i)_{i \in p},$$

那么我们称  $f$  为**反对称的**.

我们可以给出行列式的公理化构造, 它在实数上的计算方法我们已经在线性代数课程中非常熟悉了:

**Definition 7.3** (行列式). 设  $\mathbb{F}$  是一个域. 多重线性型  $\det \in \mathcal{L}_n(\mathbb{F})$  若满足:

- 1)  $\det$  是反对称的;
- 2)  $\det \mathbf{I} = 1$ , 其中  $\mathbf{I} = (\delta_{ij})_{i,j \in n}$ ,

记方阵  $\mathbf{X} := (\mathbf{x}_i)_{i \in n}$ , 则称  $\det \mathbf{X}$  是  $\mathbf{X}$  的行列式.

多重线性型中我们特别关注**双线性型** (bilinear form), 也就是 2-线性型在  $V_0 = V_1$  的特殊情况.

选定  $n$  维线性空间  $V$  的基底  $\hat{e}$ , 我们可将双线性型  $\mathcal{B} \in \mathcal{L}_2(V)$  表成矩阵的形式:

$$\mathcal{B}(\mathbf{x}, \mathbf{y}) = \mathcal{B} \left( \sum_{i \in n} x_i \hat{e}_i, \sum_{j \in n} y_j \hat{e}_j \right) = \sum_{i \in n} x_i \mathcal{B} \left( \hat{e}_i, \sum_{j \in n} y_j \hat{e}_j \right) = \sum_{i \in n} \sum_{j \in n} x_i \mathcal{B}(\hat{e}_i, \hat{e}_j) y_j.$$

令  $\mathbf{B} = (\mathcal{B}(\hat{e}_i, \hat{e}_j))_{i,j \in n}$ , 得:

$$\mathcal{B}(\mathbf{x}, \mathbf{y}) = \mathbf{x} |_{\hat{e}}^{\mathbf{T}} \mathbf{B} \mathbf{y} |_{\hat{e}}. \quad (7-1)$$

这说明, 只要给出一组基底, 我们就有一个  $\mathcal{L}_2(V; \mathbb{F})$  到  $M_n(\mathbb{F})$  的同构. 而且我们能看到: 对称双线性型 (其集合记为  $\mathcal{L}^+(V; \mathbb{F})$ ) 将对应对称矩阵, 而反对称双线性型 ( $\mathcal{L}^-(V; \mathbb{F})$ ) 对应一个反对称矩阵.

**Theorem 7.1** (对称与反对称). 如果  $\text{char } \mathbb{F} \neq 2$ , 那么

$$\mathcal{L}_2(V; \mathbb{F}) = \mathcal{L}_2^+(V; \mathbb{F}) \oplus \mathcal{L}_2^-(V; \mathbb{F})$$

**Proof.** 对于任意  $\mathcal{B} \in \mathcal{L}_2(V; \mathbb{F})$ , 令  $\mathcal{B}^{\mathbf{T}}$  表示  $\mathcal{B}^{\mathbf{T}}(\mathbf{x}, \mathbf{y}) = \mathcal{B}(\mathbf{y}, \mathbf{x})$ , 那么  $\mathcal{B}$  总能写成对称双线性型  $(\mathcal{B} + \mathcal{B}^{\mathbf{T}})/2$  和反对称双线性型  $(\mathcal{B} - \mathcal{B}^{\mathbf{T}})/2$  的和. 也就是说  $\mathcal{L}_2(V; \mathbb{F}) = \mathcal{L}_2^+(V; \mathbb{F}) + \mathcal{L}_2^-(V; \mathbb{F})$ .

设  $\mathcal{B} \in \mathcal{L}_2^+(V; \mathbb{F}) \cap \mathcal{L}_2^-(V; \mathbb{F})$ .  $\forall \mathbf{x}, \mathbf{y} \in V$ ,  $\mathcal{B}(\mathbf{y}, \mathbf{x}) = -\mathcal{B}(\mathbf{x}, \mathbf{y}) = \mathcal{B}(\mathbf{x}, \mathbf{y})$ . 移项得  $2\mathcal{B}(\mathbf{x}, \mathbf{y}) = 0$ , 如果  $\text{char } \mathbb{F} = 2$ , 这将对  $\mathcal{B}(\mathbf{x}, \mathbf{y})$  的任意取值恒成立; 但如果  $\text{char } \mathbb{F} \neq 2$ , 这只能说明  $\mathcal{B}(\mathbf{x}, \mathbf{y}) = 0$ , 即  $\mathcal{B} = \mathcal{O}$ . 这里  $\mathcal{O}$  表示  $(\mathbf{x}, \mathbf{y}) \mapsto 0$  的零双线性型.  $\square$

**Theorem 7.2** (双线性型的坐标变换). 设  $\hat{e}, \hat{f}$  是  $n$  维线性空间  $V$  的两组基底, 它们之间的转换矩阵是  $\mathbf{P}$ ; 双线性型  $\mathcal{B} \in \mathcal{L}_2(V)$  在  $\hat{e}, \hat{f}$  下的矩阵分别是  $\mathbf{B}, \mathbf{B}'$ , 有:

$$\mathbf{B}' = \mathbf{P}^{\mathbf{T}} \mathbf{B} \mathbf{P}.$$

这个定理说的是: 双线性型在不同基底下的矩阵是合同的.

## §8 二次型

**Definition 8.1** (二次型). 令  $V$  为域  $\mathbb{F}$  上的线性空间,  $q \in \mathbb{F}^V$ . 如果  $q$  满足:

i)  $\forall \mathbf{x} \in V, q(-\mathbf{x}) = -q(\mathbf{x});$

ii)  $\mathcal{B}: (\mathbf{x}, \mathbf{y}) \mapsto (q(\mathbf{x} + \mathbf{y}) - q(\mathbf{x}) - q(\mathbf{y}))/2$  是  $V$  上的双线性型,

那么, 我们称  $q$  是  $V$  上的二次型, 其得到的双线性型  $\mathcal{B}$  是极化的或说是与二次型  $q$  配极的双线性型.

倘若  $\mathcal{B} \in L_2^+(V; \mathbb{F})$ , 我们记  $q_{\mathcal{B}}: \mathbf{x} \mapsto \mathcal{B}(\mathbf{x}, \mathbf{x})$ . 显然  $q_{\mathcal{B}}$  是一个二次型. 而且  $q_{\mathcal{B}}$  将和  $\mathcal{B}$  配极.

通过这种二次型和对称双线性型的关系, 我们可以称有限维线性空间中的对称双线性型的矩阵就是与之配极的二次型的矩阵. 之后我们会混用对称双线性型和二次型的术语.

**Definition 8.2** (规范型). 我们称  $n$  维线性空间的二次型  $q$  在基底  $\hat{e}$  下具有标准型, 意思是其对应的矩阵就是一个对角矩阵  $\mathbf{B} = \text{diag}(\lambda_i)_{i \in n}$ . 与此同时, 我们也称  $\hat{e}$  为  $q$  的一组规范基底.

**Theorem 8.1** (二次型的规范型存在).  $\forall \mathcal{B} \in L_2^+(V; \mathbb{F}), \exists$  基底  $\hat{e}$  s.t.  $\mathcal{B}$  在该基底下的矩阵是对角的 i.e.  $\mathbf{B} = \text{diag}(\lambda_i)_{i \in n}$ .

**Proof.** 定理对  $\dim V = 1, \mathcal{B} = \mathcal{O}$  都显然成立.

假设  $\forall k \in n+1, \dim V = k$  的情况定理都成立. 在  $\mathcal{B} \neq \mathcal{O}$  的情况, 必然有一个  $\hat{e}_n \in V$  使得与  $\mathcal{B}$  配极的  $q(\hat{e}_n) \neq 0$  (否则,  $\mathcal{B}$  将与零二次型配极). 设  $\ell: \mathbf{x} \mapsto \mathcal{B}(\mathbf{x}, \hat{e}_n)$ , 显然  $\ell$  是一个非零的线性型. 从而  $\ker \ell$  是  $V$  的真子空间, 亦即  $\dim \ker \ell \leq n$ .

设  $(\hat{e}_i)_{i \in n}$  是  $\mathcal{B}|_{\ker \ell}$  的一组规范基底. 因为  $\forall i \in n, \hat{e}_i \in \ker \ell$ , 我们有  $\ell(\hat{e}_i) = \mathcal{B}(\hat{e}_i, \hat{e}_n) = 0$ . 结论要呼之欲出了: 如此得到的  $(\mathcal{B}(\hat{e}_i, \hat{e}_j))_{i, j \in n+1}$  确实是一个对角矩阵.

可是我们还没有确定  $(\hat{e}_i)_{i \in n+1}$  是线性无关的. 设有线性组合  $\sum_{i \in n+1} \alpha_i \hat{e}_i = \mathbf{0}$ , 作用  $\ell$ , 得:

$$\ell \left( \sum_{i \in n+1} \alpha_i \hat{e}_i \right) = \alpha_n \ell(\hat{e}_n) = \alpha_n q(\hat{e}_n),$$

因  $q(\hat{e}_n) \neq 0$ , 我们得到了  $\alpha_n = 0$ ; 又  $(\hat{e}_i)_{i \in n}$  是线性无关的,  $\sum_{i \in n} \alpha_i \hat{e}_i + 0\hat{e}_n = \sum_{i \in n} \alpha_i \hat{e}_i = \mathbf{0}$  只能给出  $\forall i \in n, \alpha_i = 0$ . 这就是  $(\hat{e}_i)_{i \in n+1}$  线性无关的证据.

