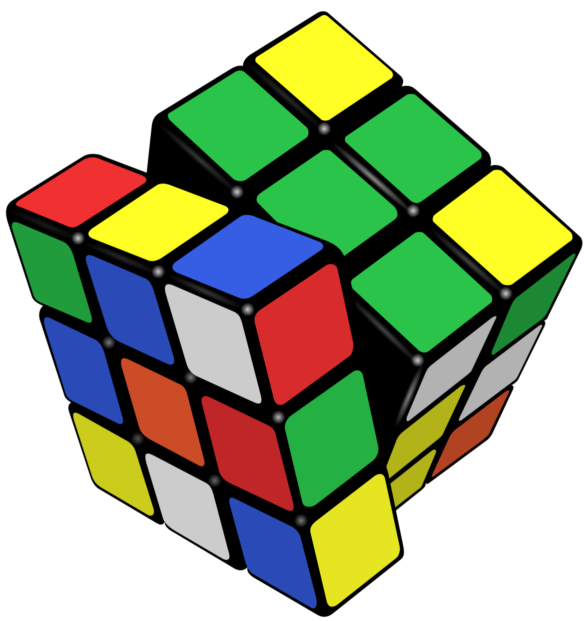
Algebra

Hoyan Mok[1]

2020 年 8 月 21 日



[1]E-mail: 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 TeX 源文档. 封面的来源是https://commons.wikimedia.org/wiki/File:Rubik%27s_cube.svg.

目录

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 $*\colon X^2 \to X$ 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 $\forall x \in A\big(e*x = x*e = x\big)$, 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 (半群和幺半群)**.** 若 $*$ 是结合的, 称 $(X,*)$ 是**半群** (semigroup); 若 $*$ 还有一个单位元, 则称 $(X,*,e)$ 是**幺半群** (monoid).

倘若幺半群 $(M,*,e)$ 是有限的 (即其元素有限), 称 $\operatorname{card} M$ 为**有限幺半群**的**阶**.

作为重要的例子, **置换幺半群** 定义为 $(X^X, \circ, \mathrm{id}_X)$, 有幺半群结构的 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:

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

同理 $x_1 + x_2 + \cdots + x_n$ 为:

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

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:

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

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

在幺半群中, 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**. 同理有幺半群M 的**子幺半群**M'.

若半群 $(S, *, e)$ 的元素 a 满足 $\exists a' \in S\big(aa' = a'a = e\big)$, 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** $\exists y$ s.t. $y * x = 1$ 或**右可逆**的概念.

§2 群

可逆幺半群 G 称为群, 即:

Definition 2.1 (群)**.** 设有集合 G. 若:

G1) 定义了二元运算 $\cdot \colon G^2 \to G; (x, y) \mapsto xy$.

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, $(S(X), \circ, \mathrm{id}_X)$ 是一个群, 称为**变换群**或**置换群**, 其中 $\circ$ 是函数的复合, id_X 是恒等变换. 当它的阶数 $\operatorname{card} X = n$ 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) $x \in G' \to x^{-1} \in G'$,

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**[1].

[1] [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, $\to$ 是显然的, 下给出 $\leftarrow$ 的证明:

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

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

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

□

这里将不加证明地给出:

Lemma 1. *群 G 的子群族 $\mathscr{H}=\{H\mid H$ 是 G 的子群$\}$ 的交 $\cap\mathscr{H}$ 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. $\langle S\rangle=\left\{\prod_{i=0}^{n-1}s_i\middle|\forall i\in n(s_i\in S\vee s_i^{-1}\in S)\right\}$.

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

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

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 $\operatorname{card}\langle g\rangle$ 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:*

$$g^n=e\ \leftrightarrow\ n=kq,\qquad n\in\mathbb{Z}. \tag{2-2}$$

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: $\exists f\colon G\to G'$ s.t.

