數學傳播　31卷2期, pp. 21-31

線性代數五講——
第一講 一些基本的代數結構

龔　昇・張德健

1.1. 線性代數所研究的對象

首先我們要開宗明義地討論一下這一系列講章的主題: 什麼是線性代數? 它所研究的對象是什麼? 要說清楚這點, 先得弄清楚什麼是代數。而代數的定義是隨著時代的變化而不斷改變的, 我們不妨簡略的回顧一下。

我們都熟知小學裡學習的數學叫算術, 主要是討論數字的一些運算, 這些內容人們很早就知道了, 後來產生了數字符號化, 才改變了這種狀況。數字符號化就是用符號代替數字。這件事在我國發生在宋元時代, 當時有天元術和四元術。也就是將未知數記作天元, 後來將兩個三個和四個未知數記作天、地、人、物等四元, 也就是相當於現在用 x、y、z、u 來表達四個未知數。有了這些元, 也就可以了解一些代數方程與聯立方程組了。在西方, 徹底完成數字符號化是在十六世紀。數字符號化的產生標誌著代數學史前時期的結束和代數學的誕生。它包括了一元二次方程的求解, 多元一次方程組的求解等。而這些正是目前中學代數課的內容。從十七到十八世紀中期, 代數被理解爲在代數符號上進行的數學, 如解三次、四次代數方程, 給出這些方程的解法及根的表達式, 建立一些代數恆等式。從十八到十九世紀代數學的首要問題是求代數方程

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \tag{1.1.1}$$

的根式解, 及推導出由方程的係數經過加、減、乘、除以及開方所構成的公式來表示方程的根。在已知一次、二次、三次、四次代數方程的根式解後, 不知多少人企圖找出五次以及更高代數方程的根式解, 但都失敗了。直到1770年, J. Lagrange (1736∼1813) 看到了五次以及更高代數方程的根式無解。又過了半個世紀, 1824年, N. Abel (1802∼1829) 解決了這個問題, 即五次以及更高代數方程是不可能有根式解的。但什麼樣的代數方程能有根式解, 在1830年由 E. Galois (1811∼1832) 徹底解決了。他證明了：代數方程式有解若且唯若它的 Galois 群可解。Abel 與 Galois 不僅解決了三百年來無法解決的著名難題, 更重要的是：他們爲了解決這個

難題, 建立了體和群的概念, 爲後來誕生的近世代數作了準備。與此相關的問題是要證明方程 (**??**) 的根存在性; 即如方程 (**??**) 的係數是複數, 則至少有一個複根, 這就是著名的代數基本定理。十八世紀末, C.F. Gauss (1777∼1855) 給出了這個定理的證明。從十九世紀中葉, 代數學最終從方程式論轉向代數運算的研究。代數學及代數運算的一般理論與近代觀點, 於二十世紀初在 D. Hilbert (1862∼1943)、E. Steinitz(1871∼1928)、A. E. Noether (1882∼1935) 以及 E. Artin (1898∼1962) 等人的影響下得以明確。

近世代數的重要內容是集合及這些集合上的代數運算。集合本身和作爲代數運算的載體的集合是不加區分的, 故實質上研究的是代數運算本身。說更仔細些, 考慮非空集合S上一個或幾個二元運算。運算作用在集合兩元素之間得到的元素仍在集合中, 對集合實行運算要適合一些法則 (或稱公理), 則集合與其上的運算共同組成一代數結構。研究代數結構的性質是近世代數的內容與任務。主要的代數結構有：群、環、體、除環、模等等, 這將在下一節中仔細定義它們。

特別要強調的是：研究一個代數結構, 除了了解它的內部構造和結構性質外, 一個重要而基本的方法就是研究這個代數結構的表示, 或這個代數結構上的模。例如一個群上的模, 粗略地講, 就是這個群在一個向量空間上的作用, 作用的效果如何當然反映出這個群本身的性質; 而一個環上的模, 就是這個環在一個 Abel 群上的作用, 模本身既可以看成是一個代數結構, 更重要的, 它是一個代數結構在另一個代數結構上的作用。因此, 我們可以說現代代數學的兩大主題是結構與表示理論。

線性代數是研究線性空間 (向量空間)、模和其上的線性變換以及與之相關問題 (線性 (linear)、雙線性 (bilinear)、二次型式等) 的數學學科。也就是說, 代數結構是線性空間。僅僅討論線性空間的結構性質是不夠的, 還要考慮線性變換在其上的作用。從表示論的觀點來看, 帶有線性變換的線性空間成爲主理想整環上的模。這就是在這一系列講章中, 我們希望用模的觀點作爲考慮線性代數的出發點。