□

## 第三章 线性算子

### §9 线性映射

**Definition 9.1** (线性映射). 设  $V, W$  是域  $\mathbb{F}$  上的线性空间. 如映射  $\mathcal{A} \in \mathcal{L}(V, W)$ , 即  $\mathcal{A}$  是  $V$  到  $W$  的一个同态, 那么我们称  $\mathcal{A}$  是  $V$  到  $W$  的一个**线性映射**, 并称其为**线性的**. 特别地, 如果它还是自同态, 我们称其为**线性变换**<sup>1</sup>或**线性算子**.

**Theorem 9.1.** 设  $\mathcal{A} \in \mathcal{L}(V, W)$ , 倘若  $(v_i)_{i \in s} \in V^s$ ,

$$f(\langle v_i \rangle_{i \in s}) = \langle f(v_i) \rangle_{i \in s}.$$

**Corollary 7.** 设  $\mathcal{A} \in \mathcal{L}(V, W)$ , 而  $U$  是  $V$  的有限维子空间, 那么  $\dim f(U) \leq \dim U$ .

我们将指出, 我们在这里所说的线性映射在某基底下可表为矩阵. 设  $V, W$  分别是  $m, n$  维线性空间, 给定各自的基底  $\hat{e}, \hat{f}$ , 那么我们可以用矩阵

$$\mathcal{A}|_{\hat{e}, \hat{f}} := \mathbf{A} = (a_{ij})_{i \in n, j \in m} = \left( f(\hat{e}_j)|_{\hat{f}} \right)_{j \in m} \quad (9-1)$$

来表示  $\mathcal{A} \in \mathcal{L}(V, W)$ .

**Theorem 9.2.** 由式 (9-1) 决定的线性映射和  $\mathbb{F}$  上的  $m \times n$  矩阵是一一对应的, 且:

$$(\mathcal{B} \circ \mathcal{A})|_{\hat{e}, \hat{g}} = \mathbf{B}\mathbf{A}, \quad (9-2)$$

其中  $\mathcal{A}: V \rightarrow U, \mathcal{B}: U \rightarrow W, V, U$  和  $W$  分别有基底  $\hat{e}, \hat{f}$  和  $\hat{g}$ .

**Proof.** 由线性映射到矩阵的单性由式 (9-1) 易证 (意思是, 只需假定有两个线性映射共用矩阵, 它们将由 5.2 得出是同一个映射). 而满性只需验证由  $f(v)|_{\hat{f}} = \mathbf{A} v|_{\hat{e}}$  决定的映射是  $\mathcal{L}(V, W)$  的元素.

---

<sup>1</sup>也有将线性映射统称为线性变换的.

同态的复合依然是同态是显然的 (可以进行枯燥的验证, 但没必要). 式 (9-2) 则由下式给出:

$$(\mathcal{B} \circ \mathcal{A})(v)|_{\hat{g}} = \mathcal{B}(\mathcal{A}(v))|_{\hat{g}} = B \mathcal{A}(v)|_{\hat{f}} = BA v|_{\hat{e}}.$$

□

**Definition 9.2 (秩).** 设  $\mathcal{A} \in \mathcal{L}(V, W)$ , 记  $\text{rank } \mathcal{A} := \dim \mathcal{A}(V)$  为线性映射  $\mathcal{A}$  的秩. 同时我们称  $\dim \ker \mathcal{A}$  为其亏数或零化度 (nullity).

**Theorem 9.3.** 若  $V, W$  都是有限维向量空间. 任取它们分别的基底  $\hat{e}, \hat{f}$ , 都有  $\text{rank } \mathcal{A} = \text{rank } A$ , 其中  $A = \mathcal{A}|_{\hat{e}, \hat{f}}$ .

**Proof.** 由定义式 (9-1), 矩阵的列向量组将张出  $\mathcal{A}(V)$ . 由 5.3, 这就给出了我们的定理<sup>2</sup>. □

**Theorem 9.4.** 设  $V$  是域  $\mathbb{F}$  上的有限维线性空间,  $W$  是域  $\mathbb{F}$  上的线性空间,  $\mathcal{A} \in \mathcal{L}(V, W)$ , 那么

$$\dim \ker \mathcal{A} + \dim \mathcal{A}(V) = \dim V.$$

**Proof.** 记  $\dim V = n, \dim \mathcal{A} = r, \dim \ker \mathcal{A} = k$ .

取  $\ker \mathcal{A}$  的一组基底  $(\hat{e}_i)_{i \in k}$  (显然  $k \leq n$ ), 并将它扩充为  $V$  的基底  $\hat{e}$  (我们又用了 Steintz 替换原则 5.4). 考虑到  $\mathcal{A}(V) = \langle \mathcal{A}(\hat{e}_i) \rangle_{i \in n}$ . 但  $\langle \mathcal{A}(\hat{e}_i) \rangle_{i \in k} = \{0\}$ . 利用  $\mathcal{A}$  的线性, 我们给出  $\forall (\lambda_i)_{i \in n} \in \mathbb{F}^n$ :

$$\sum_{i \in n} \lambda_i \mathcal{A}(\hat{e}_i) = \sum_{i \in n \wedge i \notin k} \lambda_i \mathcal{A}(\hat{e}_i) + \mathcal{A} \left( \sum_{i \in k} \lambda_i \hat{e}_i \right) = \sum_{i \in n \wedge i \notin k} \lambda_i \mathcal{A}(\hat{e}_i).$$

即是:  $(\mathcal{A}(\hat{e}_i))_{i \in n \wedge i \notin k}$  将构成  $\mathcal{A}(V)$  的一组基底. 从而:

$$r + k = n.$$

□

在  $\mathcal{L}(V, W)$  上定义加法和数乘, 可以验证它是一个线性空间.

## §10 线性算子代数

域  $\mathbb{F}$  上的线性空间  $V$  的自同态  $\mathcal{L}(V, V)$  可记作  $\mathcal{L}(V)$  或  $\text{End}(V)$ . 如前已述, 它的元素唤作线性算子. 给定  $n$  维线性空间  $V$  的一组基底  $\hat{e}$  (同时作为定义域和到达域的基底),  $\mathcal{L}(V)$  的

<sup>2</sup>矩阵的秩的最大非零子式定义和列向量组定义等价已由推论 6 保证.



元素可用  $n$  阶方阵表示. 其中恒等变换  $\mathcal{I} := \text{id}_V$  对应的矩阵通常记作  $\mathbf{I}$ , 即  $n$  阶单位阵. 零映射记为  $\mathcal{O}: \mathbf{x} \mapsto \mathbf{0}$ .

习惯上记  $\mathcal{A}\mathbf{x} := \mathcal{A}(\mathbf{x})$ ,  $\mathcal{A}\mathcal{B} := \mathcal{A} \circ \mathcal{B}$ .

**Definition 10.1** (逆算子). 设  $\mathcal{A}, \mathcal{B} \in \mathcal{L}(V)$ . 若

$$\mathcal{A}\mathcal{B} = \mathcal{B}\mathcal{A} = \text{id}_V,$$

则称它们互为**逆算子**, 记  $\mathcal{A} = \mathcal{B}^{-1}$  或  $\mathcal{B} = \mathcal{A}^{-1}$ .

**Theorem 10.1.** 设  $V$  是有限维线性空间,  $\mathcal{A} \in \mathcal{L}(V)$ .

$$\exists \mathcal{B} \in \mathcal{L}(V) (\mathcal{A} = \mathcal{A}^{-1}) \leftrightarrow \text{rank } \mathcal{A} = \dim V \leftrightarrow \ker \mathcal{A} = \{\mathbf{0}\}.$$

**Proof.** 利用定理 9.4 立刻就能证明. □

**Definition 10.2** (代数). 如果一个环  $A$  同时是域  $\mathbb{F}$  上的线性空间, 而且数乘满足:

$$\forall \lambda \in \mathbb{F} \forall \mathcal{A}, \mathcal{B} \in A (\lambda(\mathcal{A}\mathcal{B}) = (\lambda\mathcal{A})\mathcal{B} = \mathcal{A}(\lambda\mathcal{B})),$$

那么我们称  $A$  是  $\mathbb{F}$  上的一个**代数** (algebra)<sup>3</sup>. 若  $A'$  同时作为  $A$  的子环和子空间, 那么  $A'$  是  $A$  的一个子代数.

在这个意义上,  $\mathcal{L}(V)$  被称为**线性算子代数**.

多项式环  $\mathbb{F}[X]$  即是  $\mathbb{F}$  上的无穷维代数的例子, 而它在  $X = \mathcal{A} \in \mathcal{L}(V)$  时的取值, 即  $\mathbb{F}[\mathcal{A}]$  (我们记  $\mathcal{A}^0 := \text{id}_V$ ), 可以验证是  $\mathcal{L}(V)$  的子代数.

考虑到  $\mathbb{F}$  是交换的,  $\mathbb{F}[\mathcal{A}]$  也是交换的.

**Definition 10.3** (极小多项式). 设  $V$  是域  $\mathbb{F}$  上的线性空间,  $\mathcal{A} \in \mathcal{L}(V)$ ,  $P(X) \in \mathbb{F}[X]$ . 如果  $P(\mathcal{A}) = \mathcal{O}$ , 那么称多项式  $P(X)$  **零化** 线性算子  $\mathcal{A}$ . 首项系数为 1 的零化  $\mathcal{A}$  的多项式称为其**极小多项式**, 可记为  $\mu_{\mathcal{A}}(X)$ .