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

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.

$$\mathrm{card}\langle g_0 \rangle = \mathrm{card}\langle g_0' \rangle \to \langle g_0 \rangle \simeq \langle g_0' \rangle\,.$$

Proof. 倘若 $\mathrm{card}\langle g_0 \rangle = \infty$, 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 $f\colon \mathbb{Z} \to \langle g_0 \rangle$, 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 $f\colon g^k \to g'^k$, 其中 $k = 0, 1, \cdots, \mathrm{card}\langle g_0 \rangle$. $\square$

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

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

若 $\varphi\colon G \to G$ 见证了 $G \simeq G$ (如 id_G), 那么称 φ 是群 G 的一个 **自同构** (automorphism). 所有自同构组成的集合 $\mathrm{Aut}(G)$ 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 $\mathrm{Inn}(G) := \{I_a\colon g \mapsto aga^{-1} \mid a \in G\}$, 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 $\exists I_g \in \mathrm{Inn}(G)$, 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 $\mathrm{Cl}(g)$, g 为其代表元. 称 $\mathrm{card}\{\mathrm{Cl}(g) \mid g \in G\}$ 为 G 的**类数** (class number). 如果有一个函数 f 满足 $g' \in \mathrm{Cl}(g) \to f(g) = g(g')$, 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 $\forall I \in \mathrm{Inn}(G)$, $I(N) = N$, 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 $f\colon G \to G'$ 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

$$f\colon G \to \mathrm{Inn}(G);\; g \mapsto I_g$$

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**:

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

对 $\forall a, b, c \in R$ 成立.

那么, 我们称 $(R, +, \cdot)$ 是一个**环** (ring)[2]. 而且唤 $(R, +)$ 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

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

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 $R \cong R'$.

[2] 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:

$$f+g\colon x\mapsto f(x)+g(x);\qquad fg\colon x\mapsto f(x)g(x),$$

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

作为例子, 考虑到将 $[k]_n\in\mathbb{Z}/\equiv \mathrm{mod} n$ 映射到 $n^{\mathbb{Z}}\ni \mathrm{mod} n := \{(m,k)\in\mathbb{Z}\times m \mid n\equiv k \bmod n\}$ 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**, 我们能用加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**[3]. 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. □

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, $U(R):=\{x\in R\mid x$ 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. □

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.

[3] [1] 中把 0 排除在外了.

§4 域

交换除环 F 称为**域** (field)[4]. 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 $[0]$, $[1]$, ..., $[p-1]$. 由素数的定义, $\forall [k] \in \mathbb{Z}_p^* := \mathbb{Z}_p - \{[0]\}$,

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

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 $\mathrm{GF}(p)$. 值得一提的是, p^n 元有限域 $\mathrm{GF}(p^n)$ 也是存在的.

Corollary 1 (***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, $I_{[k]}\colon \mathbb{Z}_p^* \to \mathbb{Z}_p^*; [n] \mapsto [kn]$ 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 $[a]^{p-1} = [1]$. □

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. □

[4]作为总结: 域上定义了加法和乘法, 加法是 Abelian 群, 乘法是 Abelian 幺半群, 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.

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, $P := \{o, e, 2e, \cdots, (p-1)e\}$ 即构成了与 $\mathbb{Z}_p$ 同构的素子域. □

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 $\mathrm{char}(F) = p$; 特别地, 定义 $\mathrm{char}(F) = 0$, 如果不存在这样的 p.

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: $\mathbb{F} \times V \to V$; $(\lambda, \boldsymbol{x}) \mapsto \lambda\boldsymbol{x}$ 且满足:

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

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 $(\boldsymbol{x}_i)_{i \in I}$ 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 $\forall i \in n$, $\lambda_i \in \mathbb{F}$, $\boldsymbol{x}_i \in V$, n 是正整数, 那么

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

称为向量组 $(\boldsymbol{x}_i)_{i \in n}$ 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, $(\boldsymbol{x}_i)_{i \in n}$ 是其中的一个向量组, n 是正整数. 其**线性包络** (linear span) 定义为

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

或者, 设 $M \subset V$, 那么其线性包络定义为

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

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. $\forall \boldsymbol{x} \in V', \forall \lambda \in \mathbb{F}, \lambda \boldsymbol{x} \in V'$, 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 $(\boldsymbol{x}_i)_{i\in n}$. 若 $\exists (\alpha_i)_{i\in n} \in \mathbb{F}^n$ s.t. $\exists i \in n(\alpha_i \neq 0)$ 且

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

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

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

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

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

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

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, $\dim\{\boldsymbol{0}\} = 0$.

Definition 5.7 (基底)**.** 设 V 是 $\mathbb{F}$ 上的 n 线性空间, $(\hat{\boldsymbol{e}}_i)_{i\in n}$ 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 $\varnothing$ 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 $\{\hat{\boldsymbol{e}}_i\}_{i\in n}$ 表示它.