從這裡還可以看出, 線性代數所研究的對象是：線性空間; 而模是線性空間的擴充; 作用在線性空間上的線性變換, 大致上說, 線性變換就是將一個線性空間對應到另一個線性空間, 且保持線性空間中運算的映射; 定義在線性空間上的線性泛函及推廣雙線性形式, 而二次型式不過是雙線性形式的特例。因此, 可以說《線性》是線性代數的靈魂, 線性代數只考慮《線性》的問題, 而《非線性》的問題不在討論之列。

1.2. 主理想整環

我們先回顧一下一些重要的代數結構的定義。

A. 群 (group)

這是最基本、最重要的代數結構。群是一非空集合 G, 其上有一個二元運算 "$\circ$" 滿足：

1. (封閉性) 對所有 $a, b \in G$, 則 $a \circ b \in G$;
2. (結合律) 對所有 $a, b, c \in G$, 則 $(a \circ b) \circ c = a \circ (b \circ c)$;
3. (單位元之存在) G 中存在一元素 e, 使得對任意 $a \in G$, 都有 $a \circ e = e \circ a = a$;
4. (逆元素之存在) 對 G 中每一元素 a, 存在 G 中的元素 a^{-1}, 使得 $a \circ a^{-1} = a^{-1} \circ a = e$;
5. (交換律) 對所有 $a, b \in G$, 則 $a \circ b = b \circ a$, 則稱 G 爲 Abel 群 (Abelian group) 或交換群。此時運算 $\circ$ 稱爲加法, 並用 $+$ 來替代。若集合 G 只滿足條件1 及2, 則稱 G 爲半群 (semi-group)。

B. 環 (ring)

環是一非空集合R, 其上有兩個二元運算, 加法 (記作$+$) 和乘法滿足：

1. R 對加法成 Abel 群
2. R 對乘法成半群
3. (分配律) 對所有 $a, b, c \in R$, 則

$$(a + b)\, c = ac + bc;$$

及

$$c\,(a + b) = ca + cb;$$

若環 R 對乘法還滿足

4. (交換律) 對所有 $a, b \in R$, 則 $a\, b = b\, a$; 則稱 R 爲交換環。

若環 R 中有元素 e, 使得 $a\, e = e\, a = a$, 則稱 R 爲有單位元素 (identity) 的環, 單位元素記作 1。在這一系列的討論中, 我們討論的環是以交換環爲主。

使 $\alpha 1 = 0$ 的最小的正整數 α, 稱爲 R 的特徵 (characteristic)。若沒有這樣的 α, 則稱 R 的特徵爲 0。

C. 整域 (也叫整環, integral domain)

在交換環 R 中的非零元素 r, 如果存在非零元素 $s \in R$, 使得 $r\, s = 0$, 則稱 r 爲零因子 (zero divisor)。一個無零因子且有單位元的交換環稱爲整域。與之等價的說法：一個滿足消去律 (cancellation law) 的有單位元的交換環稱爲整域。消去律是：若 $x, y, r \in R$, $r \neq 0$, 則 $rx = ry$ 導出 $x = y$。

D. 除環 (division ring, 也叫斜體, skew field)

一個有單位元的環如果所有非零元素全體構成一乘法群, 則稱爲除環或斜體。也就是有乘法且具有單位元的環。

E. 體 (field)

可交換的斜體稱爲體。

F. 主理想整域 (principal ideal domain)

環 R 中的一個子集 I 稱爲 R 的理想 (ideal), 若其滿足

1. I 對 R 中的加法成 Abel 群;
2. 若 $a \in I$, $r \in R$, 則 $ar \in I$ 及 $ra \in I$。

如果將條件1. 換成

1′. I 中任意兩個元素 a, b, 滿足 $a - b \in I$; 我們不難證出條件1'及2與條件1及2等價。有一些書便是用條件1'及2來定義理想 (ideal)。

若 R 爲有單位元的交換環, S 爲 R 的一個部分集合, 則集合

$$\langle s_1, \ldots, s_n \rangle = \left\{ r_1 s_1 + \cdots + r_n s_n : \ r_j \in R, \ s_j \in S, \ j = 1, \ldots, n \right\}$$