**Theorem 10.2** (极小多项式存在). 设  $V$  是域  $\mathbb{F}$  上的  $n$  维线性空间.  $\forall \mathcal{A} \in \mathcal{L}(V)$ , 都存在极小多项式  $\mu_{\mathcal{A}}(X)$ , 且  $\deg \mu_{\mathcal{A}}(X) = \dim \mathbb{F}[\mathcal{A}]$ .

**Proof.** 考虑到  $\mathbb{F}[\mathcal{A}]$  是  $\mathcal{L}(V)$  的子代数,  $\dim \mathbb{F}[\mathcal{A}] \leq \dim \mathcal{L}(V)$ .

如果次数  $< n^2 + 1$  的非零多项式  $P(X)$  都不能零化  $\mathcal{A}$ , 我们即可说:  $\text{id}_V, \mathcal{A}, \dots, \mathcal{A}^{n^2+1}$  的任意非平凡线性组合都不为 0, 我们在维数小于  $n^2$  维的线性空间里找到了  $n^2 + 1$  个线性无关的向量, 这显然是不可能的. □

<sup>3</sup>实际上这里是结合的, 有单位元的代数. 出于简单在本部分我们还是径直称其为代数.

**Theorem 10.3** (极小多项式唯一). 设  $V$  是域  $\mathbb{F}$  上的线性空间,  $\mathcal{A} \in \mathcal{L}(V)$ . 若  $P(X) = X^n + \sum_{i \in n} p_i X^i$ ,  $Q(X) = X^n + \sum_{i \in n} q_i X^i$  都是  $\mathcal{A}$  的极小多项式, 那么  $(p_i)_{i \in n} = (q_i)_{i \in n}$ .

**Proof.** 因为  $\mathbb{F}[\mathcal{A}]$  是一个代数,  $P(\mathcal{A}) - Q(\mathcal{A}) = \sum_{i \in n} (p_i - q_i) \mathcal{A}^i = \mathcal{O}$ . 我们得到了一个能零化  $\mathcal{A}$  次数小于  $n$  的多项式. 如果它不是零多项式, 记  $m = \deg(P(X) - Q(X))$ , 那么  $\frac{1}{p_m - q_m} \sum_{i \in n} (p_i - q_i) X^i = \mathcal{O}$  将是一个首项为 1 的零化  $\mathcal{A}$  但其次数小于极小多项式的次数, 这是违背极小多项式的定义的.  $\square$

**Theorem 10.4** (可逆算子与极小多项式的常数项). 设  $V$  是域  $\mathbb{F}$  上的  $n$  维线性空间,  $\mathcal{A} \in \mathcal{L}(V)$ , 其极小多项式是  $\mu_{\mathcal{A}}(X)$ . 算子  $\mathcal{A}$  可逆当且仅当  $\mu_{\mathcal{A}}$  的常数项非零.

**Proof.** 如果极小多项式常数项为 0, 即  $\mu_{\mathcal{A}}(X) = \sum_{i \in n - \{0\}} p_i X^i$ , 那么由线性空间的分配律与方幂的分解,

$$\mathcal{A} \left( \sum_{i \in n - \{0\}} p_i \mathcal{A}^{i-1} \right) = \mathcal{O}.$$

由极小多项式的定义,  $\sum_{i \in n - \{0\}} p_i \mathcal{A}^{i-1} \neq \mathcal{O}$ . 那么,  $\exists \mathbf{x} \in V$ ,  $\sum_{i \in n - \{0\}} p_i \mathcal{A}^{i-1} \mathbf{x} \in \ker \mathcal{A} - \{\mathbf{0}\}$ , 这表明  $\text{rank } \mathcal{A} < n$ , 即不可逆.

如果极小多项式常数项不为 0,

$$\mathcal{A} \frac{1}{-p_0} \left( \sum_{i \in n - \{0\}} p_i \mathcal{A}^{i-1} \right) = \text{id}_V,$$

给出了  $\mathcal{A}$  的逆.  $\square$

**Theorem 10.5** (化零算子的多项式是极小多项式的倍式). 设  $V$  是域  $\mathbb{F}$  上的线性空间. 能零化  $\mathcal{A} \in \mathcal{L}(V)$  的多项式  $P(X) \in \mathbb{F}[X]$  一定是  $\mu_{\mathcal{A}}(X)$  的倍式.

**Proof.** 作带余除法  $P(X) = Q(X)\mu_{\mathcal{A}}(X) + R(X)$ , 其中  $\deg R(X) < \deg \mu_{\mathcal{A}}(X)$ . 如果  $R(X) \neq 0$ , 那么  $R(\mathcal{A}) = P(\mathcal{A}) - Q(\mathcal{A})\mu_{\mathcal{A}}(X) = \mathcal{O}$  说明  $R(X)$  是次数比  $\mu_{\mathcal{A}}(X)$  还小的能化零  $\mathcal{A}$  的多项式, 这与极小多项式的定义是矛盾的.  $\square$

**Definition 10.4** (幂零算子). 设  $V$  是域  $\mathbb{F}$  上的线性空间. 线性算子  $\mathcal{A} \in \mathcal{L}(V)$  如果满足  $\exists m \in \mathbb{N}_+$  使得  $\mathcal{A}^m = \mathcal{O}$ , 那么称其是一个**幂零算子** (nilpotent operator). 数  $d := \min\{m \in \mathbb{N}_+ \mid \mathcal{A}^m = \mathcal{O}\}$  则被称为幂零算子的**幂零指数**.

由域作为零环的性质, 我们很容易验证 (只需要显式设出极小多项式):

**Theorem 10.6** (幂零算子的极小多项式). 设  $V$  是域  $\mathbb{F}$  上的线性空间. 若  $\mathcal{A} \in \mathcal{L}(V)$  的幂零指数为  $d$ , 那么其极小多项式就是  $X^d$ .

通过枯燥的运算可以得出:

**Theorem 10.7** (线性算子在不同基底下的矩阵). 设  $V$  是域  $\mathbb{F}$  上的  $n$  维线性空间. 若  $A$  和  $A'$  分别是  $\mathcal{A} \in \mathcal{L}(V)$  在基底  $\hat{e}$  和  $\hat{e}'$  下的矩阵, 那么:

$$A' = P^{-1}AP,$$

其中  $P$  是  $\hat{e}$  到  $\hat{e}'$  的转换矩阵.

也就是说: 相似矩阵是同一线性算子在不同基底下的坐标表示. 借相似关系, 行列式和迹的性质:

**Theorem 10.8** (不变量). 设  $A, A' \in M_n(\mathbb{F})$ . 设  $V$  是域  $\mathbb{F}$  上的  $n$  维线性空间. 若  $A$  和  $A'$  分别是  $\mathcal{A} \in \mathcal{L}(V)$  在基底  $\hat{e}$  和  $\hat{e}'$  下的矩阵, 那么:

$$\det A = \det A', \quad \operatorname{tr} A = \operatorname{tr} A'.$$

如此我们可以径直称  $\det \mathcal{A} := \det A$  为线性算子的行列式 (determinant), 而不必指出基底; 而  $\operatorname{tr} \mathcal{A} := \operatorname{tr} A$  为线性算子的迹 (trace).

## §11 不变子空间与特征向量

**Definition 11.1** (正交等方算子组). 设  $V$  是线性空间,  $\forall i \in m, \mathcal{P}_i \in \mathcal{L}(V)$ . 倘若  $\{\mathcal{P}_i\}_{i \in m}$  满足

$$\forall i, j \in m, \quad \mathcal{P}_i \mathcal{P}_j = \delta_{ij} \mathcal{P}_i,$$

则称其为一个正交等方算子组, 其中每一个算子都称为等方算子或投影 (projection). 它们对应的矩阵组  $\{P_i\}_{i \in m}$  则称为正交等方矩阵组.

如果正交等方算子组  $\{\mathcal{P}_i\}_{i \in m}$  还满足  $\sum_{i \in m} \mathcal{P}_i = \operatorname{id}_V$ , 那么称它是一个完备正交组.

以下事实很容易得到验证: 一个正交等方算子组中的算子满足  $\mathcal{P}_i^2 = \mathcal{P}_i$ ,  $\mathcal{P}_i \mathcal{P}_j = \mathcal{O}$  若  $i \neq j$ ; 而且如果  $i \neq j$ ,  $\mathcal{P}_j(V) \subseteq \ker \mathcal{P}_i$ .

**Theorem 11.1** (线性空间用正交完备算子组的像直和分解). 设  $V$  是线性空间,  $\{\mathcal{P}_i\}_{i \in m}$  是正交完备算子组.

$$V = \bigoplus_{i \in m} \mathcal{P}_i(V).$$

*Proof.*  $\forall x \in V$ ,

$$x = \operatorname{id}_V(x) = \sum_{i \in m} \mathcal{P}_i x,$$

注意到  $\mathcal{P}_i \mathbf{x} \in \mathcal{P}_i(V)$ , 从而  $V = \sum_{i \in m} \mathcal{P}_i(V)$ .

现在要证它是一个直和.  $\forall i \in m \forall \mathbf{x} \in \mathcal{P}_i(V) \cap \left( \sum_{j \in m; j \neq i} \mathcal{P}_j(V) \right)$ ,

$$\exists (x_j)_{j \in m} \in V^m \text{ s.t. } \mathbf{x} = \mathcal{P}_i \mathbf{x}_i = \sum_{j \in m; j \neq i} \mathcal{P}_j \mathbf{x}_j,$$

将上式两侧同时作用算子  $\mathcal{P}_i$  即有

$$\mathcal{P}_i \mathbf{x} = \mathcal{P}_i^2 \mathbf{x}_i = \mathcal{P}_i \mathbf{x}_i = \mathbf{x} = \sum_{j \in m; j \neq i} \mathcal{P}_i \mathcal{P}_j (\mathbf{x}_j) = \mathbf{0}.$$

□

**Definition 11.2** (不变子空间). 设  $V$  是线性空间,  $U$  是其子空间,  $\mathcal{A} \in \mathcal{L}(V)$ . 倘若  $\mathcal{A}(U) \subseteq U$ , 我们称  $U$  是线性算子  $\mathcal{A}$  的一个**不变子空间** (invariant subspace).