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

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

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, $(\boldsymbol{v}, \hat{\boldsymbol{e}}_0, \cdots, \hat{\boldsymbol{e}}_{n-1})$ 线性相关, 从而 $\exists \alpha \in \mathbb{F}\, \exists (\alpha_i)_{i\in n} \in \mathbb{F}^n$ s.t. $(\alpha, \alpha_0, \cdots, \alpha_{n-1})$ 不全为 0 且

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

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 $(-\alpha_i/\alpha)_{i\in n}$. □

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

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

Corollary 2. *设 V' 是 V 的子空间. 如果 $V' \subsetneq V$, 那么 $\dim V' < \dim V$.*

Corollary 3. *如果线性无关的向量组 $(\boldsymbol{e}_j)_{j\in n}$ 满足 $\forall j \in n$, $\boldsymbol{e}_j \in \langle \boldsymbol{f}_i \rangle_{i\in m}$, 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 $(\boldsymbol{x}_j)_{j\in m}$ 是线性空间 V 的向量组.*

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

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 $\langle \boldsymbol{x}_j \rangle_{j\in m}$ 中取出一组基底共 r 个线性无关的向量, 这是违背推论 3 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. □

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

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

是 V 的一组基底.

Proof. 取 i_0 使得 $\hat{\boldsymbol{e}}_{i_0} \notin \langle \hat{\boldsymbol{f}}_i \rangle_{i\in s}$; 接着取 i_{k+1} 使得 $\hat{\boldsymbol{e}}_{i_{k+1}} \notin \langle \hat{\boldsymbol{f}}_0, \cdots, \hat{\boldsymbol{f}}_{s-1}, \hat{\boldsymbol{e}}_{i_k} \rangle$, 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 $(\hat{\boldsymbol{e}}_i)_{i\in n}$ 表出, 从而也就可以由 $(\hat{\boldsymbol{f}}_0, \cdots, \hat{\boldsymbol{f}}_{s-1}, \hat{\boldsymbol{e}}_{i_0}, \cdots, \hat{\boldsymbol{e}}_{i_{t-1}})$ 表出，从而 $s+t \geq n$.

另一方面, 不难通过归纳得知, $(\hat{\boldsymbol{f}}_0, \cdots, \hat{\boldsymbol{f}}_{s-1}, \hat{\boldsymbol{e}}_{i_0}, \cdots, \hat{\boldsymbol{e}}_{i_{t-1}})$ 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. □

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

$$\hat{\boldsymbol{f}}_i = \sum_{j\in n} a_{ji} \hat{\boldsymbol{e}}_j\,, \qquad \forall i \in n\,. \tag{5-1}$$

这里的 a_{ji} 决定了矩阵

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

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 §8). 让我们引入矩阵和与积的概念[1], 用 $\hat{f}$ 把 $\hat{e}$ 表出, 就可以得到转换矩阵的逆 $\boldsymbol{A}^{-1}$. 这两个矩阵之间的关系是 $\boldsymbol{A}\boldsymbol{A}^{-1} = \boldsymbol{A}^{-1}\boldsymbol{A} = \boldsymbol{I}$.

设 $\boldsymbol{v} \in V$,

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

那么,

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

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

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

1) f 是双射;
2) $\forall \alpha, \beta \in \mathbb{F}$, $\forall \boldsymbol{u}, \boldsymbol{v} \in V$, $f(\alpha\boldsymbol{v} + \beta\boldsymbol{u}) = \alpha f(\boldsymbol{v}) + \beta f(\boldsymbol{u})$,

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 $\boldsymbol{v}$ 和一组基底 $\hat{e}$, 向量 $\boldsymbol{v}$ 到它的坐标 $\boldsymbol{v}|_{\hat{e}} \in \mathbb{F}^n$ 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 U, W 都是 V 的子空间, 定义[2]

$$U + W := \langle U \cup W \rangle = \{\boldsymbol{u} + \boldsymbol{w} \mid \boldsymbol{u} \in U,\ \boldsymbol{w} \in U\}$$

为 U 和 W 的**和**. 若 $U \cap W = \varnothing$, 那么记 $U \oplus W := U + W$, 称为**直和**.

[1] 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].

[2] 这里不用 $+$ 表示集合的并.