爲 R 的一個理想, 稱爲由 S 生成 (generated) 的理想。我們稱由一個元素 a 生成的理想

$$\langle a \rangle = \left\{ ra : \ r \in R \right\}$$

爲由 a 生成的主理想 (principal ideal)。每一個理想都是主理想的整域稱爲主理想整域。

因爲我們下面的討論將著重在主理想整域上進行, 因此要再多說幾句。整數全體 $\mathbb{Z}$ 是整域, 且也是主理想整域。這是因爲 $\mathbb{Z}$ 的任一理想 I 都是由 I 中的最小正整數 a 生成。若 $\mathbb{F}$ 爲斜體, 所有係數在 $\mathbb{F}$ 上的單變量多項式的集合 $\mathbb{F}[x]$ 是一個有單位元素的交換環。若 $p(x), q(x) \in \mathbb{F}[x]$, 且 $p(x)q(x) = 0$, 則有 $p(x) = 0$ 或 $q(x) = 0$, 是故 $\mathbb{F}[x]$ 還是一個整域。不但如此, 在此要證明以下一個十分重要且有用的定理。

定理 1.2.1: $\mathbb{F}[x]$是主理想整域。

證明: 若 I 是 $\mathbb{F}[x]$ 的理想, $m(x)$ 是 I 中最低次的首一多項式 (monic polynomial), 即領導係數爲 1 的多項式。首先看出, 在 I 中, 這樣的多項式是唯一的。若還有另一個首一多項式 $n(x)$, 而且 $\deg n(x) = \deg m(x)$, 則

$$b(x) = m(x) - n(x) \in I.$$

將 $b(x)$ 乘以其最高次項係數的逆元素, 便得到一個首一多項式 $b_1(x)$, 而 $b_1(x) \in I$, 但 $\deg b_1(x) = \deg b(x) < \deg m(x)$, 故 $b_1(x) = 0$, 因此 $b(x) = 0$, 即 $n(x) = m(x)$。

繼續我們證明 I 由 $m(x)$ 生成。因爲 I 是一個理想且 $m(x) \in I$, 是故 $\langle m(x) \rangle \subset I$。現在來證反方向包含關係。若 $p(x) \in I$, 則 $p(x)$ 用 $m(x)$ 相除, 我們便得到

$$p(x) = q(x)m(x) + r(x),$$

這裡 $r(x)=0$ 或 $0\le \deg r(x)<\deg m(x)$。由於 I 是一個理想, 故

$$r(x)=p(x)-q(x)m(x)\in I.$$

將 $r(x)$ 乘以其最高次項係數的逆元素, 便得到一個首一多項式 $r_1(x)$, 而 $r_1(x)\in I$, 故 $0\le \deg r_1(x)<\deg m(x)$。由於 $m(x)$ 的次數是最低的, 所以, $r_1(x)=0$, 即 $r(x)=0$。換句話說

$$p(x)=q(x)m(x)\in\langle m(x)\rangle.$$

這就證明了 $I\subset\langle m(x)\rangle$。因此, $I=\langle m(x)\rangle$, 定理證畢。

我們還可以證明如下命題。

命題 1.2.1: 若 $p_1(x),\ldots,p_n(x)\in\mathbb{F}[x]$, 則

$$\langle p_1(x),\ldots,p_n(x)\rangle=\langle \gcd\{p_1(x),\ldots,p_n(x)\}\rangle,$$

這裡 $\gcd\{p_1(x),\ldots,p_n(x)\}$ 爲 $p_1(x),\ldots,p_n(x)$ 的最大公因子。

證明: 令 $I=\langle p_1(x),\ldots,p_n(x)\rangle$, 由定理 1.2.1 知道, 有 I 中唯一的一個最低次的首一多項式 $m(x)$, 使得 $I=\langle m(x)\rangle$。由於 $p_j(x)\in\langle m(x)\rangle$, 故有多項式 $a_j(x)\in\mathbb{F}[x]$, $j=1,\ldots,n$, 使得

$$p_j(x)=a_j(x)m(x)\qquad j=1,\ldots,n.$$

因此, $m(x)\mid p_j(x)$, $j=1,\ldots,n$, 即 $m(x)$ 是 $p_1(x),\ldots,p_n(x)$ 的公因子。假設 $q(x)\mid p_j(x)$, $j=1,\ldots,n$, 則 $p_j(x)\in\langle q(x)\rangle$, $j=1,\ldots,n$。由於 $\langle p_1(x),\ldots,p_n(x)\rangle$ 是包含 $p_1(x),\ldots,p_n(x)$ 的最小理想, 所以

$$\langle m(x)\rangle=\langle p_1(x),\ldots,p_n(x)\rangle\subset\langle q(x)\rangle.$$

因此, $m(x)\in\langle q(x)\rangle$, 即 $q(x)\mid m(x)$, 是故 $m(x)$ 爲 $p_1(x),\ldots,p_n(x)$ 的最大公因子。命題證畢。