**Definition 11.3** (特征向量). 设  $V$  是域  $\mathbb{F}$  上的线性空间,  $\mathcal{A} \in \mathcal{L}(V)$ ,  $U$  是  $\mathcal{A}$  的一个一维不变子空间 (uni-dimensional invariant subspace) i.e.  $\dim U = 1$ , 那么我们称  $\forall \mathbf{x} \in U - \{\mathbf{0}\}$  是一个  $\mathcal{A}$  的**特征向量** (eigenvector, or characteristic vector).

根据定义, 特征向量满足  $\mathcal{A} \mathbf{x} = \lambda \mathbf{x}$ ,  $\lambda \in \mathbb{F}$ .

**Definition 11.4** (特征值). 设  $V$  是域  $\mathbb{F}$  上的线性空间,  $\mathcal{A} \in \mathcal{L}(V)$ ,  $\mathbf{x}$  是  $\mathcal{A}$  的一个特征向量, 且有  $\mathcal{A} \mathbf{x} = \lambda \mathbf{x}$ . 那么我们称  $\lambda \in \mathbb{F}$  是  $\mathcal{A}$  的一个 ( $\mathbf{x}$  对应的) **特征值** (eigenvalue).

由  $\mathbf{A}' \mathbf{x}' = \mathbf{P}^{-1} \mathbf{A} \mathbf{P} \mathbf{P}^{-1} \mathbf{x} = \mathbf{P}^{-1} \mathbf{A} \mathbf{x} = \lambda \mathbf{P}^{-1} \mathbf{x} = \lambda \mathbf{x}'$  可以验证, 特征值是坐标无关的.

**Definition 11.5** (谱). 算子  $\mathcal{A}$  的特征值的集合  $\text{Spec } \mathcal{A}$  称为  $\mathcal{A}$  的**谱** (spectrum).

**Definition 11.6** (几何重数). 设  $V$  是域  $\mathbb{F}$  上的线性空间,  $\mathcal{A} \in \mathcal{L}(V)$ ,  $\lambda \in \text{Spec } \mathcal{A}$ . 与特征值  $\lambda$  相伴的**特征空间** (eigenspace)  $E_{\mathcal{A}}(\lambda) := \{\mathbf{x} \in V \mid \mathcal{A} \mathbf{x} = \lambda \mathbf{x}\}$  的维数  $\gamma_{\mathcal{A}}(\lambda) := \dim E_{\mathcal{A}}(\lambda)$  则被称为特征值  $\lambda$  的**几何重数** (geometirc multiplicity).

**Definition 11.7** (单谱). 我们称  $\mathcal{A}$  的某个特征值  $\lambda$  (或叫**谱点**) 是**单的**, 意思是说  $\gamma_{\mathcal{A}}(\lambda) = 1$ . 如果  $\forall \lambda \in \text{Spec } \mathcal{A} (\gamma_{\mathcal{A}} = 1)$ , 则我们称  $\mathcal{A}$  的谱  $\text{Spec } \mathcal{A}$  是**单的**, 或  $\mathcal{A}$  有**单谱**  $\text{Spec } \mathcal{A}$ .

我们说  $\mathbf{x}$  是对应特征值  $\lambda$  的特征向量, 也可以说是  $\mathbf{x} \in \ker(\mathcal{A} - \lambda \text{id}_V)$ . 从而  $\det(\mathcal{A} - \lambda \text{id}_V) = 0$ . 考虑到行列式和坐标无关, 且对非退化方阵  $\mathbf{P}$ :

$$\det(\mathbf{A}' - \lambda \mathbf{I}) = \det(\mathbf{P}^{-1} \mathbf{A} \mathbf{P} - \lambda \mathbf{P}^{-1} \mathbf{P}) = \det \mathbf{P}^{-1} \det(\mathbf{A} - \lambda \mathbf{I}) \det \mathbf{P} = \det(\mathbf{A} - \lambda \mathbf{I}),$$

我们可以定义与坐标无关的特征多项式:

**Definition 11.8** (特征多项式). 设  $V$  是域  $\mathbb{F}$  上的  $n$  维线性空间,  $\mathcal{A} \in \mathcal{L}(V)$ .  $\chi_{\mathcal{A}}(X) := \det(\mathcal{A} - X\text{Id}_V) \in \mathbb{F}[X]$  被称为算子  $\mathcal{A}$  的**特征多项式** (characteristic polynomial). 方程  $\chi_{\mathcal{A}}(X) = 0$  被称为**特征方程**或**久期方程**.

**Definition 11.9** (代数重数). 设  $V$  是域  $\mathbb{F}$  上的  $n$  维线性空间,  $\mathcal{A} \in \mathcal{L}(V)$ ,  $\lambda \in \text{Spec } \mathcal{A}$ . 我们称  $\lambda$  作为  $\chi_{\mathcal{A}}(X)$  的根的重数为线性算子  $\mathcal{A}$  的特征值  $\lambda$  的**代数重数** (algebraic multiplicity), 记为  $\mu_{\mathcal{A}}(\lambda)$ .

**Lemma 6.** 设  $V$  是域  $\mathbb{F}$  上的线性空间,  $\mathcal{A} \in \mathcal{L}(V)$ ,  $\forall i \in m$  ( $m \in \mathbb{N}_+$ ),  $\lambda_i \in \text{Spec } \mathcal{A}$ , 且  $\lambda_i = \lambda_j \rightarrow i = j$ . 若  $(\mathbf{x}_i)_{i \in m}$  满足  $\mathbf{x}_i \in E_{\mathcal{A}}(\lambda_i) \wedge \mathbf{x}_i \neq \mathbf{0}$ , 则  $(\mathbf{x}_i)_{i \in m}$  线性无关.

**Proof.** 显然若  $m = 1$  时命题是成立的. 假设  $m = k - 1$  时命题成立, 并在式子

$$\sum_{i \in k} \alpha_i \mathbf{x}_i = \mathbf{0} \quad (11-1)$$

的两侧左乘  $\mathcal{A}$  (其中  $\alpha_i \in \mathbb{F}$ ), 得:

$$\mathcal{A} \sum_{i \in k} \alpha_i \mathbf{x}_i = \sum_{i \in k} \alpha_i \mathcal{A} \mathbf{x}_i = \sum_{i \in k} \alpha_i \lambda_i \mathbf{x}_i = \mathbf{0} \quad (11-2)$$

$\lambda_{k-1}$ (11-1) - (11-2), 得:

$$\sum_{i \in k-1} \alpha_i (\lambda_{k-1} - \lambda_i) \mathbf{x}_i = \mathbf{0},$$

根据假设,  $\forall i \in k - 1$ ,  $\alpha_i (\lambda_{k-1} - \lambda_i) = 0$ , 又  $\lambda_i \neq \lambda_{k-1}$ , 因为  $i \neq k - 1$ , 则  $\alpha_i = 0$ . 回到式 (11-1), 这意味着  $\alpha_{k-1} \mathbf{x}_{k-1} = \mathbf{0}$ , 这只能是  $\alpha_{k-1} = 0$ .  $\square$

**Lemma 7.** 设  $V$  是域  $\mathbb{F}$  上的  $n$  维线性空间,  $\mathcal{A} \in \mathcal{L}(V)$ .  $\sum_{\lambda \in \text{Spec } \mathcal{A}} E_{\mathcal{A}}(\lambda)$  是直和.

**Proof.** 由引理 6 易证<sup>4</sup>.  $\square$

**Theorem 11.2** (几何重数不超过代数重数). 设  $V$  是域  $\mathbb{F}$  上的  $n$  维线性空间,  $\mathcal{A} \in \mathcal{L}(V)$ ,  $\lambda \in \text{Spec } \mathcal{A}$ .  $\gamma_{\mathcal{A}}(\lambda) \leq \mu_{\mathcal{A}}(\lambda)$ .

**Proof.** 设  $\gamma_{\mathcal{A}}(\lambda) = m$ . 设  $\mathcal{A}'$  表示  $\mathcal{A}$  在  $E_{\mathcal{A}}(\lambda)$  上的限制. 因为  $\forall \mathbf{x} \in E_{\mathcal{A}}(\lambda)$ ,  $\mathcal{A}' \mathbf{x} = \lambda \mathbf{x}$ , 所以对于  $E_{\mathcal{A}}(\lambda)$  的任意基底  $\hat{e}'$ ,  $\mathcal{A}'|_{\hat{e}'} = \text{diag}(\lambda)_{i \in m}$ . 所以,

$$\det(\mathcal{A}' - X\text{Id}_{E_{\mathcal{A}}(\lambda)}) = \det(\text{diag}(\lambda)_{i \in m} - X\mathbf{I}_m) = (\lambda - X)^m.$$

<sup>4</sup>因为我们没有定义无穷个向量的线性组合, 所以这个证明只能对有限个特征向量的情况有效, 出于保守我们只研究有限维线性空间.