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 $(\hat{\boldsymbol{e}}_0,\cdots\hat{\boldsymbol{e}}_{m-1};\ \hat{\boldsymbol{f}}_0,\cdots,\hat{\boldsymbol{f}}_{k-m-1})$, $\dim V$ 可取基底 $(\hat{\boldsymbol{e}}_0,\cdots\hat{\boldsymbol{e}}_{m-1};\ \hat{\boldsymbol{g}}_0,\cdots,\hat{\boldsymbol{g}}_{\ell-m-1})$, 那么

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

接下来我们证明向量组

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

线性独立. 若存在非平凡的线性组合:

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

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. □

Corollary 4. *若 $U=\sum_{i\in m}U_i$ 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. □

Theorem 5.7. *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 $\operatorname{codim}U=\dim V-\dim U$.

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 $\boldsymbol{x}+L:=\{\boldsymbol{x}+\boldsymbol{y}\mid\boldsymbol{y}\in L\}$, 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:

$$\alpha(\boldsymbol{x}+L):=\alpha\boldsymbol{x}+L\,,$$

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:

$$\boldsymbol{x} \equiv \boldsymbol{x}' \mod L \;\leftrightarrow\; \boldsymbol{x} - \boldsymbol{x}' \in L\,.$$

Theorem 5.8. *设 V 的子空间 U 和 W 互余, 那么*

$$f\colon W \to V/U;\; \boldsymbol{w} \mapsto \boldsymbol{w} + U$$

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

$$\boldsymbol{v} + U = (\boldsymbol{u} + \boldsymbol{w}) + U = (\boldsymbol{x} + U) + (\boldsymbol{w} + U) = U + (\boldsymbol{w} + U) = \boldsymbol{w} + U = f(\boldsymbol{w})\,,$$

所以 f 是满的. 满射 f 的单性由

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

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 $f\colon V \to \mathbb{F}$ 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 ℓ, 它作用于 $\boldsymbol{x} \in V$ 时, 设基底为 $\hat{e}$, 那么:

$$\ell\colon \boldsymbol{x} \mapsto \boldsymbol{\ell}|_{\hat{e}}\, \boldsymbol{x}|_{\hat{e}}\ ,$$

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

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

即:

$$\boldsymbol{\ell}|_{\hat{f}} = \boldsymbol{P}\, \boldsymbol{\ell}|_{\hat{e}}\ . \tag{6-1}$$

定义线性型的线性组合 $\alpha f + \beta g$ 为:

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

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 $0_V : \boldsymbol{x} \mapsto 0$.

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 ℓ_i 表示共变向量, 并引入 Einstein 求和约定的, 见之后第五章.

我们继续以 n 维线性空间为例子. 设 V 中有基底 $\hat{e} = (\hat{\boldsymbol{e}}_i)_{i\in n}$, 取 V^* 的基底 $\hat{e}^* := (\hat{\boldsymbol{e}}_i^*)_{i\in n}$, 使得 $\hat{\boldsymbol{e}}_i^*(\hat{\boldsymbol{e}}_i) = \delta_{ij}$, 其中 δ_{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 $\varepsilon\colon V \to V^{**}$ 定义如下:*

$$\boldsymbol{x} \mapsto \varepsilon_{\boldsymbol{x}}\,; \quad \varepsilon_{\boldsymbol{x}}\colon V^* \to \mathbb{F}\,; f \mapsto f(\boldsymbol{x})\,.$$

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

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 $r := \dim L$, $\hat{e} := (\hat{\boldsymbol{e}}_i)_{i\in r}$ 是 L 的基底. 由定理 5.4, 将其扩充至 V 的基底 $(\hat{\boldsymbol{e}}_i)_{i\in n}$.

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

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

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

Proof. 根据定理 5.1, $\exists j_0 \in m$ 使得 $\boldsymbol{x}_{j_0}$ 是其他 $(\boldsymbol{x}_j)_{j\in m;\, j\neq j_0}$ 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 λ_j, 不改变行列式的值, 但该列变成了

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

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

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 $(\boldsymbol{x}_j)_{j\in n}$ 线性无关当且仅当

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

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 $\hat{x} = (\boldsymbol{x}_j)_{j\in n}$ 也是一组基底, 那么存在转换矩阵 $\boldsymbol{P}$, 而且它的行列式恰是 $\det(f_i(\boldsymbol{x}_j))_{i,j\in n}$. 转换矩阵是可逆的, 它的行列式非零. □

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 $\langle \boldsymbol{x}_j \rangle_{j\in m}$ 的维数 r 等于