值得一提的是：由兩個變數 x 和 y 的多項式的全體組成的多項式環 $R=\mathbb{F}[x,y]$ 是整域, 但不再是主理想整域。下面來證明另一個有用且重要的主理想整域上的素元素的因子分解定理。先給出一些定義。設 R 爲整域。

1. $r,s\in R$, 若存在 $x\in R$, 使得 $s=xr$, 則稱 r 可除 (divide) s, 記作 $r\mid s$。
2. $u\in R$, 若存在 $v\in R$, 使得 $uv=1$, 則稱 u 爲一個可逆元 (unit)。
3. 若 $a,b\in R$, 若存在 R 中可逆元 u, 使得 $a=ub$, 則稱 a, b 相伴。
4. 一個非零非可逆元 $p\in R$ 稱爲素元 (prime), 若 $p\mid ab$ 導出 $p\mid a$ 或 $p\mid b$。

5. 一個非零非可逆元 $p \in R$ 稱爲不可約元 (irreducible), 若 $p = ab$ 導出 a 或 b 是可逆元。由此我們不難得到：

a. $u \in R$ 爲一個可逆元若且唯若 $\langle u \rangle = R$;

b. $a, b \in R$ 相伴若且唯若 $\langle a \rangle = \langle b \rangle$;

c. r 可除 s 若且唯若 $\langle s \rangle \subseteq \langle r \rangle$;

d. r 眞除 (properly divide)s (即 $s = xr$, x 不是一個可逆元) 若且唯若 $\langle s \rangle \subsetneq \langle r \rangle$;

對整數域 $\mathbb{Z}$, 一個整數是素元 (素數或質數) 若且唯若它是不可約元。但一般來說, 這兩者是不一致的, 不過對主理想整域, 這兩者卻是一致的。我們可證明下面的定理:

定理 1.2.2: 若 R 是主理想整域, 則R中元素是素元若且唯若它是不可約元。

證明: 若 p 是素元, 令 $p = ab$, 則 $p \mid ab$, 因此 $p \mid a$ 或 $p \mid b$。若 $p \mid a$, 則 $a = xp$, 於是 $p = ab = xpb$, 由於 R 是一個整域, 故消去律成立, 在上式消去 p 後得 $xb = 1$, 因此 b 是一個可逆元, 所以 p 不可約。注意在這個部分的證明, 我們只用到了 R 是整域, 並未用到 R 是主理想整域, 故這個部分對 R 是整域也成立, 即素元一定是不可約! 下面來證明不可約元一定是素元。我們先證明: 若 $r \in R$ 是不可約元, 則主理想 $\langle r \rangle$ 是極大理想 (maximal ideal), 即 $\langle r \rangle \neq R$, 且不存在理想 $\langle a \rangle$ 使得 $\langle r \rangle \subsetneq \langle a \rangle \subsetneq R$。若有 $\langle a \rangle$ 使得 $\langle r \rangle \subset \langle a \rangle \subset R$, 則 $r = xa$, $x \in R$。由於r爲不可約元, 故a或x爲可逆元。若a爲可逆元, 則由條件 a. 知道$\langle a \rangle = R$; 若x爲可逆元, 則由條件 b. 知道$\langle a \rangle = \langle xa \rangle = \langle r \rangle$; 這都得到矛盾。故$\langle r \rangle$爲一個極大理想。若有 r 爲不可約元, 且 $r \mid ab$, 要證 $r \mid a$ 或 $r \mid b$, 即 r 爲素元。由條件 c. 知道 $ab \in \langle r \rangle$。由剛才已知道的 $\langle r \rangle$ 爲一個極大理想, 我們要證明: $a \in \langle r \rangle$ 或 $b \in \langle r \rangle$。若$a \notin \langle r \rangle$, 由於 $\langle r \rangle$ 爲一個極大理想, 故 $\langle a, r \rangle = R$, 因此有 $x, y \in R$, 使得 $1 = xa + yr$。將此式兩邊右乘以 b, 得到 $b = xab + yrb$, 由 $r \mid ab$, 得 $r \mid xab$; 另一方面, 我們顯然知道 $r \mid yrb$, 因此 $r \mid b$, 即 $b \in \langle r \rangle$。同理可證若 $b \notin \langle r \rangle$, 則有 $a \in \langle r \rangle$。這就證明了r是素元。定理因而證畢。