我们把  $\hat{e}'$  扩展到  $V$  的基底  $\hat{e}$ , 我们容易验证,  $\mathcal{A}|_{\hat{e}}$  有如下形式:

$$\mathcal{A}|_{\hat{e}} = \begin{pmatrix} \lambda \mathbf{I}_m & \mathbf{B}_{m \times (n-m)} \\ \mathbf{O}_{n-m} & \mathbf{C}_{n-m} \end{pmatrix},$$

从而  $\chi_{\mathcal{A}}(X)$  有形式  $(\lambda - X)^m \det(\mathbf{C}_{n-m} - X\mathbf{I}_{n-m})$ . 若  $\lambda$  是  $\det(\mathbf{C}_{n-m} - X\mathbf{I}_{n-m})$  的  $k$  重根 (或者不是根时令  $k = 0$ ), 那么  $\mu_{\mathcal{A}}(\lambda) = m + k \geq m$ .  $\square$

**Definition 11.10** (可对角化). 设  $V$  是域  $\mathbb{F}$  上的  $n$  维线性空间,  $\mathcal{A} \in \mathcal{L}(V)$ . 倘若存在一组基底  $\hat{e}$ , 使得在这组基底  $\hat{e}$  下  $\mathcal{A}$  的矩阵是对角的, i.e.

$$\mathcal{A}|_{\hat{e}} = \text{diag}(\lambda_i)_{i \in n},$$

那么我们称算子  $\mathcal{A}$  是可对角化的.

**Theorem 11.3.** 设  $V$  是域  $\mathbb{F}$  上的  $n$  维线性空间,  $\mathcal{A} \in \mathcal{L}(V)$ . 当且仅当 1.  $\chi_{\mathcal{A}}(X)$  的所有根都在  $\mathbb{F}$  中; 2.  $\forall \lambda \in \text{Spec } \mathcal{A}, \mu_{\mathcal{A}}(\lambda) = \gamma_{\mathcal{A}}(\lambda)$ , 线性算子  $\mathcal{A}$  可对角化.

## 第四章 内积空间

## 第五章 张量



# 附录 A 置换

## §1 置换群

置换群  $S_n$  的定义已在正文的 §2 中给出, 我们在此重复一遍: 有限集  $n \in \mathbb{N}_+$  上的置换群  $S_n$  定义为  $n^n$  中的双射的集合, 乘法定义为函数的复合, 单位元是  $\text{id}_n$ .

不难证明  $\text{card } S_n = P_n^n = n!$ .

设  $\pi \in S_n$ . 元素  $i, j \in n$  如果满足  $\exists k \in \mathbb{N}, \pi^k(i) = j$ , 那么我们称  $i$  和  $j$  是  $\pi$ -等价的. 不难证明这是等价关系, 而且把  $n$  分成等价类  $\{n_k\}_{k \in p}, p \in \mathbb{N}_+$ . 每个等价类  $n_k$  称为置换  $\pi$  的轨道, 其元素个数  $\ell_k := \text{card } n_k$  称为轨道  $n_k$  的长度.

为方便, 我们定义  $\pi_k$  为:

$$\pi_k(i) = \begin{cases} \pi(i) & i \in n_k \\ \text{id}_n & i \notin n_k \end{cases},$$

我们得到了  $\pi = \prod_{k \in p} \pi_k$ , 这是轨道间不相交的结论.

若置换  $\pi$  至多只有一个轨道的长度大于 1 i.e.  $\exists k_0 \in p \forall k \in p (k \neq k_0 \rightarrow \ell_k = 1)$ , 我们称这个置换为**轮换**或**循环**, 并径直称  $\ell_{k_0}$  为这个轮换的**长度**. 轮换  $\pi$  可记为  $(\pi^k(i))_{k \in \ell_{k_0}}$  其中  $i \in n_{k_0}$ . 不难验证  $i$  在  $n_{k_0}$  中的选择无关紧要. 我们记  $\text{id}_n = (0)$ . 当  $\ell_{k_0} = 2$  时, 我们也叫轮换  $\pi$  为对换.

我们称两个轮换**不相交**, 如果它们的长度  $\leq 2$ , 且最长轨道不相交.

以上的叙述可以总结为:

**Theorem 1.1.** 置换群  $S_n$  中的每一个置换, 要么是  $\text{id}_n$ , 要么存在唯一的不相交长度  $\leq 2$  的轮换的集合  $\{\pi_k\}_{k \in p}$ , 使得  $\pi = \prod_{k \in p} \pi_k$ .

**Theorem 1.2.** 置换群  $S_n$  中的每一个置换  $\pi$  都可写为对换  $(\sigma_k)_{k \in q}$  的乘积, 即  $\pi = \prod_{k \in q} \sigma_k$ <sup>1</sup>.

而且, 倘若存在  $(\sigma'_k)_{k \in q'}$  也满足  $\pi = \prod_{k \in q'} \sigma'_k$ , 那么  $q \equiv q' \pmod{2}$ .

---

<sup>1</sup>注意, 这时不可对调  $\sigma_k$  间的位置.

**Proof.** 因为每个长为  $r$  的轮换都可写成:

$$(\pi^k(i))_{k \in r} = \prod_{k \in r} (i, \pi^{r-k}(i)),$$

则由定理 1.1, 每一个置换都可以写成对换的乘积.

我们先证明, 若  $\text{id}_n = \prod_{k \in q} \sigma_k$ , 其中  $\forall k \in q, \sigma_k$  是对换, 那么  $q \equiv 0 \pmod{2}$ .

我们用递归的方法证明这点. 设  $\sigma_{q-1} = (S, T)$ ,  $S, T \in n$ . 为方便, 我们记  $p := \max\{k \mid \sigma_k = (S, t), t \in n\}$ . 令  $(\sigma'_k)_{k \in q} := (\sigma_k)_{k \in q}$ ,  $\sigma'_p := (S, t)$ .

除非出现以下情况:

- a)  $p = 0$ .
- b)  $p \neq 0$  但  $\sigma'_{p-1} = (S, t)$ .

否则, 不断重复下列过程:

- 1) 如果  $\sigma_{p-1} = (S, r)$ , 其中  $r \neq t$ : 由于

$$(S, r)(S, t) = (S, t, r) = (t, S, r) = (t, S)(t, r) = (S, t)(t, r),$$

那么重新令

$$\sigma'_{p-1} = (S, t), \sigma'_p = (t, r) \text{ 其他不变,}$$

将仍然满足  $\text{id}_n = \prod_{k \in q} \sigma'_k$ . 执行 4).

- 2) 如果  $\sigma_{p-1} = (t, r)$ : 由于

$$(t, r)(S, t) = (t, S, r) = (r, t, S) = (r, S)(r, t) = (S, r)(r, t),$$

那么重新令

$$\sigma'_{p-1} = (S, r), \sigma'_p = (r, t) \text{ 其他不变,}$$

将仍然满足  $\text{id}_n = \prod_{k \in q} \sigma'_k$ . 执行 4).

- 3) 如果  $\sigma_{p-1} = (r, u)$ , 其中  $\{r, u\} \cap \{S, t\} = \emptyset$ : 由于

$$(r, u)(S, t) = (S, t)(r, u),$$

那么重新令

$$\sigma'_{p-1} = (S, t), \sigma'_p = (r, u) \text{ 其他不变,}$$

将仍然满足  $\text{id}_n = \prod_{k \in q} \sigma'_k$ . 执行 4).

- 4) 重新令  $p := \max\{k \mid \sigma'_k = (S, t), t \in n\}$  以及  $\sigma'_p = (S, t)$ .

直到满足 a) 或 b) 为止. 这个循环将总是能在有限次结束, 因为每次  $p$  都减小了 1.

当过程到结束时, 如果满足 a), 那么  $\prod_{k \in q} \sigma'_k(S) = (S, t) \prod_{k \in q, k \neq 0} \sigma'_k(S) = (S, t)(S) = t \neq S$ , 与  $\text{id}_n(S) = S$  矛盾; 那么, 只可能是满足 b), 此时因  $(S, t)(S, t) = \text{id}_n$ , 将它们消去, 我们得到了  $\text{id}_n$  的  $q' = q - 2$  个对换的分解.

重复这样的过程直到  $q' = 0$  或  $q' = 1$  为止, 而后者是不可能的, 因为  $\text{id}_n$  永远不可能等于对换. 所以:  $q \equiv 0 \pmod{2}$ .

最后, 我们断言, 任意置换和它的逆分解成的对换数目之和是偶数. 即, 考虑  $\pi$  的两种分解,  $\pi = \prod_{k \in q} \sigma_k = \prod_{k \in q'} \sigma'_k$ , 那么  $\text{id}_n = \pi \pi^{-1} = \prod_{k \in q} \sigma_k^{-1} \prod_{k \in q'} \sigma'_k = \prod_{k \in q} \sigma_k \prod_{k \in q'} \sigma'_k$ , 由前  $q + q' \equiv 0 \pmod{2}$ .  $\square$

据此我们把置换群的元素分为**奇置换** (分解得到奇数个对换) 和**偶置换** (分解得到偶数个对换), 并引入置换的**符号或奇偶性**  $\varepsilon_\pi$ , 其值对于偶置换是 1, 奇置换是 0.

所有偶置换的集合  $A_n$  是  $S_n$  的子群.

## 附录 B 矩阵和行列式

以下只是一些定义的罗列, 与一些术语的规定, 矩阵与行列式的性质则散见于正文中. 如果读者感到陌生, 可参阅任意一本初等线性代数教材, 如 [1].