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

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

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

□

Corollary 5. 设 V 是 n 维线性空间, 有基底 $\hat{e}$, 向量组 $(\boldsymbol{x}_j)_{j\in m}$ 的维数等于矩阵 $(\boldsymbol{x}_j|_{\hat{e}})_{j\in m}$ 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 $V_0, V_1, \ldots, V_{p-1}, U$ 是 $\mathbb{F}$ 上的线性空间. 若映射

$$f\colon \prod_{i\in p} V_i \to U$$

满足 $\forall i \in p$,

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

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

如 $V_0 = V_1 = \cdots = V_{p-1}$, 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 $\forall \pi \in S_p$, $\forall (\boldsymbol{x}_i)_{i\in p} \in V^p$,

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

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

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

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) $\det \boldsymbol{I} = 1$, 其中 $\boldsymbol{I} = (\delta_{ij})_{i,j\in n}$,

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

第三章　线性算子

§8　线性映射

Definition 8.1 (线性映射)**.** 设 V, W 是域 $\mathbb{F}$ 上的线性空间. 如映射 $\mathscr{A} \in \mathcal{L}(V, W)$, 即 $\mathscr{A}$ 是 V 到 W 的一个同态, 那么我们称 $\mathscr{A}$ 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**[1]或**线性算子**.

Theorem 8.1. *设 $\mathscr{A} \in \mathcal{L}(V, W)$, 倘若 $(\boldsymbol{v}_i)_{i\in s} \in V^s$,*

$$f\left(\langle \boldsymbol{v}_i \rangle_{i\in s}\right) = \langle f(\boldsymbol{v}_i) \rangle_{i\in s} .$$

Corollary 6. *设 $\mathscr{A} \in \mathcal{L}(V, W)$, 而 U 是 V 的有限维子空间, 那么 $\dim f(U) \le \dim U$.*

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

$$\mathscr{A}|_{\hat{e},\,\hat{f}} := \boldsymbol{A} = (a_{ij})_{i\in n,\, j\in m} = \Big(f(\hat{\boldsymbol{e}}_j)|_{\hat{f}} \Big)_{j\in m} \tag{8-1}$$

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

Theorem 8.2. *由式 (8-1) 决定的线性映射和 $\mathbb{F}$ 上的 $m \times n$ 矩阵是一一对应的, 且:*

$$(\mathscr{B} \circ \mathscr{A})|_{\hat{e},\,\hat{g}} = \boldsymbol{B}\boldsymbol{A}\,, \tag{8-2}$$

其中 $\mathscr{A}\colon V \to U$, $\mathscr{B}\colon U \to W$, 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 (8-1) 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 $f(\boldsymbol{v})|_{\hat{f}} = \boldsymbol{A}\,\boldsymbol{v}|_{\hat{e}}$ 决定的映射是 $\mathcal{L}(V, W)$ 的元素.

[1] 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 (8-2) 则由下式给出:

$$(\mathscr{B}\circ\mathscr{A})(\boldsymbol{v})|_{\hat{g}} = \mathscr{B}\big(\mathscr{A}(\boldsymbol{v})\big)\big|_{\hat{g}} = \boldsymbol{B}\,\mathscr{A}(\boldsymbol{v})|_{\hat{f}} = \boldsymbol{B}\boldsymbol{A}\,\boldsymbol{v}|_{\hat{e}}\,.$$

□

Definition 8.2 (秩)**.** 设 $\mathscr{A}\in\mathcal{L}(V,W)$, 记 $\operatorname{rank}\mathscr{A} := \dim\mathscr{A}(V)$ 为线性映射 $\mathscr{A}$ 的**秩**. 同时我们称 $\dim\ker\mathscr{A}$ 为其**亏数**或**零化度** (nullity).