如果 $I_1, I_2, \ldots \in R$ 且滿足

$$I_j \subset I_{j+1}, \qquad j = 1, 2, \ldots$$

則稱 $\{I_j\}$ 爲一個理想升鏈 (ascending chain of ideals)。我們先來證明下面的命題。

命題 1.2.2: 若 R 是主理想整域, 則任意理想升鏈 $\{\langle a_j \rangle\}$ 一定有限的, 即存在一個正整數 m, 使得

$$\langle a_m \rangle = \langle a_{m+1} \rangle = \langle a_{m+2} \rangle = \cdots .$$

證明: 令 $I = \cup_j \langle a_j \rangle$。則可證明 I 是一個理想。對於任意 $b, c \in I$, 則 b, c 分屬於某個 $\langle a_j \rangle$ 與 $\langle a_k \rangle$。不妨假設 $j \leq k$。於是 $\langle a_j \rangle \subset \langle a_k \rangle$。因此, $b \in \langle a_k \rangle$, $b - c \in \langle a_k \rangle$, 從而

$b-c\in I$。對於任意 $d\in R$, $b\in\langle a_j\rangle$, 得 $bd\in\langle a_j\rangle$ 及 $db\in\langle a_j\rangle$, 因此, $bd\in I$ 及 $db\in I$。所以 I 是 R 的一個理想。由於 R 是主理想整域, 故存在 $e\in R$ 使得 $I=\langle e\rangle$。由 I 的定義, 我們知道 e 屬於某個 $\langle a_m\rangle$, 從而 $I\subset\langle a_m\rangle$; 反之, 顯然 $\langle a_m\rangle\subset I$, 故 $I=\langle a_m\rangle$。對於任意大於 m 整數 n 有 $\langle a_m\rangle\subset\langle a_n\rangle\subset I$, 由 $\langle a_m\rangle=I$ 推出 $\langle a_n\rangle=I$, 最後得到

$$I=\langle a_m\rangle=\langle a_{m+1}\rangle=\langle a_{m+2}\rangle=\cdots.$$

命題證畢。

由命題1.2.2可得如下定理:

定理 1.2.3: (主理想整域上素元分解定理) 若 R 是主理想整域, 則任一 $r\in R$, $r\neq 0$ 可寫成

$$r=u\,p_1\cdots p_n,$$

這裡 u 是可逆元, $p_1,\ \ldots,\ p_n$是素元。除去排列次序及可逆元 u 外, 這樣的因子分解是唯一的。

證明: 由定裡1.2.2, R 是主理想整域時, 素元與不可約元是一致的, 故只要將 $r\in R$ 分解不可約元的乘積即可。若 $r\in R$, 如果 r 爲不可約元, 則定理之結論顯然成立。若不是, 則 $r=r_1r_2$, 而 r_1 與 r_2 都不是可逆元, 若 r_1 與 r_2 都是不可約元, 則定理得證; 如果不是, 假設 r_2 不是不可約元, 則 $r_2=r_3r_4$, 而 r_3 與 r_4 不是不可逆元, 這個步驟可一直進行下去, 則 R 分解爲

$$r=r_1r_2=r_1(r_3r_4)=(r_1r_3)(r_5r_6)=(r_1r_3r_5)(r_7r_8)=\cdots.$$

每步分解將 r 分解爲非可逆元的乘積, 但這種分解經過有限步後停止, 這是因爲

$$r_2\mid r,\ r_4\mid r_2,\ r_6\mid r_4,\ldots,$$

故由上述條件3, 我們得到一上升理想序列

$$\langle r\rangle\subset\langle r_2\rangle\subset\langle r_4\rangle\subset\langle r_6\rangle\subset\cdots. \tag{1.2.1}$$

由於所有 r_j 不可逆, 故由上述條件4, 上式的包含是眞包含。如果這種分解不能停止, 則得到一個上升的理想無窮序列, 由命題1.2.2, 這個升鏈一定有限, 即有 n 使得

$$\langle r_{2n}\rangle\subset\langle r_{2(n+1)}\rangle\subset\langle r_{2(n+2)}\rangle\subset\cdots.$$

這與前面理想無窮序列 (**??**) 中的包含是眞包含相互矛盾。於是我們得到

$$r=r_1r_3\cdots r_{2n-1}r_{2n},$$

這裡 r_{2n} 是不可約元。記 $r_1 r_3 \cdots r_{2n-1} = s$, 則 $r = s r_{2n}$。對 s 重覆上面的證明, 可分解性得證。利用素元與不可約元的一致性, 幾乎是重複整數環 $\mathbb{Z}$ 的算術基本定理 (唯一質數分解定理) 的唯一性的證明, 我們可以給出定理1.2.3 的唯一性的證明, 此處從略而定理之證明也因此完畢。