### §2 矩阵

**Definition 2.1** (矩阵). 设  $\mathbb{F}$  是一个域. 将  $\{a_{ij}\}_{i \in m, j \in n} \in 2^{\mathbb{F}}$  ( $n, m \in \mathbb{N}_+$ ) 排成一个长方形的表:

$$\mathbf{A} := (a_{ij})_{i \in m, j \in n} = \begin{pmatrix} a_{00} & a_{01} & \cdots & a_{0,n-1} \\ a_{10} & a_{11} & \cdots & a_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m-1,0} & a_{m-1,1} & \cdots & a_{m-1,n-1} \end{pmatrix}. \quad (2-1)$$

式 (2-1) 定义的  $\mathbf{A}$  被称为  $\mathbb{F}$  上的  $m \times n$  的**矩阵**,  $m \times n$  被称为它的尺寸或大小,  $\{a_{ij}\}_{i \in m, j \in n}$  是它的**元素**. 所有  $\mathbb{F}$  上的  $m \times n$  矩阵的集合记为  $M_{m \times n}(\mathbb{F})$ .

元素全为 0 的矩阵记为  $\mathbf{O}$ , 有时为了强调它的尺寸, 将之写在右下角 i.e.  $\mathbf{O}_{m \times n}$ .

通常, 我们称  $1 \times n$  或  $n \times 1$  的矩阵为  $n$  维**向量**, 前者是**行向量**, 后者是**列向量**. 列向量的集合也可记为  $\mathbb{F}^n$ , 即认为它是  $\mathbb{F}$  的  $n$  次 Cartesian 幂的元素. 但是, 当上下文明确时, 我们不特意在术语上区分行向量和列向量.

我们也常把矩阵写成列向量组的形式, 即

$$\mathbf{A} := (\mathbf{x}_j)_{j \in n}, \quad \forall j \in n (\mathbf{x}_j \in \mathbb{F}_n). \quad (2-2)$$

设矩阵  $\mathbf{A}$  的尺寸为  $n \times n$ , 我们称其为  $n$  维**方阵**, 其集合记为  $M_n(\mathbb{F})$ .

**Definition 2.2** (对角矩阵). 若方阵  $\mathbf{A}$  的元素只有对角线上的元素非零 i.e.  $a_{ij} \neq 0 \rightarrow i = j$ , 称其为**对角矩阵**, 记为  $\text{diag}(a_{ii})_{i \in n}$ . 特别地  $\mathbf{I} := \text{diag}(1)_{i \in n}$  称为  $n$  维**单位阵**.

**Definition 2.3** (转置). 设  $A = (a_{ij})_{i \in m, j \in n} \in M_{m \times n}(\mathbb{F})$ . 我们称  $(a_{ji})_{j \in n, i \in m} \in M_{n \times m}(\mathbb{F})$  为矩阵  $A$  的转置, 记为  $A^T$ .

如果  $\mathbb{F}$  是复数域  $\mathbb{C}$ , 我们通常更加关注共轭转置  $A^\dagger := \overline{A}^T$ .

**Definition 2.4** (和). 在  $M_{m \times n}$  上定义和:

$$A + B = (a_{ij})_{i \in m, j \in n} + (b_{ij})_{i \in m, j \in n} = (a_{ij} + b_{ij})_{i \in m, j \in n}.$$

不难验证,  $(M_{m \times n}, +, \mathbf{0}_{m \times n})$  构成了一个 Abelian 群.

**Definition 2.5** (积). 在  $M_{m \times \ell}(\mathbb{F})$  和  $M_{\ell \times n}(\mathbb{F})$  间定义积  $(\cdot: M_{m \times \ell}(\mathbb{F}) \times M_{\ell \times n}(\mathbb{F}) \rightarrow M_{m \times n}(\mathbb{F}))$ :

$$AB = (a_{ij})_{i \in m, j \in \ell} (b_{ij})_{i \in \ell, j \in n} = \left( \sum_{k \in \ell} a_{ik} b_{kj} \right)_{i \in m, j \in n}.$$

由域的性质, 我们能验证矩阵的乘法运算是结合的, 而且满足对和的分配律.

**Theorem 2.1** (积的转置). 设  $A \in M_{m \times \ell}(\mathbb{F})$ ,  $B \in M_{\ell \times n}(\mathbb{F})$ .

$$(AB)^T = B^T A^T.$$

**Corollary 8** (积的共轭转置). 设  $A \in M_{m \times \ell}(\mathbb{C})$ ,  $B \in M_{\ell \times n}(\mathbb{C})$ .

$$(AB)^\dagger = B^\dagger A^\dagger.$$

**Definition 2.6** (逆). 设方阵  $A \in M_n(\mathbb{F})$ . 若  $\exists B \in M_n(\mathbb{F})$ , s.t.  $BA = AB = I$  则称其为  $A$  的逆, 并记为  $A^{-1}$ , 同时称  $A$  是可逆的.

**Theorem 2.2** (逆的转置). 设  $A \in M_n(\mathbb{F})$  且可逆. 其转置  $A^T$  也可逆, 且  $(A^T)^{-1} = (A^{-1})^T$ .

*Proof.* 写出逆的定义, 两边取转置, 并应用  $I^T = I$  和定理 2.1. □

**Theorem 2.3** (逆的共轭转置). 设  $A \in M_n(\mathbb{C})$  且可逆. 其共轭转置  $A^\dagger$  也可逆, 且  $(A^\dagger)^{-1} = (A^{-1})^\dagger$ .

**Definition 2.7** (相似). 设  $A, A' \in M_n(\mathbb{F})$ . 如果  $\exists B \in M_n(\mathbb{F})$  s.t.  $B$  可逆且有  $A' = B^{-1}AB$ , 那么我们称  $A$  和  $A'$  相似 (similar), 记为  $A \sim A'$ .

不难看出, 相似关系是一个等价关系.

**Definition 2.8** (合同矩阵). 设  $A, A' \in M_n(\mathbb{F})$ . 如果  $\exists B \in M_n(\mathbb{F})$  s.t.  $B$  可逆且有  $A' = B^T A B$ , 那么我们称  $A$  和  $A'$  合同 (congruence).

**Definition 2.9** (迹). 设  $A = (a_{ij})_{i,j \in n} \in M_n(\mathbb{F})$ . 方阵  $A$  的迹定义为  $\text{tr } A := \sum_{i \in n} a_{ii}$ .

**Theorem 2.4** (迹的交换性). 设  $A, B \in M_n(\mathbb{F})$ .  $\text{tr}(AB) = \text{tr}(BA)$ .

*Proof.*

$$AB = \left( \sum_{k \in n} a_{ik} b_{kj} \right), \quad BA = \left( \sum_{k \in n} b_{ki} a_{kj} \right).$$

从而

$$\text{tr}(AB) = \sum_{i \in n} \sum_{k \in n} a_{ik} b_{ki} = \sum_{k \in n} \sum_{i \in n} b_{ki} a_{ik} = \text{tr}(BA).$$

□

### §3 行列式

行列式的公理化构造我们在定义 7.3 中已经给出了. 我们这里做出一个不加解释的定义<sup>1</sup>, 并不加证明地给出它的一些性质.

**Definition 3.1** (行列式). 方阵  $A \in M_n(\mathbb{F})$  的行列式  $\det A := |a_{ij}|_{i,j \in n}$  定义为:

$$\det A = |a_{ij}|_{i,j \in n} = \sum_{\pi \in S_n} \varepsilon_\pi \prod_{i \in n} a_{i, \pi(i)}$$

**Theorem 3.1** (行列式的反对称性). 设  $A = (a_j)_{j \in n}$ , 那么  $\forall \pi \in S_n$ ,  $|a_{\pi(j)}|_{j \in n} = \varepsilon_\pi \det A$ .

**Theorem 3.2.**  $\det A = \det A^T$ .

**Theorem 3.3** (行列式的线性 1). 设  $A = (a_j)_{j \in n}$ ,  $A' = (a'_j)_{j \in n}$ , 其中  $j \neq j_0$  时  $a'_j = a_j$ ; 但  $a'_{j_0} = \lambda a_{j_0}$ ,  $\lambda \in \mathbb{F}$ .

$$\det A' = \lambda \det A.$$

**Theorem 3.4** (行列式的线性 2). 设  $A = (a_j)_{j \in n}$ ,  $A' = (a'_j)_{j \in n}$ , 其中  $j \neq j_0$  时  $a'_j = a_j$ .

$$\det A + \det A' = |a''_j|_{j \in n},$$

其中  $j \neq j_0$  时  $a''_j = a_j$ ;  $a''_{j_0} = a'_{j_0} + a_{j_0}$ .

设  $I, J \in \mathcal{P}(n)$ , 而  $|I| = |J|$ . 记  $M_{IJ} := |a_{k\ell}|_{k \in n-I; \ell \in n-J}$  为  $A$  的子式 (minor), 而代数子式 (cofactor) 则是定义为  $A_{IJ} := (-1)^{\sum_{i \in I} i + \sum_{j \in J} j} M_{IJ}$ . 如果  $|I| = |J| = 1$ , 那么我们称  $M_{ij} := M_{\{i\}\{j\}}$  为首子式 (first minor), 对应的代数子式也可记为  $A_{ij}$ . 那么, 以下的定理将给出一种计算行列式的递推方法:

<sup>1</sup>几何解释可见于 [1].

**Theorem 3.5** (行列式按行 (列) 展开).  $\forall k \in n$ ,

$$\det \mathbf{A} = \sum_{i \in n} a_{ik} A_{ik}; \quad \det \mathbf{A} = \sum_{j \in n} a_{kj} A_{kj}.$$

以下的定理确保了定义 7.3 和定义 3.1 的一致性, 并且这是唯一的构造方式.