Theorem 8.3. *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 $\operatorname{rank}\mathscr{A} = \operatorname{rank}\boldsymbol{A}$, 其中 $\boldsymbol{A} = \mathscr{A}|_{\hat{e},\hat{f}}$.*

Proof. 由定义式 (8-1), 矩阵的列向量组将张出 $\mathscr{A}(V)$. 由5.3, 这就给出了我们的定理[2]. □

Theorem 8.4. *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, $\mathscr{A}\in\mathcal{L}(V,W)$, 那么*

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

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

取 $\ker\mathscr{A}$ 的一组基底 $(\hat{\boldsymbol{e}}_i)_{i\in k}$ (显然 $k\le n$), 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 $\mathscr{A}(V) = \langle\mathscr{A}(\hat{\boldsymbol{e}}_i)\rangle_{i\in n}$. 但 $\langle\mathscr{A}(\hat{\boldsymbol{e}}_i)\rangle_{i\in k} = \{\boldsymbol{0}\}$. 利用 $\mathscr{A}$ 的线性, 我们给出 $\forall(\lambda_i)_{i\in n}\in\mathbb{F}^n$:

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

即是: $\big(\mathscr{A}(\hat{\boldsymbol{e}}_i)\big)_{i\in n\,\wedge\, i\notin k}$ 将构成 $\mathscr{A}(V)$ 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.

§9 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 $\operatorname{End}(V)$. 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

[2] 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 5保证.

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

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

Definition 9.1 (逆算子)**.** 设 $\mathscr{A}, \mathscr{B} \in \mathcal{L}(V)$. 若

$$\mathscr{A}\mathscr{B} = \mathscr{B}\mathscr{A} = \mathrm{id}_V\,,$$

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

Theorem 9.1. *设 V 是有限维线性空间, $\mathscr{A} \in \mathcal{L}(V)$.*

$$\exists \mathscr{B} \in \mathcal{L}(V)\left(\mathscr{A} = \mathscr{A}^{-1}\right) \;\leftrightarrow\; \operatorname{rank} \mathscr{A} = \dim V \;\leftrightarrow\; \ker \mathscr{A} = \{\mathbf{0}\}\,.$$

Proof. 利用定理 8.4 立刻就能证明. □

Definition 9.2 (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:

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

那么我们称 A 是 $\mathbb{F}$ 上的一个**代数** (algebra)[3]. 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 $X = \mathscr{A} \in \mathcal{L}(V)$ 时的取值, 即 $\mathbb{F}[\mathscr{A}]$ (我们记 $\mathscr{A}^0 := \mathrm{id}_V$), 可以验证是 $\mathcal{L}(V)$ 的子代数.

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

Definition 9.3 (极小多项式)**.** 设 V 是域 $\mathbb{F}$ 上的线性空间, $\mathscr{A} \in \mathcal{L}(V)$, $P(X) \in \mathbb{F}[X]$. 如果 $P(\mathscr{A}) = \mathscr{O}$, 那么称多项式 $P(X)$ **零化**线性算子 $\mathscr{A}$. 首项系数为 1 的零化 $\mathscr{A}$ 的多项式称为其**极小多项式**, 可记为 $\mu_{\mathscr{A}}(X)$.

Theorem 9.2 (极小多项式存在)**.** *设 V 是域 $\mathbb{F}$ 上的 n 维线性空间. $\forall \mathscr{A} \in \mathcal{L}(V)$, 都存在极小多项式 $\mu_{\mathscr{A}}(X)$, 且 $\deg \mu_{\mathscr{A}}(X) = \dim \mathbb{F}[\mathscr{A}]$.*

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

如果次数 $< n^2 + 1$ 的非零多项式 $P(X)$ 都不能零化 $\mathscr{A}$, 我们即可说: $\mathrm{id}_V, \mathscr{A}, \cdots, \mathscr{A}^{n^2+1}$ 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. □

[3]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 9.3 (极小多项式唯一)**.** 设 V 是域 $\mathbb{F}$ 上的线性空间, $\mathscr{A} \in \mathcal{L}(V)$. 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 $\mathscr{A}$ 的极小多项式, 那么 $(p_i)_{i\in n} = (q_i)_{i\in n}$.

Proof. 因为 $\mathbb{F}[\mathscr{A}]$ 是一个代数, $P(\mathscr{A}) - Q(\mathscr{A}) = \sum_{i\in n}(p_i - q_i)\mathscr{A}^i = \mathscr{O}$. 我们得到了一个能零化 $\mathscr{A}$ 次数小于 n 的多项式. 如果它不是零多项式, 记 $m = \deg\big(P(X) - Q(X)\big)$, 那么 $\frac{1}{p_m - q_m}\sum_{i\in n}(p_i - q_i)X^i = \mathscr{O}$ 将是一个首项为 1 的零化 $\mathscr{A}$ 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. □

Theorem 9.4 (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, $\mathscr{A} \in \mathcal{L}(V)$, 其极小多项式是 $\mu_{\mathscr{A}}(X)$. 算子 $\mathscr{A}$ 可逆当且仅当 $\mu_{\mathscr{A}}$ 的常数项非零.