1.3. 向量空間與線性變換

在前面1.1 節中已經講到, 線性代數是研究線性空間, 即向量空間、模、和其上線性變換以及與之相關的問題, 如線性函數、雙線性型式等等的數學學科。而其中線性空間是這一切研究的基石, 因此我們先來定義線性空間。線性空間 (linear space), 也稱向量空間 (vector space); 來源於解析幾何中三維向量空間的推廣。當時向量是定義爲有方向、有大小的量, 但這個概念很容易抽象化, 因此下面給出的定義是從這個角度出發, 而其使用的範圍當然要廣泛的多。

定義 1.3.1: 體 $\mathbb{F}$ 中的元素稱爲純量 (scalar)。$\mathbb{F}$ 上的一個向量空間爲一個非空集合 $\mathcal{V}$, 它的元素稱爲向量, 有加法運算法"+", 對 $(\vec{u}, \vec{v}) \in \mathcal{V} \times \mathcal{V}$, 有 $\vec{u} + \vec{v} \in \mathcal{V}$; 以及 $\mathbb{F}$ 與 $\mathcal{V}$ 的純量乘積, 用毗連表示, 對 $(\alpha, \vec{u}) \in \mathbb{F} \times \mathcal{V}$, 有 $\alpha\vec{u} \in \mathcal{V}$, 且滿足以下條件 :

1. $\mathcal{V}$ 對 $+$ 成 Abel 群;
2. $\mathbb{F}$ 對 $\mathcal{V}$ 的純量乘積滿足: 對所有 $\alpha, \beta \in \mathbb{F}$ 及 $\vec{u}, \vec{v} \in \mathcal{V}$ 有
   a. (分配律) $\alpha(\vec{u} + \vec{v}) = \alpha\,\vec{u} + \alpha\,\vec{v}$; $\qquad (\alpha + \beta)\vec{u} = \alpha\,\vec{u} + \beta\,\vec{u}$;
   b. (結合律) $(\alpha\,\beta)\vec{u} = \alpha(\beta\,\vec{u})$,
   c. $1\vec{u} = \vec{u}$.

這樣定義的向量空間當然要比解析幾何中定義的向量空間要廣泛的多。例如 :

1. 所有將體 $\mathbb{F}$ 映到 $\mathbb{F}$ 的函數的集合是一個向量空間。
2. 所有元素 (entries) 取自體 $\mathbb{F}$ 的 $m \times n$ 矩陣之集合, 對矩陣的加法與矩陣的純量乘積成一個向量空間, 記作 $\mathcal{M}_{m\times n}(\mathbb{F})$; 若 $m = n$, 則記作 $\mathcal{M}_n(\mathbb{F})$。

我們再來定義線性變換。大致來說, 線性變換是將一個向量空間映到另一個向量空間, 且保持向量空間中運算的映射。

定義 1.3.2: $\mathcal{V}$ 與 $\mathcal{W}$ 是體 $\mathbb{F}$ 上的兩個向量空間, 映射 $T : \mathcal{V} \to \mathcal{W}$ 稱爲線性變換 (linear transform), 若對任意的 $\alpha, \beta \in \mathbb{F}$ 及 $\vec{u}, \vec{v} \in \mathcal{V}$, 有

$$T(\alpha\vec{u} + \beta\vec{v}) = \alpha T(\vec{u}) + \beta T(\vec{v}).$$

從 $\mathcal{V}$ 到 $\mathcal{W}$ 所有線性變換的集合記爲 $\mathcal{L}(\mathcal{V}, \mathcal{W})$。我們稱線性變換 $T : \mathcal{V} \to \mathcal{V}$ 爲 $\mathcal{V}$ 上的線性算子 (linear operator); 在 $\mathcal{V}$ 上所有線性算子的集合記爲 $\mathcal{L}(\mathcal{V})$。

在各種代數結構中, 就有一種結構叫代數, 定義如下。

定義 1.3.3: 若 $\mathbb{F}$ 爲一個體, $\mathbb{F}$ 上的一個代數 (algebra) $\mathcal{A}$ 爲一個非空集合 $\mathcal{A}$, 且有兩種運算：加法 (記作+), 乘法 (用毗連表示) 以及 $\mathbb{F}$ 對 $\mathcal{A}$ 的純量乘積 (也用毗連表示) 滿足以下規律：