**Theorem 3.6** (行列式的唯一性). 设  $\mathcal{D} \in \mathcal{L}_n(\mathbb{F}^n; \mathbb{F})$  (即  $\mathcal{D}: M_n(\mathbb{F}) \rightarrow \mathbb{F}$  而且是  $n$  重线性的). 倘若  $\mathcal{D}$  还是反对称的, 即  $\forall \pi \in S_n, \mathcal{D}(\mathbf{x}_{\pi(j)})_{j \in n} = \varepsilon_\pi \mathcal{D}(\mathbf{x}_j)_{j \in n}$ , 那么  $\forall \mathbf{A} \in M_n(\mathbb{F})$ ,  $\mathcal{D}(\mathbf{A}) = \mathcal{D}(\mathbf{I}) \det \mathbf{A}$ .

它的证明需要利用线性和反对称性, 利用行变换将矩阵转换为对角的. 取  $\mathcal{D}(\mathbf{I}) = 1$ , 我们就得到了  $\mathcal{D} = \det$ .

取  $\mathcal{D}(\mathbf{I}) = \det \mathbf{B}$  推出的一个重要的性质是:

**Theorem 3.7** (行列式的积).  $\forall \mathbf{A}, \mathbf{B} \in M_n(\mathbb{F})$ ,  $\det(\mathbf{AB}) = \det \mathbf{A} \det \mathbf{B}$ .

## 附录 C 多项式

### §4 多项式环

**Definition 4.1** (多项式环). 设  $R$  是一个交换环,  $\langle X \rangle := \{X^n \mid n \in \mathbb{N}\}$  是  $X$  生成的幺半群, 记  $I := X^0$ . 若形如  $P(X) := \sum_{i \in \mathbb{N}} p_i X^i$  的形式 (称为多项式, 其中只有有限个  $p_i$  非零) 的集合<sup>1</sup>:

$$R[X] := \left\{ \sum_{i \in \mathbb{N}} p_i X^i \mid (p_i)_{i \in \mathbb{N}} \in R^{<\mathbb{N}} \right\}$$

上定义了加法:

$$P(X) + Q(X) := \sum_{i \in \mathbb{N}} p_i X^i + \sum_{i \in \mathbb{N}} q_i X^i = \sum_{i \in \mathbb{N}} (p_i + q_i) X^i$$

和乘法:

$$P(X)Q(X) := \left( \sum_{i \in \mathbb{N}} p_i X^i \right) \left( \sum_{i \in \mathbb{N}} q_i X^i \right) = \sum_{\ell \in \mathbb{N}} \sum_{i+j=\ell} p_i q_j X^\ell,$$

那么, 我们称  $R[X]$  是  $R$  上变元  $X$  的**多项式环**. 在变元是明确的时候, 多项式  $P(X)$  也简记为  $P$ .

记  $\deg P(X) := \max\{n \mid p_n \neq 0\}$  为多项式  $P(X)$  的**次数**. 而  $(p_n)_{n \in \deg P(X)+1}$  是多项式的**系数**, 其中  $p_0$  是**常数项**, 而  $p_{\deg P(X)}$  是**最高次项系数**或**首项系数**.

所有系数都为 0 的多项式被称为**零多项式**, 次数为 1 的多项式被称为**线性多项式**.

不难验证,  $R[X]$  的单位元和零元分别是  $R$  的单位元和零元.

以下给出一些不难证明的定理, 如果读者感到困难, 请翻阅参考资料 [1]:

**Theorem 4.1.**  $\forall P(X), Q(X) \in A[A], \deg(P(X) + Q(X)) \leq \max\{\deg P(X), \deg Q(X)\},$   
 $\deg(P(X)Q(X)) \leq \deg P(X) + \deg Q(X).$

---

<sup>1</sup>  $R^{<\mathbb{N}} := \bigcup_{n \in \mathbb{N}} R^n$



**Theorem 4.2** (多项式环的泛性). 设  $R$  是一个交换环,  $A$  是  $R$  的子环.  $\forall t \in R, \exists! \Pi_t \in \text{Hom}(A[X], R)$ , s.t.  $\Pi_t(X) = t \wedge \forall a \in A (\Pi_t(a) = a)$ .

**Proof.** 不难验证

$$\Pi_t: \sum_{n \in \mathbb{N}} p_n X^n \mapsto \sum_{n \in \mathbb{N}} p_n t^n$$

即所求. □

我们把这样的  $\Pi_t(P) =: P(t)$  称为  $P$  在  $X = t$  时的取值, 或者说用  $t$  替换  $X$ . 当两个多项式不相等时, 它们的值却可能相等.

**Definition 4.2** (代数元和超越元). 若  $t \in R$  满足  $\exists P \in A[X]$  s.t.  $\exists n \in \mathbb{N} (p_n \neq 0) \wedge P(t) = 0$ , 那么  $t$  是  $A$  上的一个**代数元**. 若  $t \in R$  满足  $\Pi_t$  是单的, 那么我们称其为  $A$  上的一个**超越元**.

对于  $A = \mathbb{Q}, R = \mathbb{C}$  的情况, 代数元和超越元又被称为**代数数**和**超越数**.

## §5 整多项式环

**Theorem 5.1** (整性的继承). 如果  $A$  是整环,  $A[X]$  也是整环<sup>2</sup>.

**Proof.** 如果两个多项式都不是零多项式, 那么它们的最高次系数相乘不是零 (因为整环  $A$  没有零因子), 从而它们的乘积一定不是零多项式. □

类似于整数的带余除法, 我们可以建立整多项式环上的带余除法理论.

**Theorem 5.2** (多项式的带余除法). 设  $A$  是整环,  $F(X) \in A[X]$ , 其首项系数是  $A$  中的正则元 (i.e. 可逆).  $\forall G(X) \in A[X], \exists! Q(X), R(X) \in A[X]$  s.t.

$$F(X) = Q(X)G(X) + R(X) \wedge \deg R(X) < \deg G(X).$$

**Proof.** 设  $F(X) = \sum_{i \in \mathbb{N}^+} f_i X^i, G(X) = \sum_{j \in \mathbb{N}^+} g_j X^j$ , 其中  $n = \deg F(X), m = \deg G(X)$ .<sup>3</sup>

我们采取归纳法证明这样的  $Q(X), R(X)$  的存在性:  $n = 0$  时, 倘  $m > 0$ , 则令  $Q(X) = 0, R(X) = F(X)$ ; 倘  $m = 0$ , 则令  $R(X) = 0, Q(X) = f_0 g_0^{-1}$ .

若  $n > 0$ , 倘  $m > n$ , 则令  $Q(X) = 0, R(X) = F(X)$  即可; 倘  $m \leq n$ , 记

$$\bar{F}(X) := F(X) - f_0 g_0^{-1} X^{n-m} G(X).$$

<sup>2</sup>考虑到  $A$  是  $A[X]$  的子环, 逆命题也成立.

<sup>3</sup>这里排除了零多项式, 事实上, 它的情况是非常简单的, 只需让  $Q(X) = R(X) = 0$  即可.

因  $\deg \bar{F}(X) < \deg F(X)$ , 如若  $\bar{F}(X)$  满足可找到  $\bar{Q}(X)$  和  $R(X)$  s.t.  $\bar{F}(X) = \bar{Q}(X)G(X) + R(X)$ , 则令  $Q(X) = f_0 g_0^{-1} X^{n-m} + \bar{Q}(X)$ . 这里的  $Q(X)$ ,  $R(X)$  即所要找的.

综上,  $\forall n \in \mathbb{N}$  都成立.

现在我们需要证明唯一性.

倘若  $F(X) = Q(X)G(X) + R(X) = Q'(X)G(X) + R'(X)$ , 那么

$$[Q(X) - Q'(X)]G(X) = R(X) - R'(X) \quad (5-1)$$

由定理 4.1, 再考虑到  $A$  是一个整环, 假设  $Q(X) \neq Q'(X)$ ,  $R(X) \neq R'(X)$  我们能得到

$$\deg(R(X) - R'(X)) = \deg(Q(X) - Q'(X)) + \deg G(X).$$

从而我们得到  $\max\{\deg R(X), \deg R'(X)\} \geq \deg(R(X) - R'(X)) \geq \deg G(X)$ , 这和  $\deg R(X) < \deg G(X)$  矛盾. 从而, 要么  $Q(X) = Q'(X)$ , 要么  $R(X) = R'(X)$ , 而这两者因式 5-1 能互相推出.  $\square$

在整的多项式环中, 由首项可逆的  $G(X)$  和  $F(X)$  得到  $F(X) = Q(X)G(X) + R(X)$  的运算称为**多项式的带余除法** (polynomial long division). 这里  $F(X)$  被称为**被除式** (dividend),  $G(X)$  称为**除式** (divisor); 得到的  $Q(X)$  称为**商** (quotient) 而  $R(X)$  称为**余式** (remainder).

倘若余式  $R(X) = 0$ , 则称  $G(X)$  **整除**  $F(X)$ , 或  $F(X)$  被  $G(X)$  整除, 此时  $G(X)$  被称为  $F(X)$  的一个**因式** (factor or divisor), 而  $F(X)$  则是  $G(X)$  的一个**倍式** (multiple).

带余除法和  $\delta(P(X)) := \deg P(X)$ , 告诉我们, 如果  $\mathbb{F}$  是一个域 (从而任意非零多项式的首项都可逆了), 多项式环  $\mathbb{F}[X]$  是一个 Euclidean 整环 (定义 3.12), 从而也是唯一分解整环 (定理 3.7). 但是, 我们必须指出, 多项式环未必是 Euclidean 的, 而且即使不是 Euclidean 的, 也可能是唯一分解的. 例如, 当  $R$  是唯一分解整环时,  $R[X]$  也是一个唯一分解整环.