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

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

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

如果极小多项式常数项不为 0,

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

给出了 $\mathscr{A}$ 的逆. □

Theorem 9.5 (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 $\mathscr{A} \in \mathcal{L}(V)$ 的多项式 $P(X) \in \mathbb{F}[X]$ 一定是 $\mu_{\mathscr{A}}(X)$ 的倍式.

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

Definition 9.4 (幂零算子)**.** 设 V 是域 $\mathbb{F}$ 上的线性空间. 线性算子 $\mathscr{A} \in \mathcal{L}(V)$ 如果满足 $\exists m \in \mathbb{N}_+$ 使得 $\mathscr{A}^m = \mathscr{O}$, 那么称其是一个**幂零算子** (nilpotent operator). 数 $d := \min\{m \in \mathbb{N}_+ \mid \mathscr{A}^m = \mathscr{O}\}$ 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 9.6 (幂零算子的极小多项式)**.** 设 V 是域 $\mathbb{F}$ 上的线性空间. 若 $\mathscr{A} \in \mathcal{L}(V)$ 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 9.7 (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 $\boldsymbol{A}$ 和 $\boldsymbol{A}'$ 分别是 $\mathscr{A} \in \mathcal{L}(V)$ 在基底 $\hat{e}$ 和 $\hat{e}'$ 下的矩阵, 那么:*

$$\boldsymbol{A}' = \boldsymbol{P}^{-1}\boldsymbol{A}\boldsymbol{P},$$

其中 $\boldsymbol{P}$ 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 9.8 (不变量)**.** *设 $\boldsymbol{A}, \boldsymbol{A}' \in M_n(\mathbb{F})$. 设 V 是域 $\mathbb{F}$ 上的 n 维线性空间. 若 $\boldsymbol{A}$ 和 $\boldsymbol{A}'$ 分别是 $\mathscr{A} \in \mathcal{L}(V)$ 在基底 $\hat{e}$ 和 $\hat{e}'$ 下的矩阵, 那么:*

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

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

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 id_n.

不难证明 $\operatorname{card} S_n = \mathrm{P}_n^n = n!$.

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 **π-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 π 的**轨道**, 其元素个数 $\ell_k := \operatorname{card} n_k$ 称为**轨道 n_k 的长度**.

为方便, 我们定义 π_k 为:

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

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

我们称两个轮换**不相交**, 如果它们的长度 ≤ 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 id_n, 要么存在唯一的不相交长度 ≤ 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 π 都可写为对换 $(\sigma_k)_{k\in q}$ 的乘积, 即 $\pi = \prod_{k\in q} \sigma_k$[1].*

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

[1]注意, 这时不可对调 σ_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 $\mathrm{id}_n=\prod_{k\in q}\sigma_k$, 其中 $\forall k\in q$, σ_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

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

那么重新令

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

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

3) 如果 $\sigma_{p-1}=(r,u)$, 其中 $\{r,u\}\cap\{S,t\}=\varnothing$: 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 $\mathrm{id}_n=\prod_{k\in q}\sigma'_k$. 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 $\mathrm{id}_n(S)=S$ 矛盾; 那么, 只可能是满足 b), 此时因 $(S,t)(S,t)=\mathrm{id}_n$, 将它们消去, 我们得到了 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 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 π 的两种分解, $\pi=\prod_{k\in q}\sigma_k=\prod_{k\in q'}\sigma'_k$, 那么 $\mathrm{id}_n=\pi\pi^{-1}=\prod_{k\in q}\sigma_k^{-1}\prod_{k\in q'}\sigma'_k=\prod_{k\in q}\sigma_k\prod_{k\in q'}\sigma'_k$, 由前 $q+q'\equiv 0 \pmod 2$. □

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** ε_π, 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:

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

式 (2-1) 定义的 $\boldsymbol{A}$ 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 $\boldsymbol{O}$, 有时为了强调它的尺寸, 将之写在右下角 i.e. $\boldsymbol{O}_{m\times n}$.