A. 對加法與 $\mathbb{F}$ 對 $\mathcal{A}$ 的純量乘積, $\mathcal{A}$ 是一個向量空間;

B. 對加法與乘法, $\mathcal{A}$ 是一個有單位元的環;

C. 若$\alpha \in \mathbb{F}$及$\vec{u}, \vec{v} \in \mathcal{A}$, 有

$$\alpha(\vec{u}\,\vec{v}) = (\alpha\vec{u})\vec{v} = \vec{u}(\alpha\vec{v}).$$

也就是說, 代數是有向量乘法的向量空間, 代數是可以對每個元素進行純量乘積的環。也可以說代數既是向量空間又同時是環, 是向量空間與環的結合。

若 $\mathcal{V}$ 是 $\mathbb{F}$ 上的向量空間, 對於 $\mathcal{L}(\mathcal{V})$, 定義 $\mathcal{L}(\mathcal{V})$ 中兩個元素的乘法爲函數的合成, 取 $\mathcal{L}(\mathcal{V})$ 中的恆等映射爲 $\mathcal{L}(\mathcal{V})$ 中乘法的單位元, 則容易證明 $\mathcal{L}(\mathcal{V})$ 的確是 $\mathbb{F}$ 上的一個代數。當然, 我們尙可以舉出許多其他的例子, 如李代數 (Lie algebra)、四元數 (Quaternion)、八元數 (Octonion) 及其他 Clifford 代數等等。

線性變換與向量空間是相輔相成的, 是相互依存的。向量空間是線性變換的載體, 沒有向量空間, 線性變換無用武之地, 對它進行研究也就沒有多大意義。反之, 向量空間本身如果沒有線性變換作用其上, 則向量空間是死的, 沒有太多內容可討論。正如在1.1節所提到的, 近世代數的主要內容是集合及這些集合上的代數運算。集合本身和作爲代數運算的載體的集合是不加區分的, 故實質上是研究代數運算本身。而線性代數實質上是在研究$\mathcal{L}(\mathcal{V})$, 如上所述, $\mathcal{L}(\mathcal{V})$ 的確是一個代數。討論帶有一個線性變換 T 的向量空間 $\mathcal{V}$, 從模的觀點看就是討論 $\mathbb{F}[x]$ 上的模。我們將在第四講中詳細地討論主理想環上的模及其分解。這就是我們這一系列演講從模的觀點來討論線性代數的出發點。

1.4. 同構、等價、相似與相合

若 S_1 與 S_2 爲兩個集合, $f : S_1 \to S_2$ 爲從 S_1 到 S_2 的一個映射。稱 f 爲單射 (injective) 或一對一 (one to one), 若

$$x \neq y \Rightarrow f(x) \neq f(y).$$

稱 f 爲滿射 (surjective) 或映成 (onto), 若 $f(S_1) = S_2$; 我們稱 f 爲雙射 (bijective), 若 f 既是單射又是滿射。稱 $f(S_1) = \{f(s) \in S_2 : \ s \in S_1\}$ 爲 f 的像 (image), 記作 $\mathrm{Im}(f)$。

若 $\mathcal{V}$ 與 $\mathcal{W}$ 是 $\mathbb{F}$ 上的兩個向量空間, $T \in \mathcal{L}(\mathcal{V}, \mathcal{W})$, 稱 $\{\vec{v} \in \mathcal{V} : \ T(\vec{v}) = \vec{0}\}$ 爲 T 的核 (kernel), 記作 $\mathrm{Ker}(T)$。不難證出:

1. T 是滿射若且唯若 $\mathrm{Im}(T) = \mathcal{W}$;
2. T 是單射若且唯若 $\mathrm{Ker}(T) = \vec{0}$。

若線性變換 $T \in \mathcal{L}(\mathcal{V}, \mathcal{W})$ 是雙射, 則稱 T 爲從 $\mathcal{V}$ 到 $\mathcal{W}$ 的同構變換 (isomorphism), 稱 $\mathcal{V}$ 與 $\mathcal{W}$ 同構, 記作 $\mathcal{V} \approx \mathcal{W}$。

同構是線性代數中極爲重要的概念, 兩個向量空間是同構的, 則有線性變換, 使這兩個空間的向量一一對應, 且還保持線性不變, 這時我們往往將這兩個向量空間視爲同一個。如對向量空間進行分類, 就是指在同構意義下的分類。更一般地, 有等價關係。

若 X 是一個非空集合, X 上的一個二元關係 $\sim$ 稱爲 X 上的等價關係 (equivalence relation), 若它滿足如下三個條件：

a. 自反性 (reflexivity)：對所有的 $x \in X$, 有 $x \sim x$;
b. 對稱性 (symmetry)：對所有的 $x, y \in X$, 有 $x \sim y \ \Rightarrow \ y \sim x$;
c. 可遞性 (transitivity): 對所有的 $x, y, z \in X$, 有 $x \sim y \ y \sim z \ \Rightarrow \ y \sim z$。