多项式环  $A[X]$  上的素元叫做**既约多项式**.

**Definition 5.1** (本原多项式). 设  $R$  是一个整环,  $P(X) \in R[X]$ . 多项式  $P(X)$  的所有系数的最大因<sup>4</sup>  $c(P)$  叫做多项式的**容度** (content). 如果  $c(P) \in U(R)$ , 那么  $P(X)$  被称为一个**本原多项式** (primitive polynomial). 一个非零多项式  $P(X)$  所有系数对  $c(P)$  (由最大因的定义, 它们都是容度的倍数) 的商为系数的多项式  $\text{pp } P(X)$  称为该多项式的**本原部分** (primitive part).

## §6 多项式的根

<sup>4</sup>最大因的定义可以递归地推广到任意有限多个元上

## 参考文献

- [1] A.I. Kostrikin. *Introduction to Algebra*. Universitext - Springer-Verlag. Springer-Verlag, 1982. ISBN: 9783540907114. URL: <https://www.springer.com/gp/book/9780387907116>.
- [2] 柯斯特利金 (俄罗斯). 代数学引论 (第 2 卷). 线性代数. 3rd ed. 俄罗斯教材选译. 高等教育出版社, 1991. ISBN: 9787040214918. URL: <http://gen.lib.rus.ec/book/index.php?md5=aed6abf2e5b956fd92baf7bd6298dec6>.

# 符号列表

这里列出了笔记中出现的重要符号.

$A^{-1}$ , 39	$\mathbb{F}_p$ , 12
$a/b$ , 13	$\langle g_0 \rangle$ , 4
$A^\dagger$ , 39	$g * S$ , 6
$A_{IJ}$ , 40	$G/N$ , 7
$A_{ij}$ , 40	$G \simeq G'$ , 5
$(a_{ij})_{i \in m, j \in n}$ , 38	$\gamma_{\mathcal{A}}(\lambda)$ , 30
$ a_{ij} _{i, j \in n}$ , 40	$\gcd(a, b)$ , 10
$A_n$ , 37	$I$ , 38
$A^T$ , 39	$\mathcal{I}$ , 27
$a b$ , 9	$\text{Inn}(G)$ , 5
$\text{Aut}(G)$ , 5	$[k]_n$ , 8
$c(P)$ , 44	$\ker f$ , 6
$\text{char}(F)$ , 13	$\mathcal{L}^-(V; \mathbb{F})$ , 23
$\chi_{\mathcal{A}}(X)$ , 31	$\mathcal{L}_p(V; U)$ , 22
$\text{Cl}(g)$ , 6	$\mathcal{L}^+(V; \mathbb{F})$ , 23
$\deg P(X)$ , 42	$\mathcal{L}(V)$ , 26
$\det$ , 23	$\mathcal{L}(V_0, \dots, V_{p-1}; U)$ , 22
$\text{diag}(a_{ii})_{i \in n}$ , 38	$\mathcal{L}(V, U)$ , 17
$E_{\mathcal{A}}(\lambda)$ , 30	$\text{lcm}(a, b)$ , 11
$\text{End}(V)$ , 26	$M_{IJ}$ , 40
$\varepsilon_\pi$ , 37	

$M_{ij}$ , 40 $M_{m \times n}(\mathbb{F})$ , 38 $M_n(\mathbb{F})$ , 38 $\mu_{\mathcal{A}}(\lambda)$ , 31 $N \triangleleft G$ , 6 $\mathcal{O}$ , 38 $\mathcal{O}$ , 27 $\mathcal{O}_{m \times n}$ , 38 $P(X)$ , 42 $\text{pp } P(X)$ , 44 $Q(A)$ , 13 $R \cong R'$ , 7 $R[X]$ , 42 $\langle S \rangle$ , 4 $S * g$ , 6 $S_n$ , 3, 35 $S(X)$ , 3 $\text{Spec } \mathcal{A}$ , 30 $\text{tr}$ , 40 $U(R)$ , 8 $V^*$ , 20 $(X, *)$ , 2 $(X, *, e)$ , 2 $(\mathbf{x}_j)_{j \in n}$ , 38 $\mathbf{x} + L$ , 19 $\mathbb{Z}_n$ , 8 $\mathbb{Z}_p^*$ , 12

# 索引

- Abelian 群, 3
- Cayley 定理, 5
- domain, 8
- Euclidean 函数, 11
- Euclidean 整环, 11
- Fermat 小定理, 12
- Grassmann 恒等式, 18
- $n$  维向量, 38
- $n$  阶元, 4
- $p$ -线性型, 22
- $\pi$ -等价, 35
- Steintz 替换, 16
- 不变子空间, 30
- 不相交, 35
- 久期方程, 31
- 二元运算, 2
- 二次型, 24
- 亏数, 26
- 互补, 18
- 交换环, 7
- 交换的, 2
- 代数, 27
- 代数元, 43
- 代数子式, 40
- 代数数, 43
- 代数系统, 2
- 代数结构, 2
- 代数重数, 31
- 余元, 11
- 余向量, 20
- 余式, 44
- 倍式, 44
- 偶置换, 37
- 元素, 38
- 共变向量, 20
- 共轭, 5
- 共轭映射, 5
- 共轭类, 6
- 共轭转置, 39
- 内自同构群, 5
- 几何重数, 30
- 函数环, 8
- 分式域, 13

- 分配律, 7  
列向量, 38  
剩余类环, 8  
半群, 2  
单位元, 2  
单位阵, 38  
单同态, 7  
单态射, 6  
单的, 30  
单谱, 30  
双线性型, 23  
反变向量, 20  
反对称域, 8  
反对称的, 22  
变换群, 3  
可对角化的, 32  
可逆的, 3  
右可逆, 3  
右陪集, 6  
右零因子, 8  
合同, 39  
同态, 6, 7, 17  
同构, 5, 7, 17  
同构映射, 5  
向量, 14, 38  
向量空间, 14  
向量组, 14  
和, 2, 18  
唯一分解整环, 10  
商, 11, 44  
商元, 11  
商空间, 19  
商群, 7  
因子, 9  
因式, 44  
坐标, 15  
域, 12  
基底, 15  
多重线性型, 22  
多项式, 42  
多项式环, 42  
多项式的带余除法, 44  
奇偶性, 37  
奇置换, 37  
子半群, 3  
子域, 12  
子么半群, 3  
子式, 40  
子环, 7  
子空间, 15  
子群, 3  
完备正交组, 29  
容度, 44  
对偶基底, 20, 21  
对偶空间, 20  
对称的, 22  
对角矩阵, 38  
左可逆, 3  
左正规, 3  
左陪集, 6  
常数项, 42  
幂零指数, 28  
幂零算子, 28  
平凡群, 3  
平凡零因子, 8  
么半群, 2  
张出, 15  
循环, 35

- 循环群, 4
- 态射, 6, 7
- 扩域, 12
- 投影, 29
- 整数环, 7
- 整环, 8
- 整除, 9, 44
- 斜域, 8
- 方阵, 38
- 无穷维线性空间, 15
- 既约元, 9
- 既约多项式, 44
- 最大因, 10
- 最大线性无关组, 16
- 最小倍, 11
- 最高次项系数, 42
- 有限么半群, 2
- 本原多项式, 44
- 本原部分, 44
- 极化的, 24
- 极小多项式, 27
- 标准型, 24
- 核, 6, 7
- 模  $n$  的剩余类的导出集, 8
- 模  $n$  的剩余类环, 8
- 次数, 42
- 正交等方矩阵组, 29
- 正交等方算子组, 29
- 正则元, 9
- 正规子群, 6
- 满同态, 7
- 满态射, 6
- 特征, 13
- 特征值, 30
- 特征向量, 30
- 特征多项式, 31
- 特征方程, 31
- 特征空间, 30
- 环, 7
- 生成, 15
- 生成元, 4
- 直和, 18
- 相伴元, 9
- 相似, 39
- 真子群, 3
- 矩阵, 38
- 矩阵的和, 39
- 矩阵的积, 39
- 秩, 16, 26
- 积, 2
- 符号, 37
- 等方算子, 29
- 类函数, 6
- 类数, 6
- 系数, 42
- 素元, 9
- 素分解, 9
- 素域, 13
- 纯量, 14
- 线性函数, 19
- 线性包络, 14
- 线性变换, 25
- 线性型, 19
- 线性多项式, 42
- 线性无关, 15
- 线性映射, 25
- 线性泛函, 19



线性独立, 15  
线性的, 25  
线性相关, 15  
线性空间, 14  
线性算子, 25  
线性算子代数, 27  
线性组合, 14  
结合的, 2  
维数, 15  
置换幺半群, 2  
置换群, 3, 35  
群, 3  
  
自同态, 6  
自同构, 5  
自同构群, 5  
自然同构, 21  
行列式, 23, 29, 40  
行向量, 38  
被除元, 11  
被除式, 44  
规范基底, 24  
谱, 30  
谱点, 30  
超越元, 43  
超越数, 43  
轨道, 35

轨道长度, 35  
转换矩阵, 17  
转置, 39  
轮换, 35  
轮换长度, 35  
迹, 29  
  
逆, 3, 39  
逆元, 3  
逆算子, 27  
酉性, 14  
配极, 24  
阶, 2  
阶数, 4  
除元, 11  
除式, 44  
除环, 8  
陪集, 6  
零元, 2  
零化, 27  
零化度, 26  
零因子, 8  
零多项式, 42  
非结合环, 7  
首子式, 40  
首项系数, 42