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

$$\boldsymbol{A} := (\boldsymbol{x}_j)_{j\in n}, \qquad \forall j \in n\big(\boldsymbol{x}_j \in \mathbb{F}_n\big)\,. \tag{2-2}$$

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

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

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

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

不难验证, $(M_{m\times n}, +, \boldsymbol{O}_{m\times n})$ 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**($\cdot\colon M_{m\times\ell}(\mathbb{F})\times M_{\ell\times n}(\mathbb{F}) \to M_{m\times n}(\mathbb{F})$):

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

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.

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

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

不难看出, 相似关系是一个等价关系.

Definition 2.8 (迹)**.** 设 $\boldsymbol{A} = (a_{ij})_{i,j\in n}\in M_n(\mathbb{F})$. 方阵 $\boldsymbol{A}$ 的迹定义为 $\operatorname{tr}\boldsymbol{A} := \sum_{i\in n} a_{ii}$.

Theorem 2.1 (迹的交换性)**.** 设 $\boldsymbol{A}, \boldsymbol{B}\in M_n(\mathbb{F})$. $\operatorname{tr}(\boldsymbol{A}\boldsymbol{B}) = \operatorname{tr}(\boldsymbol{B}\boldsymbol{A})$.

Proof.

$$\boldsymbol{A}\boldsymbol{B} = \left(\sum_{k\in n} a_{ik}b_{kj}\right), \quad \boldsymbol{B}\boldsymbol{A} = \left(\sum_{k\in n} b_{ik}a_{kj}\right).$$

从而

$$\operatorname{tr}(\boldsymbol{A}\boldsymbol{B}) = \sum_{i\in n}\sum_{k\in n} a_{ik}b_{ki} = \sum_{k\in n}\sum_{i\in n} b_{ki}a_{ik} = \operatorname{tr}(\boldsymbol{B}\boldsymbol{A})\,.$$

□

§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[1], 并给出它的一些性质.

[1] 几何解释可见于 [1].

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

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

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

Theorem 3.2. $\det \boldsymbol{A} = \det \boldsymbol{A}^{\mathrm{T}}$.

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

$$\det \boldsymbol{A}' = \lambda \det \boldsymbol{A}\,.$$

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

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

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

设 $I, J \in \mathscr{P}(n)$, 而 $|I| = |J|$. 记 $M_{IJ} := |a_{k\ell}|_{k\in n-I;\, \ell\in n-J}$ 为 $\boldsymbol{A}$ 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:

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

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

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[1]:

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

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

Theorem 4.2. 如果 A 是整环, $A[X]$ 也是整环[2].

[1] $R^{<\mathbb{N}} := \bigcup_{n\in\mathbb{N}} R^n$

[2] 考虑到 A 是 $A[X]$ 的子环, 逆命题也成立.

Theorem 4.3 (多项式环的泛性)**.** *设 R 是一个交换环, A 是 R 的子环. $\forall t \in R$, $\exists! \mathit{\Pi}_t \in \mathrm{Hom}(A[X], R)$, s.t. $\mathit{\Pi}_t(X) = t \wedge \forall a \in A\big(\mathit{\Pi}_t(a) = a\big)$.*

Proof. 不难验证

$$\mathit{\Pi}_t \colon \sum_{n\in\mathbb{N}} p_n X^n \mapsto \sum_{n\in\mathbb{N}} p_n t^n$$

即所求. □

我们把这样的 $\mathit{\Pi}_t(P) =: P(t)$ 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 $\mathit{\Pi}_t$ 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**.

类似于整数的带余除法, 我们可以建立整的多项式环上的带余除法理论.

Theorem 4.4 (多项式的带余除法)**.** *设 A 是整环, $F(X) \in A[X]$, 其首项系数在 A 中可逆. $\forall G(X) \in A[X]$, $\exists! Q(X), R(X) \in A[X]$ s.t.*

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

Proof. 设 $F(X) = \sum_{i\in n^+} f_i X^i$, $G(X) = \sum_{j\in m^+} g_j X^j$, 其中 $n = \deg F(X)$, $m = \deg G(X)$. [3]

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

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

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.

现在我们还需要证明唯一性.

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

$$[Q(X) - Q'(X)]G(X) = R(X) - R'(X) \tag{4-1}$$

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

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

[3] 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.

从而我们得到 $\max\{\deg R(X), \deg R'(X)\} \geq \deg(R(X)-R'(X)) \geq G(X)$, 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 4-1 能互相推出. □

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), 而 $F(X)$ 则是 $G(X)$ 的一个**倍式** (multiple).

§5 多项式的根

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.

索引