若 $x \in X$, 集合 $[x] = \{y \in X : \ y \sim x\}$ 稱爲 x 的等價類 (equivalent class)。若 X 是一個非空集合, X 上的一個劃分 (partition) 是 X 的一個非空部分集合的集合 $\{A_1, \ldots, A_n, \ldots\}$ 滿足

i. $A_j \cap A_k = \emptyset$ 對所有 $j \neq k$ 都成立;
ii. $X = A_1 \cup A_2 \cup \cdots \cup A_n \cup \cdots$。

這些A_j, $j = 1, \ldots, n, \ldots$, 稱爲塊 (block)。

顯然, 若 $\sim$ 是 X 上的一個等價關係, 對 $\sim$ 所得到的不同的等價類是 X 上劃分的塊; 反之, 若 $\mathcal{P}$ 是 X 上的一個劃分, 定義 $x \sim y \ \Leftrightarrow \ x, y$ 在 $\mathcal{P}$ 的同一個塊中, 則 $\sim$ 是等價關係, 它的等價類就是 $\mathcal{P}$ 的塊。於是, X 的等價關係與 X 的劃分是一一對應的。

設 $\sim$ 是 X 的等價關係, X 的一個部分集合 C 稱爲對 $\sim$ 而言的標準形式 (canonical form), 若對每一個 $x \in X$, 在 C 中有唯一的一個 c, 使得 $x \sim c$。顯然, 對於向量空間, 同構就是等價關係, 在後面幾次演講中, 我們將討論這個等價關係下, 向量空間的標準形式。

假設 $A, B \in \mathcal{M}_n(\mathbb{F})$, 稱 A 與 B 等價 (equivalent), 若存在可逆矩陣 P 及 Q 使得

$$A = PBQ;$$

稱 A 與 B 相似 (similar), 若存在可逆矩陣 P 使得

$$A = PBP^{-1};$$

稱 A 與 B 相合 (congruent), 若存在可逆矩陣 P 使得

$$A = PBP^{T};$$

這裡 P^T 爲矩陣 P 的轉置 (transport)。

顯而易見, 這三種矩陣的關係都是等價關係。在一個有限維向量空間上同一個線性算子在不同的基下所對應的矩陣之間的關係是相似關係 (參閱第3.1節)。我們在第五講中將給出相似關係下的標準型式。在一個有限維向量空間上同一個雙線性型式在不同的基下所對應的矩陣之間的關係是相合關係 (參閱第3.2節)。我們在第二講中將給出相合關係下的標準型式。在兩個有限維向量空間之間的線性變換, 在這兩個向量空間的各自取定的基下所對應的矩陣之間的關係是等價關係 (參閱第3.1節)。

若 $A \in \mathcal{M}_n(\mathbb{F})$, 熟知對 A 有三個初等運算:

1. 對 A 中的一行 (或一列) 乘以非零的 $\alpha \in \mathbb{F}$;
2. 將 A 中的兩行或兩列交換;
3. 對 A 中的一行 (或一列) 乘以非零的 $\alpha \in \mathbb{F}$, 然後加到另一行 (或一列) 上。

對 A 行 (或列) 的初等運算相當於對 A 左 (或右) 乘以相應的矩陣。不難證明: 任意 $A \in \mathcal{M}_n(\mathbb{F})$, 經過行與列的初等運算都可以變爲

$$N_k = \begin{bmatrix} I_k & 0 \\ 0 & 0 \end{bmatrix}.$$

這裡 $k \leq n$, I_k 爲 $k \times k$ 的單位矩陣。因此, 在等價關係下, 矩陣 $A \in \mathcal{M}_n(\mathbb{F})$ 的標準型式就是 N_k, $k = 0, 1, 2, \ldots, n$。

後記

這幾篇文章是依據第一作者在中國科技大學及第二作者在美國喬治城大學、馬里蘭大學 College Park 分校所作的一系列演講所編寫而成。作者特別在此向這幾間大學的同仁致謝, 感謝他們對這些演講所提供的意見。第二作者希望將這五篇文章獻給他在新竹清華大學求學時的一位老師: 呂輝雄教授, 作爲對他的思念與感謝, 他是教導第二作者外微分型式及 Jordan 標準型式的第一個人。

—本文作者龔昇任教於中國科技大學; 張德健任教於美國 Georgetown University 數學系—